Pietro Di Martino

Algebra

Nuova edizione

PISA
UNIVERSITY
PRESS

MANUALI

Di Martino, Pietro
Algebra / Pietro Di Martino. - Nuova ed. - Pisa : Pisa university press, 2013. - (Didattica e ricerca. Manuali)

512 (22.)
1. Algebra - Manuali

CIP a cura del Sistema bibliotecario dell'Università di Pisa

UPI
UNIVERSITY PRESS ITALIANE

Membro Coordinamento
University Press Italiane

Società con socio unico Università di Pisa
Capitale Sociale € 20.000,00 i.v. - Partita IVA 02047370503
Sede legale: Lungarno Pacinotti 43/44 - 56126 Pisa
Tel. + 39 050 2212056 - Fax + 39 050 2212945
press@unipi.it
www.pisauniversitypress.it

ISBN 978-88-6741-229-7

Indice

Premessa alla nuova edizione

La prima edizione di questo volume ha avuto un discreto successo. Nonostante ciò il volume necessitava di un aggiornamento legato anche ai cambiamenti dell'insegnamento dell'Algebra per il Corso di Laurea in Matematica.

La nuova edizione dunque, mantenendo la filosofia che ha ispirato il primo volume, si presenta essenzialmente come un testo nuovo: sono state tolte alcune parti che tipicamente vengono trattate in corsi differenti da quelli di base di algebra (come ad esempio la cardinalità per insiemi infiniti) e ne sono state aggiunte altre (ad esempio tutta la parte sui p-gruppi).

Sono stati inoltre approfonditi e ri-organizzati tutti i contenuti, ed il volume stesso è stato organizzato in due parti separate: la prima in cui sono trattati gli argomenti dell'aritmetica, e la seconda in cui si introducono le strutture algebriche. Si è inoltre organizzato i capitoli per difficoltà e gradi di astrazione crescenti. In questo modo si è pensato di rendere il volume, pensato di ausilio per corsi di Algebra di livello diverso, di più facile uso e consultazione.

Un ulteriore aspetto di novità riguarda la ri-organizzazione, l'ampliamento e l'aggiornamento degli esercizi presenti. Gli esercizi sono stati rinnovati ed inseriti tutti all'interno del testo (e non più in appendice), aumentando il numero di quelli proposti (più di 200 dei quali più della metà risolti) e cercando di aumentare la diversificazione tra un esercizio e l'altro.

È stata inoltre posta maggiore attenzione all'indice analitico, arricchendolo con molte voci, con l'obiettivo di rendere più semplice la consultazione rapida del testo.

I pre-requisiti sono rimasti essenzialmente quelli della versione originale. Per seguire i contenuti di questo volume è necessario conoscere le definizioni e le proprietà basilari relative alla nozione di insieme. In particolare supporremo conosciute le definizioni di: insieme (come collezione di oggetti), appartenenza di un elemento ad un insieme, sottoinsieme, insieme unione, insieme intersezione, insieme differenza, insieme complementare e prodotto cartesiano di insiemi. Supporremo inoltre conosciuti i connettivi logici di "e" ($\wedge$), "o" ($\vee$), "not", "implica" e le rispettive tavole di verità e i quantificatori esistenziali ($\exists$) e universali ($\forall$), nonché una certa dimestichezza con i simboli di sommatoria ($\sum$) e produttoria ($\prod$). Altre nozioni preliminari sono invece richiamate brevemente nei prossimi paragrafi.

Più avanti, quando tratteremo di radici di polinomi, sarà invece supposta la conoscenza dei numeri complessi almeno per quanto riguarda la loro rappresentazione, le operazioni su di essi e il metodo per il calcolo delle radici n-esime di un numero complesso. La scelta di omettere questo argomento è dovuta al fatto che, se è vero che tale insieme numerico non sempre è trattato a livello di scuola superiore, è anche vero che dovrebbe però essere argomento del corso di Analisi: si presuppone perciò che lo studente li abbia già incontrati. Se così non fosse consigliamo di studiarsi le nozioni riportate sopra su qualsiasi libro di Analisi zero (ovvero di raccordo scuola superiore-università). Si parlerà anche di spazi vettoriali senza definirli, supponendo che la conoscenza di questa struttura sia acquisita nel corso del primo anno che tratta l'algebra lineare.

P. Di Martino, Pisa $23 - 09 - 2013$

Ringraziamenti e dediche

Per il lavoro di questa nuova edizione devo ringraziamenti a molte persone, a partire da Roberto Dvornicich. L'idea di questo volume è nata dagli appunti presi al corso di Algebra da lui tenuto quasi 15 anni fa. Come scrissi per la prima edizione: "L'idea di scrivere quegli appunti mi è venuta non solo per fornire agli studenti un sussidio per i loro corsi di Algebra di base, ma anche per trasmettere la mia passione per quel corso alle nuove matricole."

Un grosso ringraziamento anche a Ilaria Del Corso, che contribuì alla riuscita di quel corso di Algebra di tanti anni fa, e che mi ha dato molti consigli utili per la riorganizzazione del volume, nonché prestato la sua copia del testo con preziosissime correzioni a margine.

Altri ringraziamenti ai tanti che, nel corso degli anni, mi hanno segnalato errori vari riscontrati nella prima versione del testo. Un ringraziamento in particolare a Elena Addis e Marta Lemmi che, saputo della nuova edizione, mi hanno fornito la loro lista dettagliata di commenti; a Massimo Caboara, con il quale ho condiviso un anno di esercitazioni di Aritmetica; a Giovanni Gronchi per le consulenze informatiche dell'ultimo minuto.

Un grazie a Giovanni Gaiffi, non solo perché facendo esercitazioni con lui in vari corsi all'Università ho imparato tanto, ma anche per essersi prestato a leggere parti del presente volume e a commentarle con la consueta maestria.

Un grazie speciale a Sara Chiti, che ha letto con pazienza e attenzione praticamente tutti i capitoli: il presente volume conterrebbe molte meno virgole e molti più errori senza il suo intervento. I suoi commenti, di natura molto variegata, sono stati per me realmente fondamentali al fine di migliorare il volume, e hanno influenzato, ritengo in maniera decisamente positiva, molte delle scelte fatte.

Un grazie di natura diversa, ma ugualmente sentito, ad Elisa, Cecilia e Niccolò, i quali, nel periodo in cui ho lavorato alla ri-organizzazione del volume, hanno convissuto con un compagno/babbo piuttosto occupato, più distratto del solito (assicuro che non è un'impresa facile), e con una casa piena di fogli sparsi.

Infine una dedica, ad una persona con la quale ho condiviso la passione per la matematica, che mi convinse tanti anni fa, con il suo entusiasmo e i suoi racconti, a fare l'interRail e che mi ha accompagnato in tutti questi giorni al computer, con il calendario di ceramica, frutto delle sue mani e della sua fantasia, in bella vista nel mio studio: mia cugina Claudia.

Parte I

Aritmetica

CAPITOLO 1

Nozioni preliminari

1. Relazioni

In questa sessione introduciamo alcuni concetti che useremo spesso, come ad esempio il concetto di relazione binaria su un insieme X.

Definizione 1.1. Dato un insieme A, una **relazione binaria** $\Re$ su A è un sottoinsieme dell'insieme $A \times A$. Se una coppia (a, b) in $A \times A$ appartiene a $\Re$, si dice che l'elemento a di A è **in relazione** con l'elemento b di A e si scrive $a\Re b$ in luogo di $(a, b) \in \Re$.

Dunque una relazione binaria su un insieme A non è niente di più che un sottoinsieme del prodotto cartesiano $A \times A$. Tra tutte le proprietà che può soddisfare una relazione binaria, alcune, che introduciamo ora, sono particolarmente importanti nello studio delle strutture matematiche.

Definizione 1.2. Una relazione binaria $\Re$ su un insieme A si dice **totale** se per ogni $a, b \in A$ si ha che almeno una delle due condizioni: $a\Re b$, $b\Re a$ è soddisfatta. In termini insiemistici la condizione di essere una relazione totale significa che per ogni a, b di A almeno una delle coppie (a, b), (b, a) appartiene a $\Re$.

Esempio 1.3. Dato un gruppo T di persone, la relazione $\Re$ su T, definita da $a\Re b$ se e solo se a è alto in cm come b o più di b, è una relazione totale su T. È interessante osservare che, se avessimo definito $\Re$ dicendo che $a\Re b$ se e solo se a è più alto di b, allora $\Re$ non sarebbe una relazione totale nel caso in T ci siano due persone alte uguali.

Definizione 1.4. Sia $\Re$ una relazione binaria su A. Se:

i $\forall a \in A$, $a\Re a$ la relazione si dice **riflessiva** su A.
ii $\forall a, b \in A$, $(a\Re b \Rightarrow b\Re a)$ la relazione si dice **simmetrica** su A.
iii $\forall a, b, c \in A$ $(a\Re b \wedge b\Re c \Rightarrow a\Re c)$ la relazione si dice **transitiva** su A.

Esercizio 1.5. *Considerare l'insieme F degli iscritti a Facebook. Su questo insieme considerare la relazione $\Re$ definita da $a\Re b$ se e solo se a appartiene agli amici* fb *di b. Discutere se $\Re$ è totale su F, riflessiva, simmetrica e transitiva.*

Definizione 1.6. Una relazione binaria $\Re$ su un insieme A che sia riflessiva, simmetrica e transitiva si dice una **relazione di equivalenza** su A.

Esempio 1.7. Sia I l'insieme di tutti i residenti in Italia. Consideriamo la relazione $\Re$ definita da $a\Re b$ se e solo se a e b sono residenti nello stesso comune. La relazione $\Re$ su I è di equivalenza.

Definizione 1.8. Data una relazione di equivalenza $\Re$ su un insieme A, e dato un elemento $a \in A$, il sottoinsieme di A formato da tutti gli elementi di A

che sono equivalenti ad a è detto **classe di equivalenza** dell'elemento a rispetto alla relazione $\Re$ ed è solitamente indicato con $[a]_\Re$ (il riferimento a $\Re$ è spesso omesso, quando dal contesto sia evidente a quale relazione di equivalenza si faccia riferimento).

Esempio 1.9. Considerata la relazione totale introdotta nell'Esempio 1.7, le singole classi di equivalenza sono formate da tutti i residenti in uno stesso comune.

Osservazione 1.10. Data una relazione di equivalenza $\Re$ su un insieme A, per ogni $a \in A$ la classe di equivalenza $[a]_\Re$ non è vuota, infatti per la proprietà riflessiva $a \in [a]_\Re$. Inoltre un'altra proprietà che segue dalla simmetria e dalla transitività è che gli elementi che stanno nella classe di equivalenza $[a]_\Re$ sono tutti in relazione tra loro: infatti se $b, c \in [a]_\Re$ allora per definizione $a\Re b$ e $a\Re c$. Per simmetria da questo segue che $c\Re a$ e per transitività che $c\Re b$.

Definizione 1.11. Dato un insieme A, un insieme (finito od infinito) $\mathfrak{F}$ di sottoinsiemi non vuoti di A si dice una **partizione** di A se:

(1) L'unione degli elementi di $\mathfrak{F}$ è uguale ad A, in simboli: $\bigcup_{X\in\mathfrak{F}} X = A$;
(2) Gli elementi di $\mathfrak{F}$ sono a due a due disgiunti (cioè non hanno elementi in comune), in simboli: $\forall B, C \in \mathfrak{F}\ (B \neq C \Rightarrow\ B \cap C = \emptyset)$.

Proposizione 1.12. *Dato un insieme A, e una relazione di equivalenza $\Re$ su A, l'insieme $E = \bigcup_{a\in A}[a]_\Re$, unione di tutte le classi di equivalenza $[a]_\Re$ di A, al variare di a in A, è una partizione di A (sappiamo che le $[a]_\Re$ sono non vuote).*

Dimostrazione. Che l'unione delle classi di equivalenza $[a]_\Re$ di A al variare di a in A sia uguale ad A segue dal fatto che per ogni elemento x di A, per la proprietà riflessiva x appartiene alla classe di equivalenza: $[x]_\Re$.

Consideriamo adesso due classi di equivalenza $[a]_\Re$ e $[b]_\Re$ e sia c un elemento in comune alle due classi (ovvero c è in relazione sia con a che con b). Allora per ogni $x \in [a]_\Re$ si ha, per transitività, che x è in relazione con c. Sempre per transitività, da questo segue che x è in relazione con b, ovvero che $x \in [b]_\Re$. Dunque $[a]_\Re \subset x \in [b]_\Re$. Analogamente si dimostra che ogni elemento di $[b]_\Re$ appartiene ad $[a]_\Re$. Dunque si conclude che $[b]_\Re = [a]_\Re$. Abbiamo dimostrato che se le due classi non sono disgiunte allora sono uguali. □

Definizione 1.13. Data una relazione di equivalenza $\Re$ su di un insieme A, l'insieme delle classi di equivalenza di $\Re$ su A si dice **insieme quoziente** di A rispetto a $\Re$. Tale insieme si indica solitamente con $A/_\Re$.

Osservazione 1.14. Osserviamo che, per come è definito, l'insieme quoziente di A rispetto a $\Re$ è un insieme di sottoinsiemi di A.

Definizione 1.15. Data una relazione di equivalenza $\Re$ su di un insieme A, un sottoinsieme R di A si dice un **insieme di rappresentanti** per $\Re$ se per ogni elemento C di $A/_\Re$ si ha che R e C hanno in comune uno e un solo elemento.

Introduciamo infine un'altra categoria importante di relazioni:

Definizione 1.16. Sia $\Re$ una relazione binaria su A, se $\forall a, b \in A\ a\Re b$ e $b\Re a$ implica $a = b$ la relazione si dice **antisimmetrica** su A.

Definizione 1.17. Una relazione binaria $\Re$ su A che sia riflessiva, antisimmetrica, e transitiva si dice una **relazione di ordine** su A. Si dice anche che il sottoinsieme delle coppie in $A \times A$ appartenenti a $\Re$ definisce un **ordine** su A.

2. Funzioni

Il concetto di funzione è sicuramente un concetto trattato a livello di scuola superiore. Spesso si fa riferimento alla seguente definizione:

Definizione 1.18. Una funzione f da A a B è una legge che ad ogni elemento di A associa uno e un solo elemento di B. Gli insiemi A e B si dicono rispettivamente **dominio**, e **codominio** della funzione f.

La Definizione 1.18 non è una vera e propria definizione matematica, in quanto il significato del termine *legge* è tutt'altro che univocamente definito. Per dare dunque una definizione più rigorosa, spesso si identifica la funzione con quello che solitamente viene chiamato il *grafico* della funzione:

Definizione 1.19. Siano A, B non vuoti, una **funzione** f da A a B, che indicheremo con la notazione $f : A \longrightarrow B$, è un sottoinsieme del prodotto cartesiano $A \times B$ tale che:

(1) $\forall a \in A \ \exists b \in B \ (a, b) \in f$.
(2) Se $(a, b_1) \in f$ e $(a, b_2) \in f$ allora $b_1 = b_2$.

Scriveremo $f(a) = b$ per indicare che $(a, b) \in f$: l'elemento b è detto l'**immagine** di a tramite f, mentre a è detta una **controimmagine** di b rispetto a f.

Osservazione 1.20. L'immagine di un elemento del dominio è unica per definizione di funzione (proprietà 2 della Definizione 1.19), ma, in generale, questo non è vero per la controimmagine di un elemento b di B (e per questo nella definizione si usa l'articolo indeterminativo *una*). Infatti nella Definizione 1.19 non è richiesto che, se (a_1, b) e (a_2, b) appartengono a f allora $a_1 = a_2$.

È inoltre possibile che la controimmagine di un elemento b di B non esista: ovvero che non ci sia nessuna a in A per cui $f(a) = b$ (in termini insiemistici che, per ogni a di A, (a, b) non appartiene a f).

Definizione 1.21. Dati una funzione $f : A \longrightarrow B$ e $C \subset B$, l'insieme

$$f^{-1}(C) = \{a \in A | f(a) \in C\}$$

è detto **insieme controimmagine** di C tramite f. L'insieme

$$f(A) = \{b \in B | \exists a \in A \ \ f(a) = b\}$$

delle immagini di tutti gli elementi di A tramite f è detto **insieme immagine** di A tramite f.

Abbiamo osservato in 1.20 come, in generale, data una funzione f da A a B, non è detto che per ogni b in B esista un a in A con $f(a) = b$, e nemmeno che in caso a esista, sia unico. Introduciamo allora le seguenti definizioni per caratterizzare quelle funzioni che hanno una o entrambe le proprietà.

Definizione 1.22. Una funzione f da A in B si dice **iniettiva**, se per ogni $b \in f(A)$ esiste un solo $a \in A$ tale che $f(a) = b$. Ovvero una funzione è iniettiva se da $f(a_1) = b$ e $f(a_2) = b$ segue necessariamente che $a_1 = a_2$

Definizione 1.23. Una funzione f da A in B si dice **surgettiva** se $f(A) = B$, ovvero per ogni $b \in B$ esiste almeno un $a \in A$ tale che $f(a) = b$.

Definizione 1.24. Una funzione f da A in B si dice **bigettiva** se è iniettiva e surgettiva.

Esempio 1.25. Dato un insieme A la funzione **identità** i da A in A che ad ogni a di A associa a stesso ($\forall a \in A\ i(a) = a$) è bigettiva.

Esempio 1.26. Sia $\Re$ una relazione di equivalenza su un insieme A. La funzione $\pi_\Re : A \longrightarrow A/_\Re$, che ad ogni a in A associa la sua classe di equivalenza $[a]_\Re$, è detta **proiezione canonica sul quoziente**, ed è surgettiva. Se R è un insieme di rappresentanti per $\Re$, allora la restrizione di $\pi_\Re$ al sottoinsieme R di A è bigettiva.

Definizione 1.27. Date $f : A \longrightarrow B$ e $g : B \longrightarrow C$ la funzione $g \circ f$ da A in C definita da $\forall a \in A$, $g \circ f(a) = g(f(a))$ è detta **funzione composta** di f con g.

Esercizio 1.28. *Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$. Dimostrare che:*

(1) *Se f, g sono iniettive anche $g \circ f$ lo è.*
(2) *Se f, g sono surgettive anche $g \circ f$ lo è.*
(3) *Se $g \circ f$ è iniettiva allora f è iniettiva ma g può non esserlo.*
(4) *Se $g \circ f$ è surgettiva allora g è surgettiva ma f può non esserlo.*

Svolgimento. Verifichiamo le quattro proposizioni proposte una ad una, facendo riferimento alle Definizioni 1.22 e 1.23.
(1) Per dimostrare che $g \circ f$ è iniettiva, bisogna far vedre che se $x, y \in A$ hanno la stessa immagine tramite $g \circ f$ (ovvero $g \circ f(x) = g \circ f(y)$) allora sono lo stesso elemento, (ovvero $x = y$).

$$\underbrace{g(f(x))}_{g\circ f(x)} = \underbrace{g(f(y))}_{g\circ f(y)} \underbrace{\Rightarrow}_{g\ iniettiva} f(x) = f(y) \underbrace{\Rightarrow}_{f\ iniettiva} x = y$$

(2) Per ogni $c \in C$ dobbiamo dimostrare che esiste $a \in A$ tale che $g \circ f(a) = c$. Essendo g surgettiva per ipotesi, esiste $b \in B$ tale che $g(b) = c$. Essendo f surgettiva per ipotesi esiste $a \in A$ tale che $f(a) = b$ allora $g \circ f(a) = g(f(a)) = g(b) = c$.

(3) Supponiamo che esistano $x, y \in A$ diversi, e tali che $f(x) = f(y) = b$. Avremmo che $g \circ f(x) = g(f(x)) = g(b) = g(f(y)) = g \circ f(y)$. Assurdo in quanto $g \circ f$ è per ipotesi iniettiva. Mostriamo ora con un controesempio che $g \circ f$ iniettiva non garantisce che g sia iniettiva. Basta considerare il caso di A con un solo elemento, B con più di un elemento e C con un solo elemento. Evidentemente ogni funzione da un insieme con un solo elemento è iniettiva (quindi ogni funzione da A in B e anche ogni funzione A in C sono in questo caso iniettive), mentre una funzione da un insieme con più di un elemento in un insieme di un elemento non può essere iniettiva. Quindi scegliendo f, g funzioni qualsiasi tra insiemi A, B, C di questo tipo si ha: f iniettiva, g non iniettiva e $g \circ f$ iniettiva.
(4) Se $g(B)$ fosse contenuto strettamente in C, $g \circ f(A)$, che è sempre contenuto in $g(B)$, sarebbe contenuto strettamente in C, e quindi $g \circ f$ non sarebbe surgettiva. Deve quindi essere $g(B) = C$, ossia g surgettiva. Per mostrare che f non è necessariamente surgettiva basta considerare lo stesso controesempio del punto precedente: infatti ogni funzione da A (con un solo elemento) a B (con più di un elemento) non può essere surgettiva, invece qualsiasi funzione da A in C e da B in C essendo C con un solo elemento è surgettiva.

Esercizio 1.29. *Siano A, B insiemi e $f : A \longrightarrow B$ allora:*

(1) *f è iniettiva se e solo se per ogni insieme C e per ogni coppia di funzioni g, h da B a C $g \circ f = h \circ f$ implica $g = h$.*

(2) *f è surgettiva se e solo se per ogni insieme C e per ogni coppia di funzioni g, h da C in A $f \circ g = f \circ h$ implica $g = h$.*

Definizione 1.30. Una funzione $f : A \longrightarrow B$ si dice **invertibile** se esiste una funzione $g : B \longrightarrow A$ tale che, per ogni $a \in A$, $(g \circ f)(a) = a$ e per ogni $b \in B$ $(f \circ g)(b) = b$, ovvero $g \circ f = i_A$ e $f \circ g = i_B$. La funzione g si dice **inversa** di f.

Esercizio 1.31. *Dimostrare che l'inversa di una funzione invertibile f è unica (e sarà denotata con f^{-1}) e che è bigettiva.*

Teorema 1.32. *Una funzione $f : A \longrightarrow B$ è invertibile se e solo se è bigettiva.*

DIMOSTRAZIONE. $\Rightarrow$) Per ipotesi esiste $g : B \longrightarrow A$ tale che $g \circ f = id_A$ e $f \circ g = id_B$. Dall'Esercizio 1.28 segue che: f è sia iniettiva (in quanto $g \circ f$ lo è), che surgettiva (in quanto $f \circ g$ lo è), ovvero f è bigettiva.

$\Leftarrow$) Supponiamo f bigettiva e sia $b \in B$. Dalla bigettività di f segue che esiste un unico $a \in A$ tale che $f(a) = b$. Consideriamo la funzione $g : B \longrightarrow A$ che ad ogni $b \in B$ associa l'unico elemento a di A tale che $f(a) = b$. La funzione g è inversa di f, in quanto, per ogni $a \in A$, $(g \circ f)(a) = g(f(a)) = g(b) = a$, e, per ogni $b \in B$, $(f \circ g)(b) = f(g(b)) = f(a) = b$. □

Esercizio 1.33. *Se $f : A \longrightarrow B$ è una funzione surgettiva, allora esiste un sottoinsieme X di A tale che f ristretta ad X è una funzione bigettiva da X a B.*

Esercizio 1.34. *Se $f : A \longrightarrow B$ è una funzione iniettiva, allora esiste un sottoinsieme Y di B tale che f è una funzione bigettiva da A a Y.*

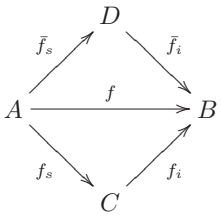
Esercizio 1.35. *Se f è una funzione bigettiva da A a B, e g, h sono funzioni da B in C con $g \circ f = h \circ f$, allora $g = h$. Se s, t sono funzioni da C in A tali che $f \circ s = f \circ t$ allora $s = t$.*

Il seguente teorema mostra come ogni funzione tra due insiemi possa essere vista come la composizione di una funzione surgettiva con una iniettiva.

Teorema 1.36 (Teorema di omomorfismo tra insiemi)**.** *Sia $f : A \longrightarrow B$, esistono un insieme C, e due funzioni $f_s : A \longrightarrow C$ surgettiva e $f_i : C \longrightarrow B$ iniettiva, tali che $f = f_i \circ f_s$. Inoltre dati un insieme D, $\bar{f}_s : A \longrightarrow D$ surgettiva e $\bar{f}_i : D \longrightarrow B$ iniettiva, esiste un'unica funzione $\varepsilon : D \longrightarrow C$ bigettiva e tale che $f_s = \varepsilon \circ \bar{f}_s$ e $\bar{f}_i = f_i \circ \varepsilon$.*

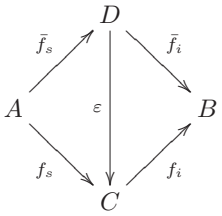
DIMOSTRAZIONE. Consideriamo $C = f(A)$ e siano $f_s = f$[1] e $f_i = id_C$, allora è facile osservare che effettivamente $f = f_i \circ f_s$ e che f_s è surgettiva, e f_i è iniettiva (osserviamo anche che se f è surgettiva allora f_i è bigettiva).

Per la seconda parte, la situazione è quella descritta nel seguente diagramma:



[1]In realtà, seguendo la definizione formale di funzione che abbiamo dato, c'è una differenza tra f_s e f: entrambe sono lo stesso insieme di coppie di elementi di $A \times B$ ma f_s è un sottoinsieme di $A \times f(A)$ mentre f è un sottoinsieme di $A \times B$.

Quello che vogliamo dimostrare è che esiste una bigezione ε da D a C tale che $f_s = \varepsilon \circ \bar{f}_s$ e $\bar{f}_i = f_i \circ \varepsilon$. Questo equivale a dire, usando un linguaggio che adotteremo spesso, che il diagramma sotto **commuta**. Ovvero, partendo da un qualsiasi punto del diagramma, è indifferente il percorso scelto per arrivare al punto di arrivo: seguendo le frecce orientate, il risultato finale non dipenderà dalla *strada* scelta.



Per ogni $d \in D$ definiamo $\varepsilon(d) = \bar{f}_i(d)$ ne segue che ε è iniettiva e che $\varepsilon \circ \bar{f}_s = \bar{f}_i \circ \bar{f}_s = f = f_s$ e dunque ε è anche surgettiva (si applica il risultato dell'Esercizio 1.28 alla funzione surgettiva f_s). L'unicità segue dall'Esercizio 1.35. □

Abbiamo introdotto il concetto di relazione di equivalenza e di funzione, data $f : A \longrightarrow B$ possiamo definire la seguente relazione binaria su A: $r \Re_f s$ se e solo se $f(r) = f(s)$.

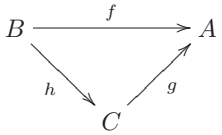
Esercizio 1.37. *Dimostrare che data una funzione $f : A \longrightarrow B$, la relazione binaria $\Re_f$ su A introdotta sopra è di equivalenza su A.*

Proposizione 1.38. *Sia f una funzione da A a B. Consideriamo l'insieme $D = A/_{\Re_f}$ e la proiezione canonica $\pi : A \longrightarrow D$. Esiste un'applicazione iniettiva $\bar{f}$ da D a B tale che $f = \bar{f} \circ \pi$.*

Dimostrazione. Per ogni elemento $d \in D$ esiste almeno un elemento $a \in A$ tale che $\pi(a) = d$ (la proiezione canonica è surgettiva). Definiamo $\bar{f}(d) = f(a)$, dobbiamo mostrare che questa è una buona definizione, ovvero che $\bar{f}(d)$ sia univocamente determinato. Affinché lo sia, per come è definito, non deve dipendere dal rappresentante a di d scelto in A. Ovvero se a_1, a_2 sono due elementi di A tali che $\pi(a_1) = \pi(a_2) = d$ allora deve essere $f(a_1) = f(a_2)$. Questo è vero per definizione di $\Re_f$: a_1 e a_2 stanno nella stessa classe di equivalenza se e solo se la loro immagine tramite f è uguale. Questo dimostra anche che $\bar{f}$ è iniettiva, infatti se d_1, d_2 sono due elementi diversi di D allora prendendo due rispettivi rappresentanti a_1, a_2 in A si ha $f(a_1) \neq f(a_2)$ e dunque $\bar{f}(a_1) \neq \bar{f}(a_2)$. Infine il fatto che $\bar{f} \circ \pi$ sia uguale a f è un'immediata conseguenza della definizione data di $\bar{f}$. □

Da questo, e dal teorema 1.36, segue che l'insieme $D = A/_{\Re_f}$ è in corrispondenza biunivoca con $f(A)$.

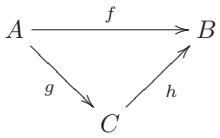
Esercizio 1.39. *Siano A, B, C insiemi non vuoti e $f : B \longrightarrow A$, $g : C \longrightarrow A$ allora esiste $h : B \longrightarrow C$ che commuta con il seguente diagramma (cioè $g \circ h = f$):*



se e solo se $f(B) \subseteq g(C)$. Inoltre se g è iniettiva allora h è unica.

Svolgimento. Se $g \circ h = f$ allora $g \circ h(B) = f(B)$ ma $g \circ h(B) = g(h(B)) \subseteq g(C)$ (osserviamo che $h(B) = C$ solo se h è surgettiva). Viceversa, se $f(B) \subseteq g(C)$, allora per ogni $b \in B$ $f(b)$è un elemento di $g(C)$. Dunque esiste almeno un $c \in C$ tale che $g(c) = f(b)$. Definiamo $h(b) = c$ e abbiamo che h commuta con il diagramma come richiesto, inoltre se g è iniettiva esiste esattamente un $c \in C$ tale che $g(c) = f(b)$ e perciò $h(b)$ è univocamente determinato per ogni $b \in B$, ovvero h è unica.

Esercizio 1.40. *Siano A, B, C insiemi non vuoti e $f : A \longrightarrow B$, $g : A \longrightarrow C$ allora esiste $h : C \longrightarrow B$ che commuta con il seguente diagramma (cioè $h \circ g = f$):*



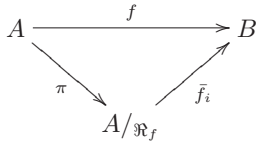
se e solo se per ogni $a_1, a_2 \in A$ $g(a_1) = g(a_2)$ implica $f(a_1) = f(a_2)$. Inoltre se g è surgettiva allora h è unica.

Svolgimento. Se $h \circ g = f$ e $g(a_1) = g(a_2)$ allora:

$$f(a_1) = (h \circ g)(a_1) = h(g(a_1)) = h(g(a_2)) = (h \circ g)(a_2) = f(a_2)$$

Viceversa, se per ogni $a_1, a_2 \in A$ da $g(a_1) = g(a_2)$ segue $f(a_1) = f(a_2)$, allora per ogni $c \in C$: se $c \in g(A)$, allora esiste $a \in A$ tale che $g(a) = c$, e definiamo $h(c) = f(a)$; se $c \in C \setminus g(A)$ possiamo definire $h(c)$ come vogliamo. Quella data è una buona definizione nel senso che non dipende dalla controimmagine di c tramite g scelta. Infatti se a_1, a_2 sono due controimmagini diverse di c tramite g abbiamo, per ipotesi, che $f(a_1) = f(a_2)$ e di conseguenza che $h(a_1) = h(a_2)$. h commuta con il diagramma per costruzione e se g è surgettiva h è univocamente determinata su tutto il dominio e quindi unica.

I risultati che emergono da questi esercizi ci permettono di fare il passaggio inverso rispetto alla Proposizione 1.38: in quel caso data una funzione f da A in B avevamo definito una relazione di equivalenza $\Re_f$, considerato l'insieme quoziente $A/_{\Re_f}$ e dimostrato che esiste una funzione $\bar{f}_i$ che commuta con il diagramma:

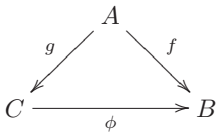


Ora, data una relazione di equivalenza $\Re$ su A, vogliamo trovare un insieme B e un'applicazione surgettiva f tali che $\Re = \Re_f$. Per questo basta considerare ad esempio $B = A/_{\Re}$ e f la proiezione canonica da A in B.

Esercizio 1.41. *Verificare che effettivamente con la scelta fatta $\Re = \Re_f$.*

Quello che in realtà vogliamo dimostrare attraverso l'Esercizio 1.40 è qualcosa di più forte, ovvero che se (C, g) sono una coppia con le stesse proprietà di (B, f) (cioè $g(A) = C$ e $\Re = \Re_g$) allora esiste un'unica funzione $\phi : C \longrightarrow B$ bigettiva che

commuta con il seguente diagramma:



Vista la surgettività di g e l'Esercizio 1.40, per provare esistenza e unicità di ϕ che commuta con il diagramma, basta provare (vista la surgettività di g) che per ogni $a_1, a_2 \in A$ $g(a_1) = g(a_2)$ implica $f(a_1) = f(a_2)$. Questo segue dalle ipotesi, infatti:

$$g(a_1) = g(a_2) \Leftrightarrow a_1 \Re_g a_2 \Leftrightarrow a_1 \Re a_2 \Leftrightarrow a_1 \Re_f a_2 \Leftrightarrow f(a_1) = f(a_2)$$

Osserviamo che potevamo aspettarci la catena di doppie implicazioni visto il ruolo totalmente simmetrico della coppia (B, f) rispetto alla coppia di (C, g). Ci rimane da provare che ϕ è surgettiva, ma questo segue dal fatto che ϕ commuta con il diagramma (ovvero $\phi \circ g = f$) e che f è surgettiva. Abbiamo quindi dimostrato che la coppia (B, f) è un modello dell'insieme quoziente $A/_{\Re}$, unico a meno di bigezioni.

Introduciamo adesso una *particolare* tipo di funzioni:

Definizione 1.42. Sia A un insieme, un'**operazione** n**-aria**, o di arietà n, su A è una funzione $* : \underbrace{A \times \cdots \times A}_{n \text{ Volte}} \longrightarrow A$. Nel caso di operazioni binarie (ovvero funzioni da $A \times A$ in A) diremo semplicemente *operazione* su A.

Definizione 1.43. Sia $*$ operazione su A, dati $a, b \in A$ si dice che a **divide** b (o che a è un **divisore** di b) se esiste $c \in A$ tale che $b = a * c$. Se a divide b si dice anche che b è un **multiplo** di a. Scriveremo che $a \mid b$.

Definizione 1.44. Data un'operazione $*$ su A, la relazione $\Re$ definita da $a \Re b$ se e solo se $a \mid b$, si dice **relazione di divisibilità** su A, rispetto a $*$.

Esercizio 1.45. *Consideriamo* $(\mathbb{N}, +)$. *Quali coppie* (m, n) *in* $\mathbb{N} \times \mathbb{N}$ *appartengono alla relazione di divisibilità* $\mid$ *introdotta nella Definizione 1.44?*

Esercizio 1.46. *Consideriamo un insieme* A *su cui è definita una operazione* $*$. *Dati* $a, b, c \in A$ *sapendo che* $a \mid b$ *e* $b \mid c$ *si può concludere che* $a \mid c$*? In altre parole: la relazione di divisibilità è sempre transitiva?*

Svolgimento. Le ipotesi che abbiamo ci dicono che esistono $h, k \in A$ tali che $b = a * h$ e $c = b * k$. Da queste due uguaglianze si ottiene che $c = (a * h) * k$.

Se $*$ è associativa abbiamo che $c = a * (h * k)$, ed essendo $*$ una operazione in A, $h * k$ è un elemento di A (indichiamolo con t). Perciò $c = a * t$ ovvero $a \mid c$. Possiamo quindi concludere che, se l'operazione $*$ è associativa, la relazione di divisibilità è transitiva.

Se $*$ non è associativa non possiamo scrivere che $(a * h) * k = a * (h * k)$, quindi non si può procedere come sopra. In generale, se $*$ non è associativa, non vale la proprietà *transitiva* della divisibilità: un esempio di questo è l'operazione di esponenziazione $(a * b = a^b)$.

Definizione 1.47. Siano A un insieme e $\Re$, $*$ rispettivamente una relazione e un'operazione[2] su A. Si dice che $\Re$ è **compatibile** con $*$ se $\forall a, b, c, d \in A$ da $a \Re b$ e $c \Re d$ segue che $(a * c) \Re (b * d)$.

[2]Questa definizione può essere generalizzata alla compatibilità di relazioni n-arie, rispetto ad operazioni n-arie.

CAPITOLO 2

L'insieme $\mathbb{N}$ dei numeri naturali

1. Introduzione

I numeri naturali sono stati creati per un'esigenza primaria, quella di contare oggetti. Il numero naturale è particolarmente importante perché è il primo (sia nella storia della matematica che nella storia di ogni persona) approccio con il concetto primitivo di numero. Infatti fin da piccoli abbiamo imparato ad usare i numeri cosiddetti **naturali** $(0, 1, 2, 3, \ldots)$ per contare oggetti e in generale la numerosità di insiemi di oggetti.

Uno dei grandi contributi attribuito alla scuola greca è l'aver evidenziato il fatto che i numeri sono idee che vivono nella mente e che sono nettamente distinte dagli oggetti o dalle rappresentazioni fisiche. Dedekind $(1831 - 1916)$ affermava: "I numeri sono creazioni dell'intelletto umano, essi servono a cogliere più facilmente e profondamente la diversità delle cose".

Oggi sembra banale pensare che il numero 8 sia un'astrazione di tutti gli insiemi contenenti 8 oggetti, indipendentemente dalle caratteristiche degli oggetti ma a dimostrazione che questo sia stato un passaggio tutt'altro che *naturale* ci sono gli studi sui linguaggi primitivi che rivelano come il numero avesse una valenza concreta: per contare oggetti di tipo diverso venivano usati nomi di numeri diversi. Questa complessità è intuibile anche se ci soffermiamo sul significato matematico di questa astrazione del numero: considerare il numero 8 come rappresentante di tutti gli insiemi di 8 oggetti significa considerare una relazione di equivalenza (che poi corrisponde a quella che viene chiamata cardinalità degli insiemi finiti).

D'altra parte anche la formalizzazione dell'insieme dei numeri naturali è tutt'altro che semplice, ed è avvenuta in tempi *piuttosto recenti* (nella seconda metà dell'Ottocento), in seguito allo sviluppo dell'analisi infinitesimale (la sistematizzazione dei numeri naturali è strettamente connessa alla necessità di *ben fondare*, di *capire la reale natura* dei numeri reali. Questo, in particolare, mostra come l'evoluzione e la sistemazione di concetti matematici sia, nella storia della matematica, tutt'altro che lineare.

In questo capitolo ci soffermeremo su alcune proprietà strutturali dei numeri naturali, accennando solo brevemente all'introduzione formale di questo insieme numerico attraverso gli assiomi di Peano.

Proprio per cominciare ad osservare proprietà strutturali, molte delle definizioni che introdurremo saranno valide per un insieme generico A e poi *lette* in $\mathbb{N}$.

2. Definizione di $\mathbb{N}$ e proprietà delle operazioni

L'assiomatizzazione dei numeri naturali viene proposta usando alcuni enti primitivi: il concetto di numero, di zero, di appartenenza ad un insieme e di funzione successore.

Peano (e similmente Dedekind) assume che esistano un insieme $\mathbb{N}$ che chiamiamo **insieme dei numeri naturali** (che contiene un elemento 0, chiamato zero), e una funzione successore $S : \mathbb{N} \to \mathbb{N}$, di $\mathbb{N}$ in sé, che soddisfi le seguenti proprietà:

(1) S è iniettiva,
(2) $0 \notin S(\mathbb{N})$,
(3) Se un sottoinsieme M di $\mathbb{N}$ contiene lo zero ed è chiuso rispetto a S (cioè $S(M) \subseteq M$) allora $M = \mathbb{N}$.

Osservazione 2.1. La sistematizzazione dei numeri naturali non si ferma con il supporre che esista un insieme che verifica le proprietà suddette. Quello che vogliamo è che tali proprietà caratterizzino in maniera esclusiva l'insieme dei numeri naturali, ovvero che, se esiste un insieme $\mathbb{N}'$ con un elemento $0'$ e una funzione successore S' su $\mathbb{N}'$ che soddisfa gli assiomi di Peano, allora $(\mathbb{N}, S, 0)$ e $(\mathbb{N}', S', 0')$ *sono la stessa cosa*. Dove *essere la stessa cosa* va inteso in senso matematico, cioè fondamentalmente che esista una funzione bigettiva $f : \mathbb{N} \to \mathbb{N}'$ con $f(0) = 0'$ e $S' \circ f = f \circ S$. Tale risultato è l'enunciato del cosidetto teorema di unicità, che sarà dimostrato da Dedekind nel 1888.

Definizione 2.2. La proprietà che l'unico sottoinsieme di $\mathbb{N}$ che contiene lo 0 ed è chiuso per S sia proprio $\mathbb{N}$ è nota come **principio d'induzione**.

Come vedremo nel prossimo paragrafo, il principio d'induzione fornisce un potente metodo dimostrativo per proposizioni su $\mathbb{N}$. Ma il principio di induzione può essere usato anche per definire successioni e operazioni su $\mathbb{N}$, con il metodo detto *per ricorrenza*. Ovvero: nel caso delle successioni si definisce il valore del primo termine a_0, e si fornisce la regola per passare dal valore dell'n-esimo termine a_n, a quello dell'$n+1$-esimo a_{n+1}, nel caso delle operazioni binarie $*$, fissato $m \in \mathbb{N}$, si definisce il valore di $m*0$, e si fornisce la regola per calcolarsi $m*(n+1)$ conoscendo il valore di $m * n$.

È facile mostrare che dal Principio d'Induzione segue che, procedendo come descritto, abbiamo definito la successione (o l'operazione con m) per tutti i numeri naturali. Infatti, sia I l'insieme degli indici i per cui abbiamo definito la successione. $0 \in I$ perché abbiamo dato a_0, inoltre se conosciamo il valore a_n allora la regola data ci permette di calcolare a_{n+1}, cioè se $n \in I$ allora $n + 1 \in I$. Dunque $I = \mathbb{N}$.

Esempio 2.3. Vediamo la definizione per ricorrenza di una successione piuttosto nota in matematica, e che useremo spesso nella parte di calcolo combinatorio. Consideriamo la successione a_n definita da:

$$\begin{cases} a_0 = 1 \\ a_{n+1} = a_n \cdot (n+1) \end{cases}$$

La successione così definita si chiama **fattoriale**, e, in luogo di a_n, solitamente si usa la notazione $n!$.

Esercizio 2.4. *Dimostrare che* $n! = \prod_{i=1}^{n} i$.

Osservazione 2.5. Sulla base di quanto detto possiamo definire, usando il principio di induzione, le due operazioni addizione e moltiplicazione su $\mathbb{N}$:
Fissato $m \in \mathbb{N}$ definiamo l'addizione di m con qualsiasi naturale in questo modo:

$$\begin{cases} m + 0 = m \\ m + S(n) = S(m + n) \end{cases}$$

Fissato $m \in \mathbb{N}$, e avendo già definito la somma tra m e un qualsiasi naturale, definiamo il moltiplicazione di m con un naturale qualsiasi come segue:

$$\begin{cases} m \cdot 0 = 0 \\ m \cdot S(n) = m \cdot n + m \end{cases}$$

Osserviamo che, nella definizione di addizione con m, abbiamo assunto, per definizione, l'esistenza dell'elemento neutro 0. Per la moltiplicazione per m, invece l'esistenza di tale elemento neutro, che corrisponderà al successore di 0 comunemente indicato con 1, si deve dimostrare (segue dalla definizione di moltiplicazione).

Si può dimostrare, attraverso gli assiomi di Peano, che:

Teorema 2.6. *Addizione e moltiplicazione di $\mathbb{N}$ verificano, per ogni a, b, c in $\mathbb{N}$, le proprietà riassunte nella seguente tabella :*

Proprietà	*Addizione*	*Moltiplicazione*
Associativa	$(a+b)+c = a+(b+c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Commutativa	$a+b = b+a$	$a \cdot b = b \cdot a$
Esistenza el. neutro	$0+a = a+0 = a$	$1 \cdot a = a \cdot 1 = a$

Vale inoltre la proprietà distributiva della moltiplicazione rispetto all'addizione, ovvero $\forall\ a, b, c \in \mathbb{N}$ si ha che $a \cdot (b+c) = a \cdot b + a \cdot c$.

Un primo risultato che si può dimostrare da queste proprietà è l'unicità dell'elemento neutro:

Proposizione 2.7. *Gli elementi neutri di addizione e moltiplicazione in $\mathbb{N}$ sono unici.*

Dimostrazione. Supponiamo che $t \in \mathbb{N}$ sia un elemento neutro per l'addizione: vogliamo dimostrare che necessariamente deve essere $t = 0$. Considerando la somma $t + 0$, abbiamo che:

$$t + 0 = \begin{cases} \text{t in quanto 0 é elemento neutro} \\ \text{0 in quanto t é elemento neutro} \end{cases}$$

Perciò $t = 0$ necessariamente. Analogamente si procede per dimostrare che e' è unico.

Osserviamo che la dimostrazione è replicabile per qualsiasi insieme A su cui sia stata definita un'operazione con le proprietà precedenti. □

Dato un insieme A con un'operazione commutativa $*$ e con l'elemento neutro per quella operazione (che indichiamo con e), introduciamo il concetto di inverso di un elemento:

Definizione 2.8. Dato $a \in A$, se esiste un elemento $b \in A$ tale che $a * b = e$, si dice che b è **l'inverso** di a.

Osservazione 2.9. Osserviamo che in $\mathbb{N}$, sia per l'addizione che per la moltiplicazione, l'elemento inverso esiste solo per i rispettivi elementi neutri.

Osservazione 2.10. Dati A insieme e $*$ operazione su A, la relazione $\Re$ definita da $a \Re b$ se a è l'inverso di b rispetto a $*$, è simmetrica.

L'esistenza degli inversi per ogni elemento permetterebbe di definire (e dunque poter eseguire) sottrazione e divisione a partire da addizione e moltiplicazione. Infatti, dati $a, b \in \mathbb{N}$, supponiamo di cercare il numero x uguale a $b - a$. Per le proprietà dell'uguaglianza questo è equivalente a trovare x tale che $x + a = b$. Se avessimo l'inverso di ogni elemento rispetto all'addizione, in particolare lo avremmo per a (e lo potremmo indicare con $-a$). In questo caso, aggiungendolo ad entrambe i membri dell'uguaglianza precedente, otterremmo $x+a+(-a) = b+(-a)$. Avremmo dunque x come risultato di una addizione, quella di b con l'opposto di a. La stessa cosa si potrebbe fare tra moltiplicazione e divisione.

Introduciamo adesso la relazione binaria su $\mathbb{N}$ di maggiore o uguale:

Definizione 2.11. Si dice che a è maggiore o uguale di b (e scriveremo $a \geq b$ invece di $a\Re b$), se esiste $c \in \mathbb{N}$ tale che $a = b + c$.

Esercizio 2.12. *Dimostrare che la relazione $\geq$ definisce un ordine totale su $\mathbb{N}$.*

Osservazione 2.13. A questo punto dovrebbe essere chiaro come definire la maggiorazione stretta $>$ su $\mathbb{N}$: $a > b$ se esiste c in $\mathbb{N}$, $c \neq 0$ tale che $a = b + c$.

Osserviamo che la relazione di maggiorazione stretta non è una relazione d'ordine perché, pur essendo simmetrica (in quanto la condizione $a > b$ e $b > a$ non si verifica mai) e transitiva, non è riflessiva.

Esercizio 2.14. *Dimostrare che addizione e moltiplicazione su $\mathbb{N}$ sono compatibili con $\geq$, ovvero che:*

(1) $\forall a, b, c \in \mathbb{N} : \ a \geq b \Rightarrow a + c \geq b + c.$
(2) $\forall a, b, c \in \mathbb{N} : \ a \geq b \Rightarrow a \cdot c \geq b \cdot c.$

Si potrebbe notare che nell'esercizio precedente, abbiamo provato qualcosa di apparentemente diverso da quanto richiesto nella Definizione 1.47 di operazioni compatibili con una relazione di equivalenza su di un insieme. Provare per esercizio che:

Esercizio 2.15. *Dimostrare che la definizione di compatibilità tra una operazione $*$, e una relazione $\Re$ su un insieme A, data in 1.47, se $\Re$ è transitiva è equivalente a richiedere che:*

$$\forall x, y, z \in \mathcal{A} : \ x\Re y \Rightarrow (x * z)\Re(y * z)$$

Osservazione 2.16. Introdotto l'ordinamento $\geq$ possiamo definire, dati a, b in $\mathbb{N}$ con $a \geq b$, il naturale $a - b$ come quel c tale che $b + c = a$. Non abbiamo definito una operazione in $\mathbb{N}$ in quanto non abbiamo un valore per ogni coppia di naturali (in particolare, $-$ è definito per la coppia (a, b) di $\mathbb{N} \times \mathbb{N}$ se e solo se non lo è per la coppia (b, a)).

Esercizio 2.17. *Dimostrare che la relazione di divisibilità rispetto all'operazione di moltiplicazione di $\mathbb{N}$ (vedi Definizione 1.44), è una relazione di ordine. Mostrare inoltre che, a differenza della relazione di ordine $\geq$ precedentemente introdotta, la relazione di divisibilità non è totale.*

3. Forme equivalenti del principio d'induzione

In questo paragrafo mostreremo altre forme equivalenti del principio d'induzione. Intendiamo cioè proprietà che, da una parte possono essere dimostrate a partire dalla definizione assiomatica dei numeri naturali data, e dall'altra se sostituite al

posto del principio d'induzione nell'assiomatica di $\mathbb{N}$, permettono di dimostrare il principio d'induzione stesso. In poche parole, avremmo potuto scegliere di mettere una di queste proprietà al posto del principio d'induzione nella definizione assiomatica di $\mathbb{N}$ e avremmo caratterizzato lo stesso insieme. L'interesse per le forme equivalenti del principio di induzione non è solo quello di mostrare come l'assiomatizzazione dello stesso insieme (che abbiamo indicato con $\mathbb{N}$) possa essere fatta in maniera differente, ma è legata anche ad un interesse *pratico*. Nell'uso del principio d'induzione come metodo dimostrativo, a seconda del tipo di enunciato da provare, l'uso di una forma equivalente del principio d'induzione in luogo di un'altra può semplificare molto le cose. Il teorema finale di questo paragrafo, che dimostra appunto l'equivalenza delle varie forme, ci permetterà di usarle indifferentemente.

La prima delle forme equivalenti al principio di induzione che analizziamo è la cosiddetta **induzione forte**. Questo nome, con cui solitamente viene indicato il principio che riporteremo, è in qualche modo *fuorviante* in quanto, come detto, in realtà il principio di induzione e questo principio di induzione forte sono equivalenti[1]. Fatto sta che ci sono casi in cui è immediato provare il passo induttivo dell'induzione forte, mentre è meno facile provare il passo induttivo usando l'induzione introdotta nel paragrafo precedente.

Principio di induzione forte: Se S è un sottoinsieme di $\mathbb{N}$ tale che:

- $0 \in S$.
- Per ogni $k \in \mathbb{N}$, se $0, \dots, k$ appartengono a S allora anche $k+1$ appartiene a S.

Allora $S = \mathbb{N}$.

La differenza rispetto al principio d'induzione sta nel fatto che, nel passo induttivo, per dimostrare che $k+1$ appartiene a S, possiamo usare che tutti i numeri minori di $k+1$ appartengono a S e non solo k. Questo, come vedremo, sarà fondamentale per dimostrare che ogni numero intero è primo o si può scrivere come prodotto di primi. Ma lo è anche per definire successioni per ricorrenza il cui valore del termine n-esimo non dipenda solo dal valore precedente (a_{n-1}), ma da più termini precedenti.

Esempio 2.18. Consideriamo il seguente problema: supponiamo di sapere che ogni coppia di batteri genera ogni minuto una coppia di batteri, la quale a sua volta comincia a generare coppie di batteri a partire dal secondo minuto di vita. Ci chiediamo: quante coppie di batteri ci saranno (se non sono presenti azioni che distruggono i batteri) dopo n minuti partendo al tempo $t = 0$ con una singola coppia di batteri?

L'idea è che se indichiamo con F_t il numero di batteri al minuto t si ha che:

- $F_0 = 1$ (per ipotesi l'unica coppia presente al minuto 0 è quella iniziale).
- $F_1 = 1$ (i batteri cominciano a generare dopo 2 minuti).
- $F_2 = 1 + 1 = 2$ (la coppia iniziale più quella generata).
- $F_3 = 2 + 1 = 3$ (le 2 coppie presenti al minuto precedente più la coppia generata dalla prima coppia di batteri. La seconda coppia, essendo al primo minuto di vita, non genera ancora).
- $F_4 = 3 + 2$ (le 3 coppie che si avevano al terzo minuto più le due coppie generate dalle due coppie che hanno più di un minuto di vita).

[1]Per questo su alcuni testi i due principi sono invece chiamati rispettivamente prima forma e seconda forma del principio d'induzione.

Da questi primi conti si può intuire come F_n sia la somma di F_{n-1} (le coppie di batteri presenti al minuto precedente continuano ad esserci) più F_{n-2} (le coppie generate dalle coppie di batteri che hanno più di un minuto di vita, che sono per l'appunto F_{n-2}).

Abbiamo dunque che la successione definita per ricorrenza da:

$$\begin{cases} F_0 = 1 \quad F_1 = 1 \\ \text{Per ogni } n \geq 2,\ F_n = F_{n-1} + F_{n-2} \end{cases}$$

risolve, per qualsiasi minuto n, il problema di calcolare il numero di batteri.
La successione appena definita, molto nota in matematica, prende il nome di **successione di Fibonacci**, e i suoi termini sono chiamati **numeri di Fibonacci**.

Teorema 2.19. *La prima e la seconda forma del principio d'induzione sono equivalenti.*

Esercizio 2.20. *Dimostrare il teorema 2.19.*

Un altro principio, che mostreremo essere equivalente al principio d'induzione all'interno dell'assiomatica di Peano (ovvero lasciando inalterate le altre proprietà caratterizzanti $\mathbb{N}$ nell'assiomatica di Peano, e considerando uno dei due principi, si può dimostrare l'altro), è il cosiddetto **Principio del buon ordinamento** o **principio del minimo**: ogni sottoinsieme S non vuoto di $\mathbb{N}$ possiede minimo. Ovvero esiste $m \in S$ tale che $\forall x \in S$ si ha $x \geq m$.

Teorema 2.21. *Il principio del buon ordinamento e il principio d'induzione sono equivalenti all'interno dell'assiomatica di Peano.*

Dimostrazione. $\Rightarrow$)Supponiamo di aver assunto l'assioma del buon ordinamento sui naturali, e consideriamo S un sottoinsieme di $\mathbb{N}$ tale che $0 \in S$ e se $n \in S$ allora $n + 1 \in S$. Vogliamo dimostrare che $S = \mathbb{N}$, questo equivale, indicando con T il complementare di S in $\mathbb{N}$, a dimostrare che $T = \emptyset$.

Per assurdo supponiamo che la tesi sia falsa, cioè $T \neq \emptyset$. Dal principio del buon ordinamento segue che T ha un elemento minimo m. Sicuramente $m \neq 0$, perché $0 \in S$ e, per definizione di complementare, $S \cap T = \emptyset$. Dunque $m > 0$ ed esiste[2] $m - 1$ in $\mathbb{N}$. $m - 1$ non appartiene a T (in quanto m è il minimo di T), e quindi $m - 1$ appartiene ad S (sempre per definizione di complementare). Ma per ipotesi sappiamo che, se un elemento n appartiene a S allora anche $n + 1$ appartiene a S, quindi anche $(m - 1) + 1 = m \in S$. Questo è assurdo, perché come giá osservato, per definizione di complementare, non esistono elementi in comune tra S e T.

Si conclude quindi che T è vuoto perché se così non fosse, avremmo comunque un assurdo.

$\Leftarrow$) Supponiamo che valga il principio di induzione, e consideriamo un sottoinsieme S di $\mathbb{N}$ non vuoto. Supponiamo per assurdo che S non abbia minimo. Consideriamo la proposizione $P(n)$ relativa al numero n: *nessun naturale minore o uguale di n appartiene ad S* e il seguente sottoinsieme di $\mathbb{N}$:

$$T = \{n \in \mathbb{N} | P(n) \text{ è vera}\}$$

Osserviamo che $0 \in T$ in quanto, se $P(0)$ fosse falsa, vorrebbe dire che $0 \in S$ e dunque sarebbe un minimo di S. Inoltre, se $n \in T$, necessariamente $n + 1$ appartiene a T. Infatti, così non fosse, avremmo:

[2]Questa proprietà, che ogni $m > 0$ abbia un predecessore in $\mathbb{N}$, segue dagli assiomi di Peano.

- $P(n)$ è vera, cioè nessun numero minore o uguale a n sta in S.
- $P(n+1)$ è falsa, quindi esiste un numero minore o uguale di $n+1$ che sta in S.

Ovvero $n+1$ appartiene ad S ed è un minimo di S, contro l'ipotesi che S non abbia minimo.

Abbiamo cioè dimostrato che T rispetta le ipotesi del principio di induzione, ovvero $T = \mathbb{N}$, ma questo è equivalente a $S = \emptyset$. □

Diamo un'ulteriore forma equivalente al principio di induzione, spesso utilizzata.
Principio della catena discendente: Non esistono successioni strettamente decrescenti infinite di numeri naturali.

Esercizio 2.22. *Dimostrare che il principio della catena discendente e il principio del minimo sono equivalenti (da cui segue per* transitività *della doppia implicazione, che il principio della catena discendente è equivalente alle due forme dell'induzione).*

4. Il principio di induzione come metodo dimostrativo

Abbiamo introdotto nel paragrafo precedente alcune forme equivalenti al principio d'induzione, con la motivazione che potranno essere utili come tecniche dimostrative. Mostriamo dunque finalmente come, dal principio d'induzione, segua una tecnica dimostrativa molto usata in matematica per provare proposizioni su $\mathbb{N}$. Le dimostrazioni che usano tale tecnica verranno chiamate **dimostrazioni per induzione**.

Anche per quanto riguarda il metodo dimostrativo per induzione, come per molte altre *conquiste* del pensiero matematico, non è possibile stabilire una data di *scoperta*: non è l'invenzione di un particolare individuo in una data fissata, ma piuttosto un metodo implicito nel lavoro di molti matematici, che emerge lentamente e altrettanto lentamente viene formalizzato. Per dimostrare che i numeri primi sono infiniti, Euclide, nella proposizione 20, libro IX degli Elementi, afferma che *i numeri primi sono più di ogni assegnata moltitudine di numeri primi.* Euclide in realtà prova *solo* che dati tre primi A, B, C ne esiste un quarto D diverso dai precedenti, ma il metodo dimostrativo che usa (e che vedremo in seguito) è di carattere generale, e può essere usato per provare l'esistenza di $n+1$ primi partendo dall'ipotesi che ne esistano n. La prima formulazione dell'induzione formalmente soddisfacente viene attribuita a Pascal, il quale, nel 1654, la usa per provare alcuni risultati sul triangolo che porta il suo nome; tuttavia alcune indicazioni importanti possono essere riconosciute nei lavori di Maurolico $(1494 - 1575)$ e Fermat $(1601 - 1665)$. In "Scienza e ipotesi" del 1952, Henry Poincarè descrive il metodo dimostrativo per induzione come il ragionamento matematico per eccellenza. Al di là di questa considerazione personale di un eminente matematico, è evidente il ruolo e la rilevanza della dimostrazione per induzione in matematica.

Proposizione 2.23 (Metodo d'induzione)**.** *Sia $P(n)$ una proposizione che abbia senso per ogni n in $\mathbb{N}$. Se valgono le due seguenti condizioni:*

(1) *$P(0)$ è vera,*
(2) *Per ogni n ($P(n)$ vera implica $P(n+1)$ vera),*

allora la proposizione $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Dimostrazione. Consideriamo l'insieme A così definito:

$$A = \{n \in \mathbb{N} \mid P(n) \text{ é vera}\}$$

Cioè A è l'insieme dei numeri naturali per cui P è vera. A contiene lo 0, inoltre è chiuso per successore in quanto per ipotesi, se P è vera per n (cioè $n \in A$) allora P è vera per $n+1$ (cioè $n+1 \in A$). □

Osservazione 2.24. Il principio di induzione si può generalizzare per mostrare che una proposizione P è vera da un certo n_0 in poi. Se valgono le due seguenti condizioni:

(1) $P(n_0)$ è vera,
(2) Per ogni $n \geq n_0$ ($P(n)$ vera implica $P(n+1)$ vera),

allora la proposizione $P(n)$ è vera per ogni $n \geq n_0$.

In particolare, dal principio di induzione, segue che, se $m \in S$ e, per ogni $n \geq m$, $n \in S$ implica $n+1 \in S$, allora S contiene l'insieme dei numeri naturali maggiori o uguali di m. Questo ci permette di definire successioni per ricorrenza a partire da a_m con m diverso da 0.

Quando ci troveremo a dimostrare una proposizione $P(n)$ che dipende da $n \in \mathbb{N}$, la verifica che $P(n_0)$ sia vera è chiamata **passo base** della dimostrazione per induzione. La dimostrazione che per ogni $n \geq n_0$ da $P(n)$ vero segua $P(n+1)$ vero si chiama **passo induttivo**. Nel passo induttivo l'ipotesi che $P(n)$ sia vero si chiama **ipotesi induttiva**.

Esercizio 2.25. *Dimostrare per induzione che la successione:*

$$\{a_n\} = \begin{cases} a_0 = 1 \\ a_{n+1} = 7 \cdot a_n \end{cases}$$

può essere definita in maniera non ricorsiva (cioè per calcolare il valore di a_n non dobbiamo conoscere valori precedenti della successione ma abbiamo a_n espressa in termini di funzione di n) attraverso la formula $a_n = 7^n$.

Esempio 2.26 (La torre di Hanoi)**.** Consideriamo l'antico gioco chiamato "torre di Hanoi" consistente in tre pioli verticali: in uno dei quali sono posti alcuni dischi di diametro decrescente (ovvero il disco più grande di diametro è sul fondo e quello più piccolo in cima), mentre gli altri pioli sono senza dischi. Una mossa del gioco consiste nello spostare un disco da uno dei tre pioli ad un altro qualsiasi degli altri due, la regola da rispettare è che nessun disco può essere messo sopra un disco di diametro inferiore.

Esercizio 2.27. *Al variare del numero di dischi n, quante mosse servono per (ovvero* quale è il numero minimo di mosse necessario per*) spostare l'intera torre di dischi da un piolo (che chiamiamo primo) ad un altro piolo (che chiamiamo terzo), rispettando la regola?*

Svolgimento. Cominciamo a vedere cosa accade con n (numero di pioli) piccolo:
Se $n = 1$ basta una mossa per spostare l'unico disco da un piolo all'altro.
Se $n = 2$ spostiamo il disco più piccolo nel secondo piolo, mettiamo il disco più grande nel terzo piolo, e infine spostiamo il disco piccolo dal secondo piolo al terzo. Abbiamo spostato la torre in 3 mosse.
Se $n = 3$ per spostare, rispettando le regole, i due dischi più piccoli sul secondo piolo abbiamo bisogno di 3 mosse (vedi passo precedente). A questo punto spostiamo

il disco più grande sul terzo piolo, e poi dobbiamo spostare nuovamente una torre alta due dischi da un piolo (il secondo) ad un altro (il terzo), e quindi necessitiamo di altre 3 mosse.

Analizziamo la procedura usata per spostare i 3 dischi: spostiamo 2 dischi sul secondo piolo, poi il disco più grande sul terzo, e infine 2 dischi dal secondo al terzo. Tale procedura può essere generalizzata per un numero qualsiasi di dischi: indichiamo con $M(n)$ il numero di mosse per spostare n dischi da un piolo ad un altro, e calcoliamo $M(n+1)$ (ovvero il numero per spostare $n+1$ dischi dal primo al terzo piolo). La strategia è quella di spostare n dischi dal primo al secondo piolo (mosse necessarie $M(n)$), spostare il disco più grosso rimasto nel primo piolo, dal primo al terzo piolo (1 mossa necessaria), e infine spostare gli n dischi del secondo piolo sul terzo piolo (mosse necessarie $M(n)$). Dunque:

$$M(n+1) = 2 \cdot M(n) + 1$$

Esercizio 2.28. *Dimostrare per induzione che la formula diretta per calcolare il numero di mosse $M(n)$ necessarie per spostare una torre di Hanoi alta n dischi dal primo al terzo piolo seguendo la regola è $M(n) = 2^n - 1$.*

In altre parole, si tratta di mostrare che $M(n) = 2^n - 1$ è la forma esplicita della successione definita per ricorrenza da:

$$M(n) = \begin{cases} M(1) = 1 \\ M(n+1) = 2 \cdot M(n) + 1 \end{cases}$$

Esercizio 2.29. *Dimostrare che per ogni $n > 1$ la somma dei primi n numeri dispari è uguale a n al quadrato.*

Svolgimento. Procediamo per induzione sul numero n di dispari da sommare.
Passo base. Se $n = 2$ dobbiamo verificare che la somma dei primi due dispari (1 e 3) sia uguale a 2 al quadrato. Effettivamente è vero che $1 + 3 = 2^2$.
Passo induttivo. Supponiamo che la somma dei primi n dispari sia n^2, da questo dobbiamo dedurre che la somma dei primi $n+1$ dispari è $(n+1)^2$, e questa deduzione non deve dipendere da proprietà di un particolare n (perché l'implicazione deve valere per ogni n) ma solo dall'ipotesi induttiva.
La somma dei primi $n+1$ numeri dispari sarà uguale alla somma dei primi n numeri dispari più l'$n+1$-esimo numero dispari, ovvero introducendo il simbolo di sommatoria:

$$\sum_{i=1}^{n+1} \underbrace{(2 \cdot i - 1)}_{i-esimo\ numero\ dispari} = \underbrace{(2(n+1) - 1)}_{n+1-esimo\ numero\ dispari} + \sum_{i=1}^{n} (2 \cdot i - 1)$$

A questo punto:

$$(2(n+1) - 1) + \sum_{i=1}^{n} (2 \cdot i - 1) \underbrace{=}_{ip.induttiva} 2n + 1 + n^2 = (n+1)^2$$

Esercizio 2.30. *Dimostrare che dati $x, y \in \mathbb{R}$ tali che $x \geq 0$ e $x + y \geq 0$ si ha:*

$$\forall n \in \mathbb{N},\ n > 0 :\ (x+y)^n \geq x^n + nx^{n-1}y.$$

Svolgimento. Per provare che la disuguaglianza è vera per ogni $n \in \mathbb{N}$ procediamo per induzione su n.
Passo base. Per $n = 1$, la proposizione equivale a $x + y \geq x + y$, che è vera.

Passo induttivo. Supponiamo la disuguaglianza vera per tutti i $k \leq n$, e dimostriamola per $n+1$:

$$(x+y)^{n+1} = (x+y)^n(x+y) \underbrace{\geq}_{ip.ind.} (x^n + nx^{n-1}y)(x+y)$$

Da cui:

$$(x+y)^{n+1} \geq x^{n+1} + (n+1)x^n y + nx^{n-1}y^2 \geq x^{n+1} + (n+1)x^n y$$

Esercizio 2.31. *Dati n numeri reali $x_1, \ldots, x_n$ non negativi, chiamiamo*

$$a = (x_1 + \ldots + x_n)/n$$

e

$$b = \sqrt[n]{x_1 \cdot \ldots \cdot x_n}$$

rispettivamente **media aritmetica** *e* **media geometrica** *degli n elementi. Dimostrare che la media geometrica b è sempre minore o uguale della media aritmetica a e che l'uguaglianza si verifica solo nel caso che gli x_i siano tutti uguali.*

Svolgimento. Anche in questo caso procediamo per induzione sul numero degli elementi n di cui si fa media aritmetica e geometrica.
Passo base. Se $n = 2$ la tesi equivale a $2\sqrt{x_1 x_2} \leq x_1 + x_2$, cioè $4x_1x_2 \leq (x_1+x_2)^2$, che è vera in quanto equivale a $(x_1 - x_2)^2 \geq 0$.
Passo induttivo. Enumeriamo gli n numeri reali, e indichiamo con A_i, G_i rispettivamente la media aritmetica e geometrica dei primi i elementi. Per ipotesi induttiva $G_i \leq A_i \ \forall i < n$, vogliamo dimostrare che questo implica che $G_n \leq A_n$.

$$A_n = \frac{(x_1 + ... + x_{n-1}) + x_n}{n} = \frac{(n-1)A_{n-1} + x_n}{n} = A_{n-1} + \frac{x_n - A_{n-1}}{n}$$

$$A_n^n = (\underbrace{A_{n-1}}_{x} + \underbrace{\frac{x_n - A_{n-1}}{n}}_{y})^n \underbrace{\geq}_{ese\ 2.30} A_{n-1}^n + A_{n-1}^{n-1}(x_n - A_{n-1}) = A_{n-1}^{n-1} \cdot x_n$$

e su A_{n-1}^{n-1} possiamo usare l'ipotesi induttiva:

$$A_{n-1}^{n-1} \cdot x_n \underbrace{\geq}_{ip.ind.} G_{n-1}^{n-1} \cdot x_n = G_n^n$$

E lavorando su numeri naturali da $A_n^n \geq G_n^n$ si ottiene $A_n \geq G_n$.

Esercizio 2.32. *Sia a_n la successione definita per ricorrenza come segue:*

$$\begin{cases} a_0 = 4, \quad a_1 = 3 \\ a_{n+1} = \frac{a_n + a_{n-1}}{2} \end{cases}$$

Dimostrare che:

(1) $3 \leq a_n \leq 4$.
(2) *Se $n \geq 2$, allora a_n è un razionale con numeratore un numero naturale dispari e denominatore 2^{n-1}.*

Svolgimento. Il primo punto si dimostra rapidamente con l'induzione forte, osservando che la media aritmetica m tra due numeri a e b con $a \leq b$, è tale che $a \leq m \leq b$. Il passo base per $n = 0$ e $n = 1$ è verificato (conviene verificarlo su due elementi per *partire*, perché poi la successione è definita su due elementi, e passare da $P(1)$ a $P(2)$ tramite ipotesi induttiva potrebbe creare delle difficoltà). Se supponiamo che ogni a_n con n minore di un certo k sia compreso tra 3 e 4, allora

a_k (che è la media aritmetica tra i due valori a_{k-1} e a_{k-2}, compresi tra 3 e 4) è, per quanto osservato inizialmente sulla media aritmetica, compreso tra il maggiore dei due (supponiamo a_{k-1}) e il minore. Dunque si ha:

$$3 \leq a_{k-2} \leq a_k \leq a_{k-1} \leq 4$$

Dimostriamo il secondo punto per induzione. Il passo base è verificato, infatti per $n = 2$, a_2 ha numeratore 7 e denominatore $2^{2-1} = 2$, e per $n = 3$, a_3 ha numeratore 13 e denominatore $2^{3-1} = 4$.
Supponiamo ora che la tesi sia vera per ogni a_n con n minore di un certo k, e consideriamo a_k. Per ipotesi induttiva, esisteranno due numeri dispari r e s tali che:

$$a_{k-2} = \frac{r}{2^{(k-2)-1}} \quad a_{k-1} = \frac{s}{2^{(k-1)-1}}$$

Dunque:

$$a_k = \frac{a_{k-1} + a_{k-2}}{2} = \frac{\frac{r}{2^{k-3}} + \frac{s}{2^{k-2}}}{2} = \frac{\frac{2r+s}{2^{k-2}}}{2} = \frac{2r+s}{2^{k-1}}$$

Per concludere basta osservare che $2r + s$ è dispari, se, come ipotizzato, s è dispari.

Esercizio 2.33. *Consideriamo la successione di Fibonacci. Dimostrare che, per ogni $n \geq 1$ vale:*

(1) $\sum_{i=1}^{n} F_{2i-1} = F_{2n}$.
(2) $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

Svolgimento. Procediamo, per induzione, punto per punto.
(1) **Passo base.** Se $n = 1$, la uguaglianza si riduce ad una sommatoria con un solo elemento (F_1) uguale a F_2. E questo è vero perché $F_2 = F_1 + F_0 = 1 + 0 = 1$.
Passo induttivo. Supponiamo che $\sum_{i=1}^{n} F_{2i-1} = F_{2n}$, e consideriamo la sommatoria dei primi $n + 1$ numeri di Fibonacci con indice dispari. Vogliamo dimostrare che tale sommatoria è uguale a $F_{2(n+1)} = F_{2n+2}$:

$$\sum_{i=1}^{n+1} F_{2i-1} = \underbrace{\sum_{i=1}^{n} F_{2i-1}}_{=F_{2n}} + F_{2n+1} = F_{2n+2}$$

(2) **Passo base.** Se $n = 1$, la uguaglianza da provare equivale a:

$$\underbrace{F_2}_{=1} \cdot \underbrace{F_0}_{=0} - \underbrace{F_1^2}_{=1} = (-1)^1$$

Passo induttivo. Supponendo vera l'uguaglianza $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$, dobbiamo dimostrare che: $F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$. Sostituendo $F_{n+1} + F_n$ al posto di F_{n+2} si ha:

$$F_{n+1}F_n + F_n^2 - F_{n+1}^2 = F_{n+1}\underbrace{(F_n - F_{n+1})}_{=-F_{n-1}} + F_n^2$$

Da cui:

$$F_{n+2}F_n - F_{n+1}^2 = F_n^2 - F_{n+1}F_{n-1} \underbrace{=}_{ip.ind} -(-1)^n = (-1)^{n+1}$$

Esercizio 2.34. *Determinare per quali n in $\mathbb{N}$ si ha: $3^n > n^2 + 5n + 1$.*

Svolgimento. La successione 3^n cresce molto più rapidamente della successione n^2+5n+1, è quindi probabile che da un certo n in poi la maggiorazione sia sempre vera. Per dimostrarlo useremo l'induzione. Inizialmente si tratta di individuare quale potrebbe essere il numero naturale n tale che da quel valore in poi la maggiorazione è sempre vera. Cominciamo dunque con alcune prove numeriche:

- Se $n = 0$ abbiamo $1 > 1$ falso.
- Se $n = 1$ abbiamo $3 > 7$ falso.
- Se $n = 2$ abbiamo $9 > 10$ falso.
- Se $n = 3$ abbiamo $27 > 25$ vero.

Per quanto detto prima *sospettiamo* che valga il risultato che per ogni $n > 2$ vale $3^n > n^2 + 5n + 1$. Proviamo a dimostrarlo per induzione, sfruttando l'osservazione 2.24 che generalizza il principio d'induzione al caso di un insieme S uguale a tutti i numeri naturali maggiori di un certo n:

Passo base. In questo caso, volendo dimostrare che l'insieme S degli n che verificano la proprietà, è il sottoinsieme dei numeri naturali maggiori di 2, il passo base consiste nel verificare la proposizione per $n = 3$. Dunque lo abbiamo già verificato attraverso la precedente verifica.

Passo induttivo. Dobbiamo dimostrare che per ogni $n \in \mathbb{N}$ da (ipotesi induttiva) $3^n > n^2 + 5n + 1$ segue che:

$$3^{n+1} > \underbrace{(n+1)^2 + 5(n+1) + 1}_{=n^2+7n+7}$$

Ora 3^{n+1} per definizione è uguale a $3 \cdot 3^n$ e sapendo che $3^n > n^2 + 5n + 1$ si ha che:

$$3 \cdot 3^n = 3^{n+1} > 3 \cdot (n^2 + 5n + 1) = 3n^2 + 15n + 3$$

Abbiamo quindi dimostrato che $3^{n+1} > 3n^2 + 15n + 3$, e, per concludere, basta mostrare che per ogni $n > 2$ si ha $3n^2 + 15n + 3 > n^2 + 7n + 7$ (infatti dovendo in generale mostrare che $a > b$, sapendo che $a > c$, se mostriamo che $c > b$ abbiamo, per la transitività del $>$, che $a > b$). La disequazione da provare è equivalente a $n^2 + 4n - 2 > 0$, che è effettivamente vera per ogni $n > 0$, e quindi in particolare è vera per ogni $n > 2$.

Per il prossimo esercizio invece il suggerimento è di usare il principio di induzione forte.

Esercizio 2.35. *Dimostrare per induzione che, per ogni $n \in \mathbb{N}$, vale la seguente formula per i numeri di Fibonacci:*

$$F_n = \frac{1}{\sqrt{5}} \cdot (\frac{1+\sqrt{5}}{2})^{n+1} - \frac{1}{\sqrt{5}} \cdot (\frac{1-\sqrt{5}}{2})^{n+1}$$

Mostriamo adesso un esempio importante di applicazione del principio del minimo, dimostrando una parte di quello che sarà il teorema di divisione euclidea.

Teorema 2.36. *Dati due numeri naturali a, b con $b \neq 0$ esistono due naturali q, r tali che $a = b \cdot q + r$ e $r < b$. q e r vengono detti* **quoziente** *e* **resto** *della divisione euclidea di a con b.*

Dimostrazione. Consideriamo l'insieme:

$$S = \{a - b \cdot x | x \in \mathbb{N} \text{ e } a - b \cdot x \in \mathbb{N}\}$$

S non è vuoto in quanto a appartiene a S (basta prendere $x = 0$). Per il principio del minimo S ha un minimo $a - b \cdot q$ che chiamiamo r. Per terminare la dimostrazione

basta provare che r soddisfa la proprietà di essere minore di b. Supponiamo per assurdo $r \geq b$ allora $r - b \in \mathbb{N}$ e $r - b = a - b \cdot q - b = a - b \cdot (q + 1)$. Dunque avremmo $r - b \in S$ (perché è un naturale e abbiamo visto che è della forma $a - b \cdot x$, con $x = q - 1$); inoltre, essendo $b \neq 0$, $r - b < r$. Questo è assurdo perché r è il minimo di S. □

Teorema 2.37 (Archimedeità di $\mathbb{N}$)**.** $\mathbb{N}$ *è* **archimedeo**, *ovvero dati* $a, b \in \mathbb{N}$ *con* $a \geq b$ *esiste* $c \in \mathbb{N}$ *tale che* $b \cdot c > a$.

Dimostrazione. Consideriamo quoziente q e resto r della divisione euclidea di a per b. Dalla dimostrazione del teorema 2.36 sappiamo che $b \cdot (q + 1) > a$. □

Osservazione 2.38. Concludiamo il capitolo, mostrando come sia necessario verificare entrambe le condizioni presenti nell'enunciato del principio di induzione, per verificare la validità di una proprietà su tutto $\mathbb{N}$. Infatti non è difficile mostrare esempi di proposizioni $P(n)$ che soddisfano una sola delle due condizioni, e non sono vere per tutti i numeri naturali.

- Una qualsiasi condizione che sia falsa per ogni n soddisfa sempre il passo induttivo, ma mai il passo base. Per esempio, la proposizione $P(n)$: $n = n + 5$, non verifica il passo base ma verifica il passo induttivo.
- La proposizione $P(n)$: "n è un numero pari", verifica il passo base ma non il passo induttivo. In questo caso addirittura per ogni n, se è vera $P(n)$, allora è falsa $P(n + 1)$.
- La proposizione $P(n)$: "n è minore di 7" soddisfa il passo base, ma non per tutti gli n il passo induttivo. In particolare se $n = 6$ abbiamo che $P(6)$ vera non implica $P(7)$ vera.

È altrettanto vero che a volte individuare errori nelle dimostrazioni per induzione non è facile. Prova ne è il seguente esempio (usato in versioni differenti, ma sempre riconducibili al caso generale qui presentato), in cui la conclusione, palesemente falsa, fa intuire che qualcosa deve *non andare* nella dimostrazione.

Esempio 2.39. Consideriamo la proposizione $P(n)$ (definita per ogni $n > 0$): "ogni relazione di equivalenza $\Re$ su un insieme finito con n elementi è una relazione totale" (e quindi in particolare si potrebbe concludere che tutti i numeri sono uguali, oppure che in un insieme di n bambini tutti i bambini hanno gli occhi dello stesso colore). Proviamo a dimostrare questo risultato, evidentemente falso, usando il principio di induzione.

Passo base. $n = 1$. Se su un insieme con un solo elemento a mettiamo una relazione di equivalenza è immediato mostrare che tale relazione è totale, infatti l'unica coppia di elementi che possono essere in relazione è la coppia (a, a). Ma sappiamo che $a \Re a$ in quanto $\Re$ è simmetrica.

Passo induttivo. Supponiamo che (ipotesi induttiva) una relazione di equivalenza su un insieme di n elementi $\{a_1, \ldots, a_n\}$ sia totale, e consideriamo l'insieme di $n + 1$ elementi $\{a_1, \ldots, a_n,\ a_{n+1}\}$. Sappiamo per ipotesi induttiva che $\{a_1, \ldots, a_n\}$ e $\{a_2, \ldots, a_{n+1}\}$ sono in relazione tra loro (cioè sono nella stessa classe di equivalenza). Da questo segue, per la transitività di una relazione di equivalenza, che $\{a_1, \ldots, a_n, a_{n+1}\}$ sono nella stessa classe di equivalenza. Infatti da $a_1 \Re a_n$ e $a_n \Re a_{n+1}$ segue che $a_1 \Re a_{n+1}$.

Esercizio 2.40. *Trovare l'errore nella dimostrazione precedente (che la dimostrazione sia sbagliata si evince dall'assurdità dei risultati che ne conseguirebbero).*

CAPITOLO 3

Calcolo Combinatorio

1. Insiemi finiti

In questo capitolo introduciamo il tema del contare la numerosità, ovvero il numero di elementi, di insiemi finiti. Ma cosa si intende per insieme finito? Una risposta naif, ma non troppo, a questa domanda potrebbe essere: un insieme è finito se è possibile contare i suoi elementi. Contare gli elementi di un insieme finito A corrisponde ad enumerarli, ovvero a trovare una corrispondenza biunivoca tra gli elementi di A e l'insieme dei primi n numeri naturali positivi. Osserviamo infatti, che non si inizia mai a contare da zero: nel calcolo combinatorio lo zero è comunque essenziale per indicare il numero di elementi dell'insieme vuoto, che, per definizione, ha zero elementi. Da queste considerazioni informali, possiamo trarre una definizione formale di insieme finito:

Definizione 3.1. Dato un insieme A, si dice che A è **finito** se esistono $n \in \mathbb{N}$ e una funzione bigettiva f da A a $\mathbb{N}_n$ (l'insieme dei numeri naturali positivi minori o uguali di n). In questo caso si dice che A ha **cardinalità** n (e scriveremo $|A| = n$).

Per essere sicuri che la definizione data di cardinalità di un insieme sia una *buona definizione*, dobbiamo dimostrare che dato un insieme A, se questo è in corrispondenza biunivoca con $\mathbb{N}_n$, allora non è in corrispondenza biunivoca con nessun $\mathbb{N}_m$ con $m \neq n$ (cioè vogliamo essere sicuri che ad un insieme non possano essere associate due cardinalità diverse).

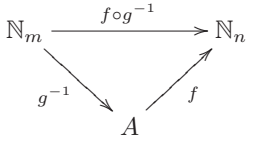
La dimostrazione di questo fatto si basa su un risultato intuitivo, la cui dimostrazione formale per induzione, che omettiamo, è piuttosto laboriosa:

Lemma 3.2 (Lemma dei cassetti o della piccionaia)**. Versione informale:** *se più di n piccioni stanno appollaiati su n piccionaie, allora qualche piccionaia deve contenere almeno due piccioni.*
Versione formale: *se $n > m$ allora non esistono funzioni iniettive da $\mathbb{N}_n$ a $\mathbb{N}_m$.*

Dal lemma dei cassetti segue appunto che:

Proposizione 3.3. *Se esiste una corrispondenza biunivoca f tra un insieme A e $\mathbb{N}_n$, allora non può esistere una corrispondenza biunivoca tra A e $\mathbb{N}_m$, con $m \neq n$.*

Dimostrazione. Sia $m \neq n$ e supponiamo per assurdo che esista una corrispondenza biunivoca g da A a $\mathbb{N}_m$. Allora l'inversa g^{-1} di g è una corrispondenza biunivoca da $\mathbb{N}_m$ in A, e abbiamo il seguente diagramma commutativo:



Questo è assurdo in quanto contraddice il lemma dei cassetti. Infatti $f \circ g^{-1}$, composizione di due funzioni bigettive, è una funzione bigettiva da $\mathbb{N}_m$ in $\mathbb{N}_n$ con $m \neq n$. □

Osservazione 3.4. In particolare due insiemi finiti X e Y hanno la stessa cardinalità se e solo se esiste una corrispondenza biunivoca tra X e Y.

Il principio dei cassetti può essere generalizzato per funzioni tra insiemi finiti come segue:

Teorema 3.5. *Siano X e Y insiemi finiti con cardinalità rispettivamente n e m e con $n > m$, allora non esistono funzioni iniettive da X a Y.*

Dimostrazione. Per ipotesi esistono due bigezioni f e g rispettivamente da X a $\mathbb{N}_n$ e da Y a $\mathbb{N}_m$. Supponiamo per assurdo esista una funzione iniettiva h da X a Y, allora avremmo il seguente diagramma commutativo:

$$\begin{array}{ccc} & h & \\ X & \longrightarrow & Y \\ f^{-1} \uparrow & & \uparrow g \\ \mathbb{N}_n & & \mathbb{N}_m \end{array}$$

La funzione $g \circ h \circ f^{-1}$ è una funzione iniettiva (in quanto composizione di funzione iniettive) da $\mathbb{N}_n$ a $\mathbb{N}_m$ e questo è in contraddizione con il Lemma 3.2. □

Dal Teorema 3.5 seguono due corollari importanti:

Corollario 3.6. *Se X è un insieme finito e $Y \subseteq X$, allora $|X| \geq |Y|$.*

Dimostrazione. $|Y|$ non può essere strettamente maggiore di $|X|$ altrimenti per il Teorema 3.5 non esisterebbero funzioni iniettive da Y in X, mentre l'identità i_Y è una mappa iniettiva da Y in X. □

Corollario 3.7. *Se dati X e Y finiti esistono una funzione f da X a Y iniettiva e una funzione g da Y a X iniettiva allora esiste una funzione h da X a Y bigettiva.*

Dimostrazione. Il fatto che esista una funzione iniettiva da X a Y ci dice, in seguito al Teorema 3.5, che $|X| \leq |Y|$. Analogamente l'esistenza di una funzione iniettiva da Y a X ci dice che $|Y| \leq X$, da cui segue che $|X| = |Y|$, ovvero che esiste una funzione bigettiva da X in Y. □

Abbiamo visto (Teorema 3.5) che non esistono funzioni iniettive da X a Y con X, Y insiemi finiti e $|X| > |Y|$. Viceversa si ha che:

Teorema 3.8. *Siano X e Y insiemi finiti con cardinalità rispettivamente n e m e con $n > m$, allora non esistono funzioni surgettive da Y a X.*

Dimostrazione. Supponiamo per assurdo che esista una funzione surgettiva f da Y a X, allora (vedi Esercizio 1.33) esiste un sottoinsieme Z di Y che è in corrispondenza biunivoca con X. Ma questo è assurdo perché avremmo che $|Y| \geq |Z| = |X|$ mentre per ipotesi sappiamo che $n > m$. □

Da questi risultati segue un teorema molto importante, che in qualche modo *caratterizza* gli insiemi finiti.

Teorema 3.9. *Se A è un sottoinsieme proprio di B finito, allora $|A| < |B|$.*

Dire che X e Y sono insiemi finiti di uguale cardinalità significa che esiste una funzione bigettiva da X a Y. Il seguente teorema ci dice che dati due insiemi con la stessa cardinalità, ogni funzione tra tali insiemi inettiva o surgettiva, è bigettiva.

Teorema 3.10. *Se X e Y sono insiemi finiti della stessa cardinalità, allora f da X a Y è iniettiva se e solo è surgettiva.*

DIMOSTRAZIONE. Supponiamo che f da X a Y sia iniettiva, allora c'è una corrispondenza biunivoca tra X e $f(X)$, dunque $|Y| = |X| = |f(X)|$. Da cui segue che f è surgettiva.

Viceversa, se g da X a Y è surgettiva allora $g(X) = Y$, dunque $|X| = |Y| = |g(X)|$, e quindi X e $g(X)$ sono in corrispondenza biunivoca, e perciò g è surgettiva. □

Concludiamo questo paragrafo introduttivo con un esempio importante:

Esempio 3.11. Supponiamo che A e B siano due insiemi finiti non vuoti di cardinalità rispettivamente m e n, vogliamo dimostrare che la cardinalità dell'insieme prodotto cartesiano $A \times B$ è $m \cdot n$. Per far questo dobbiamo trovare una corrispondenza biunivoca tra $\mathbb{N}_m \times \mathbb{N}_n$ e $\mathbb{N}_{m \cdot n}$. Dimostriamolo per induzione sul numero di elementi n di B:

Passo base. Se $n = 1$ dobbiamo mostrare che $|A \times B| = m \cdot 1 = m$. In questo caso B ha un solo elemento b e quindi $A \times B$ è in corrispondenza biunivoca con A: basta associare alla coppia (a, b) di $A \times B$ l'elemento a di A. Perciò la cardinalità di $A \times B$ è uguale alla cardinalità m di A.

Passo induttivo. Supponiamo di avere un insieme B di cardinalità $n + 1$: $B = \{b_1, b_2, \ldots, b_n, b_{n+1}\}$, dobbiamo dimostrare che $A \times B$ ha cardinalità $m \cdot (n + 1)$.

Indicato con B' l'insieme $B \setminus \{b_{n+1}\}$, sappiamo per ipotesi induttiva che $A \times B'$ ha cardinalità $m \cdot n$. Ovvero esiste una bigezione f da $A \times B'$ e $\mathbb{N}_{m \cdot n}$. Sappiamo anche che esiste una bigezione h tra $A \times b_{n+1}$ e $\mathbb{N}_m$; ed è facile (esercizio) costruire una bigezione g tra $\mathbb{N}_m$ e l'insieme dei numeri $\{m \cdot n + 1, \ldots, m \cdot n + m\}$. A questo punto possiamo costruire la bigezione t da $A \times B$ in $\mathbb{N}_{m \cdot (n+1)}$ come segue:

$$t(a, b) = \begin{cases} f(a, b) \text{ se } b \neq b_{n+1} \\ g \circ h(a, b) \text{ se } b = b_{n+1} \end{cases}$$

Esercizio 3.12. *Dimostrare che se A è un insieme finito di cardinalità m allora A^n (il prodotto cartesiano di n copie di A) ha cardinalità m^n.*

2. Contare il numero di funzioni tra due insiemi finiti

Consideriamo l'insieme F delle funzioni $f : A \to B$, con $|A| = m$ e $|B| = n$. Vogliamo contare il numero di elementi di F, ovvero il numero di funzioni distinte da A a B. Si ha il seguente risultato:

Teorema 3.13. *Se A e B sono due insiemi finiti di cardinalità rispettivamente m e n, la cardinalità dell'insieme F delle funzioni da A a B è n^m.*

DIMOSTRAZIONE. Sappiamo che per definire una funzione da A in B, bisogna associare ad ogni elemento di A un elemento di B. Dimostriamo il teorema per induzione sul numero m di elementi di A.

Passo base. Se $m = 1$, allora per l'unico elemento di A abbiamo n scelte possibili, ognuna delle quali definisce una funzione diversa da A a B. Perciò ci sono n funzioni distinte da A a B.

Passo induttivo. Supponiamo la tesi vera per insiemi di $m-1$ elementi, e proviamola per insiemi di m elementi. Di funzioni da $A' = \{x_2, \ldots, x_m\}$ a B ce ne sono, per ipotesi induttiva, n^{m-1}. Da ognuna di queste funzioni otteniamo una funzione da A a B associando x_1 ad un elemento di B. Perciò da ogni funzione da A' a B otteniamo n diverse funzioni da A a B e quindi ci sono $n^{m-1} \cdot n = n^m$ funzioni distinte da A a B. □

Osservazione 3.14. La dimostrazione appena conclusa può generare qualche perplessità, in quanto, al fine di dimostrare che la cardinalità di un insieme è m, abbiamo abbandonato il formalismo fin qui adottato legato alla ricerca di bigezioni su insiemi del tipo $\mathbb{N}_m$. Proponiamo quindi un'altra dimostrazione del fatto che l'insieme F delle funzioni da un insieme A di cardinalità m ad un insieme B di cardinalità n è tale che $|F| = n^m$.

Elenchiamo gli m elementi di A: $\{a_1, a_2, \ldots, a_m\}$ e mostriamo come esista una funzione biunivoca dall'insieme F in B^m. Consideriamo la funzione h da F in B^m definita da: $h(f) = (f(a_1), f(a_2), \ldots, f(a_m)) \in B^m$. Provare (esercizio) che h è iniettiva.

Consideriamo poi la funzione g da B^m in F definita da: $g(b_1, \ldots, b_m) = f$ tale che $f(a_i) = b_i$ per ogni i. Anche in questo caso provare (esercizio) che g è iniettiva. Il Corollario 3.7 ci assicura che esiste una t bigettiva da F in B^m e quindi che $|F| = |B^m|$. La conclusione segue dal risultato dell'Esercizio 3.12, il quale afferma che, la cardinalità di B^m, è uguale alla cardinalità di B elevata alla m, cioè n^m.

E se invece volessimo contare la cardinalità dell'insieme F_i delle funzioni iniettive da A in B? Sappiamo già (vedi Teorema 3.5) che se $m > n$ (dove ricordiamo m e n sono le cardinalità rispettivamente di A e B) F_i è vuoto. Inoltre osserviamo che F_i è un sottoinsieme dell'insieme F di tutte le funzioni da A a B di cui abbiamo appena calcolato la cardinalità quindi: $|F_i| \leq m^n$. Possiamo essere più precisi e determinare la cardinalità esatta di F_i:

Teorema 3.15. *L'insieme F_i delle funzioni iniettive da A a B, con A e B di cardinalità rispettivamente m e n, ha cardinalità uguale a:*

$$n \cdot (n-1) \cdot \ldots \cdot (n-(m-1)) = \prod_{i=0}^{m-1} (n-i)$$

Dimostrazione. Elenchiamo gli m elementi di A:

$$A = \{a_1, \ldots, a_m\}$$

Se $m > n$ sappiamo che non ci sono funzioni iniettive, e la formula da provare funziona perché nella produttoria compare un fattore 0. Supponiamo dunque che $m \leq n$. Definire una funzione iniettiva da A in B vuol dire assegnare, ad ogni elemento di A, un elemento di B, in modo che due elementi distinti di A non siano assegnati allo stesso elemento di B. Allora procediamo a contare in quanti modi possiamo *costruire* funzioni siffatte. Anche in questo caso procediamo per induzione sulla cardinalità m di A.

Passo base. Se $m = 1$, $A = \{a_1\}$ e quindi ogni funzione da A in B è iniettiva (cioè $F = F_i$). Se ne conclude che $|F_i| = |F| = n$.

Anche senza usare tale formalismo si poteva notare che, per definire una funzione (iniettiva) da A a B, basta associare all'unico elemento a_1 di A un qualsiasi elemento di B. Abbiamo dunque n scelte, che corrispondono a n diverse funzioni

(iniettive) da A in B.
Passo induttivo. Consideriamo $A = \{a_1, \ldots, a_m\}$ con $m > 1$, e cominciamo a costruire una funzione iniettiva da A a B. Scegliamo un elemento b di B da assegnare a $f(a_m)$: abbiamo n scelte possibili. Fissato $f(a_m)$ dobbiamo assegnare a tutti gli altri $f(a_i)$ (con $i < m$) un elemento di B in modo che:

$$\forall 1 \leq i < j \leq m \quad f(a_i) \neq f(a_j)$$

In pratica dobbiamo definire una funzione iniettiva da $A \setminus \{a_m\}$ in $B \setminus \{b\}$. Per ipotesi induttiva il numero di queste funzioni è:

$$c = \prod_{i=0}^{m-2} (n - 1 - i) = \prod_{i=1}^{m-1} (n - i)$$

Per ognuna delle n scelte possibili di $f(a_m)$ abbiamo c funzioni iniettive da A in B. Dunque il totale delle funzioni iniettive da A in B è $n \cdot c$, ovvero:

$$n \cdot \prod_{i=1}^{m-1} (n - i) = \prod_{i=0}^{m-1} (n - i)$$

□

A questo punto, *ci abbiamo preso gusto* e ci chiediamo: quante sono le funzioni bigettive fra due insiemi finiti A a B? La prima osservazione è che, affinché esista una funzione bigettiva da A a B, deve essere $|A| = |B| = n$. Inoltre, dal Teorema 3.10 segue che una funzione tra due insiemi A e B della stessa cardinalità è bigettiva se e solo se è iniettiva. Dunque basta applicare il Teorema 3.15 per contare quante sono le funzioni iniettive tra due insiemi di cardinalità n.

Teorema 3.16. *Il numero di funzioni bigettive da A a B, insiemi finiti con n elementi è $n!$.*

Un caso particolare che analizzeremo anche in seguito è quello dell'insieme delle funzioni bigettive da un insieme in se stesso:

Definizione 3.17. Le funzioni bigettive di un insieme A in se stesso si dicono **permutazioni** di A.

3. Numero di sottoinsiemi di un insieme finito e binomio di Newton

Consideriamo un insieme $A = \{x_1, \ldots, x_n\}$ con n elementi. Vogliamo contare quanti sono i sottoinsiemi distinti X di A con k elementi ($0 \leq k \leq n$). È importante sottolineare come, ovviamente, questo calcolo prescinde completamente dalla natura degli oggetti contati. Procediamo per passi:

- Contiamo il numero di stringhe di lunghezza k in A (cioè sequenze ordinate di k elementi distinti di A). In pratica costruire una stringa significa costruire una funzione iniettiva tra l'insieme dei posti in una stringa (identificabile con $\mathbb{N}_k$: all'elemento i di $\mathbb{N}_k$ facciamo corrispondere il posto i-esimo nella stringa) e A. Dunque, la cardinalità dell'insieme contenente le stringhe di k elementi distinti di A è uguale alla cardinalità dell'insieme delle funzioni iniettive da $\mathbb{N}_k$ ad A, ovvero a $\prod_{i=0}^{k-1}(n - i)$.

- Osserviamo che, ad ogni stringa di quelle costruite nel passo precedente, possiamo associare il sottoinsieme di k elementi di A formato dai k elementi della stringa. Tale associazione si guarda bene però dall'essere bigettiva in quanto, per esempio, le stringhe $x_1, x_2, x_3, ..., x_k$ e $x_2, x_1, x_3, ..., x_k$ sono distinte (in un caso il primo elemento è x_1 nell'altro x_2). D'altra parte il sottoinsieme individuato è il medesimo, perché nelle due stringhe ci sono gli stessi elementi ordinati in maniera diversa. La domanda da farsi è quindi: quante stringhe distinte sono associate allo stesso insieme? Tante quanti sono i modi di ordinare in maniera diversa k elementi in k caselle, cioè il numero di funzioni bigettive tra due insiemi di k elementi, ovvero $k!$.

Riassumendo abbiamo che ci sono $\prod_{i=0}^{k-1}(n-i)$ stringhe di k elementi distinti di A, con gruppi di $k!$ stringhe definiscono lo stesso insieme. Dunque:

Teorema 3.18. *Dato A di cardinalità n, e k con $0 \leq k \leq n$, il numero di sottoinsiemi distinti di A di cardinalità k è:*

$$\frac{\prod_{i=0}^{k-1}(n-i)}{k!}$$

Definizione 3.19. Indicheremo il numero dei sottoinsiemi di k elementi di un insieme di n elementi con il simbolo: $\binom{n}{k}$. Tale numero sarà detto anche **coefficiente binomiale** n su k.

Osservazione 3.20. Introduciamo anche la notazione $\wp_k(A)$ per indicare l'insieme di tutti i sottoinsiemi P_k di A che hanno cardinalità k. Il Teorema 3.18 può essere dunque riscritto in simboli:

$$|\wp_k(A)| = \binom{n}{k} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}$$

Moltiplicando numeratore e denominatore per $(n-k)!$ si ha anche che:

$$|\wp_k(A)| = \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

Osserviamo che il numero $|\wp_k(A)|$ dipende solo dalla cardinalità di A, e non dalla natura dei suoi elementi.

Esempio 3.21. Supponiamo di voler calcolare quante sono le possibili cinquine che possono uscire da una estrazione di 5 numeri del lotto (che pesca dall'insieme dei numeri interi da 1 a 90). Nel gioco del lotto appunto non è importante l'ordine di estrazione, quel che conta è l'insieme di 5 numeri giocato, quindi quello che vogliamo contare, per rispondere alla domanda "quanti sono i sottoinsiemi distinti di 5 elementi dell'insieme di 90 elementi dei numeri del lotto?", è la cardinalità di $\wp_5(\mathbb{N}_{90})$. La risposta l'abbiamo già, ed è:

$$\binom{90}{5} = \frac{90!}{5! \cdot 85!} = \frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{120}$$

Se vogliamo proprio calcolarlo questo numero è 43.949.268. Ciò significa che, giocando una cinquina secca, la probabilità (considerando l'estrazione di ogni numero equiprobabile, e dunque che non ci siano imbrogli) che dall'estrazione di 5 numeri dai 90 escano proprio i numeri che abbiamo giocato è praticamente una su 44 milioni...

Osservazione 3.22. Una proprietà interessante dei coefficienti binomiali è una immediata conseguenza del loro esprimere la cardinalità di un $\wp_k(A)$.

L'osservazione chiave è che la funzione f, che ad ogni elemento X in $\wp_k(A)$ associa il suo complementare $\overline{X}$ (di cardinalità $n-k$), è una bigezione tra $\wp_k(A)$ e $\wp_{n-k}(A)$. Dunque i due insiemi hanno la stessa cardinalità, ovvero:

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right)$$

A questo punto vogliamo usare i coefficienti binomiali per dare una formula che permetta di sviluppare, dati $x, y \in \mathbb{R}$, il binomio $(x+y)^n$ al variare di $n \in \mathbb{N}$.

Innanzitutto osserviamo che sviluppando $(x+y)^n$ si ottengono tanti addendi il cui grado totale in x, y è sempre n. Come si fanno ad ottenere questi addendi? Scriviamo *per esteso* $(x+y)^n$:

$$(x+y)^n = \underbrace{(x+y) \cdot \ldots \cdot (x+y)}_{n \text{ volte}}$$

Calcolare il prodotto a secondo membro significa, per la proprietà distributiva, scegliere da ognuno degli n fattori $x+y$ uno tra x e y. Ad esempio se scegliamo x nei primi $n-1$ fattori e y nell'ultimo, otteniamo l'addendo $x^{n-1}y$. Al variare di tutte le possibili scelte otteniamo tutti gli addendi di $(x+y)^n$. Questo implica che il risultato sarà *simmetrico* in x, y (d'altra parte questo era ovvio anche per la proprietà commutativa della somma, infatti $(x+y)^n = (y+x)^n$).

Ci interessa contare però in quanti modi diversi a troverò un particolare addendo: perché questo vorrà dire che nello sviluppo del binomio quell'addendo apparirà moltiplicato per a. Cerchiamo di capire come fare attraverso un esempio: consideriamo lo sviluppo di $(x+y)^3$. Scriviamolo per esteso e sotto le possibili scelte:

$(x+y)$	$(x+y)$	$(x+y)$
x	x	x
x	x	y
x	y	x
x	y	y
y	x	x
y	x	y
y	y	x
y	y	y

Ovvero se scegliamo x da tutti i fattori otteniamo x^3. Se scegliamo x da un fattore e y dagli altri 2, otteniamo xy^2: lo possiamo fare (quarta, sesta e settima riga) in 3 modi differenti, e dunque avremo nello sviluppo del binomio $3xy^2$. Procedendo analogamente per x^2y e y^3, si ottiene il ben noto sviluppo:

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

Cerchiamo, a partire dall'esempio sopra, di studiare il caso generale. Quanti addendi della forma $x^i y^{n-i}$, con $i \leq n$, avremo nello sviluppo del binomio $(x+y)^n$? Si tratta di contare in quanti modi differenti posso scegliere i fattori dalla produttoria di n fattori (dai fattori individuati sceglieremo x, e dai restanti $n-i$ fattori sceglieremo y). Se associamo un etichetta numerica ai fattori della produttoria (1 per il primo, 2 per il secondo, etc.), si tratta di capire in quanti modi diversi possiamo scegliere i etichette dall'insieme delle etichette (che in questo caso essendoci

n fattori) è $\mathbb{N}_n$. Ovvero il numero di addendi della forma $x^i y^{n-i}$ nello sviluppo del binomio $(x+y)^n$ equivale alla cardinalità di $\wp_i(\mathbb{N}_n)$. Abbiamo dunque il seguente teorema.

Teorema 3.23 (Teorema del binomio di Newton)**.** *Siano x, y numeri reali, per ogni $n \in \mathbb{N}$ si ha:*

$$(x+y)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) x^i y^{n-i}$$

Osservazione 3.24. Osserviamo che, per possibili generalizzazioni ad insiemi diversi da $\mathbb{R}$, la dimostrazione di questo risultato usa (esercizio: dove?) la commutatività e l'associatività della moltiplicazione in $\mathbb{R}$.

Dal teorema del binomio di Newton segue un risultato importante sul numero totale di sottoinsiemi di un insieme finito A di cardinalità n. Prima di enunciare e dimostrare il risultato introduciamo la terminologia e la notazione usata.

Definizione 3.25. L'insieme dei sottoinsiemi di un insieme A è detto **insieme delle parti** di A. Indicheremo tale insieme con il simbolo $\wp(A)$.

Teorema 3.26. *Dato A insieme finito con n elementi si ha $|\wp(A)| = 2^n$.*

Dimostrazione. Proponiamo due dimostrazioni differenti di questo risultato. Si può procedere osservando che, per contare tutti i sottoinsiemi di A, si può sommare tra loro il numero di sottoinsiemi di A con un numero k fissato di elementi, al variare di k tra 0 e n. Dal Teorema 3.18 segue che:

$$|\wp(A)| = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right)$$

Il secondo membro è uguale allo sviluppo del binomio di Newton con $x = y = 1$, dunque:

$$|\wp(A)| = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) = (1+1)^n = 2^n$$

Un altra strada per provare lo stesso risultato è quella di elencare gli elementi di A: $A = \{a_1, \ldots, a_n\}$, e di osservare che identificare un sottoinsieme B di A, equivale a dire per ogni a_i, se a_i appartiene a B o non appartiene a B.

Per ogni a_i abbiamo dunque 2 scelte: a_i appartiene a B, a_i non appartiene a B. Al variare di tutte le scelte possibili differenti, si individuano tutti i sottoinsiemi di A. Quante sono dunque queste scelte possibili? Tante quante sono le funzioni da un insieme di n elementi ad un insieme di 2 elementi (appartiene - non appartiene), ovvero - per il Teorema 3.13 - proprio 2^n. □

Il Teorema 3.26 può essere dimostrato anche per induzione.

Esercizio 3.27. *Provare a dimostrare l'enunciato del Teorema 3.26 per induzione sul numero di elementi n di A.*

Svolgimento. Questo esercizio permette di evidenziare un metodo per contare sottoinsiemi che spesso è utile.
Passo base. Se $n = 0$ l'insieme vuoto ha un solo sottoinsieme (l'insieme vuoto stesso), ed effettivamente $2^0 = 1$.
Passo induttivo. Consideriamo un insieme A di $n+1$ elementi e isoliamone 1

che indichiamo con a (il caso A insieme vuoto lo abbiamo già trattato nel passo base quindi possiamo supporre che A abbia almeno un elemento). I sottoinsiemi di A che non contengono a sono i sottoinsiemi di $A \setminus \{a\}$, quindi i sottoinsiemi di un insieme di n elementi, e perciò, per ipotesi induttiva, sappiamo essere 2^n. I sottoinsiemi di A che contengono a si ottengono unendo ad a un qualsiasi sottoinsieme di $A - \{a\}$, e quindi sono ancora 2^n. Un sottoinsieme di A o contiene a o non lo contiene, cioè in questi due casi sono compresi tutti i sottoinsiemi di A che perciò sono $2^n + 2^n = 2^{n+1}$.

Esercizio 3.28. *Dimostrare che:*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 \tag{3.1}$$

Svolgimento. Basta osservare che la formula 3.1 è lo sviluppo del binomio di Newton $(1 + (-1))^n$.

Esercizio 3.29. *Dato $k \in \mathbb{N}$, quante sono le n-uple $(x_1, \ldots, x_n)$ di numeri naturali che risolvono l'equazione $\sum_{i=1}^{n} x_i = k$?*

Svolgimento. Osserviamo che rispondere a questa domanda equivale a dire in quanti modi diversi si possono mettere k oggetti in n scatole (le scatole sono gli x_i). Usiamo una semplice rappresentazione grafica su un esempio numerico che aiuterà a rispondere alla domanda in generale: supponiamo di avere 17 oggetti e 5 scatole.

.....|..|......| |....

Nella rappresentazione grafica usata, i 17 punti rappresentano gli oggetti e le 4 sbarre individuano le 5 scatole: nella prima scatola ci sono 5 oggetti, nella seconda 2, nella terza 6, nella quarta nessuno e nella quinta 4.

L'osservazione chiave è che esiste una corrispondenza biunivoca tra le rappresentazioni grafiche del tipo sopra, e le possibili disposizioni oggetti-scatole, che è quello che vogliamo contare. Dunque per rispondere alla nostra domanda, possiamo anche contare il numero delle rappresentazioni grafiche possibili con k punti e n scatole. Per contare il numero di diverse rappresentazioni grafiche possibili, basta osservare che si tratta di *posizionare* $n - 1 + k$ oggetti ($n - 1$ sbarre tra loro indistinguibili e k oggetti anch'essi tra loro indistinguibili) su $n - 1 + k$ spazi. Si tratta perciò di decidere dove mettere i k oggetti o equivalentemente le $n-1$ sbarre che individuano le n scatole.

Il numero delle rappresentazioni grafiche possibili (ovvero numero di soluzioni di $\sum_{i=1}^{n} x_i = k$) è dunque:

$$\binom{n+k-1}{k} \text{ oppure } \binom{n+k-1}{n-1}$$

infatti $n + k - 1$ è il numero di oggetti che compongono il grafico mentre

$$\binom{n+k-1}{k} \quad \text{e} \quad \binom{n+k-1}{n-1}$$

sono rispettivamente i modi distinti in cui si possono disporre nel grafico i k punti e le $n - 1$ sbarre.

Esercizio 3.30. (1) *Calcolare il numero di terne ordinate (A, B, C) di sottoinsiemi di $\mathbb{N}_n$ a due a due disgiunti con $A \cup B \cup C = \mathbb{N}_n$.*
(2) *Dimostrare che il numero di terne ordinate (A, B, C) di sottoinsiemi di $\mathbb{N}_n$ tali che $A \cup B \cup C = \mathbb{N}_n$ è 7^n.*

Svolgimento. (1) Determinare una terna (A, B, C) con le caratteristiche richieste, corrisponde ad associare *ognuno* degli elementi di $\mathbb{N}_n$ ad uno ed *uno solo* dei tre insiemi A, B e C. *Ognuno* perché l'unione dei tre insiemi è $\mathbb{N}_n$, ed *uno solo* perché i tre insiemi sono disgiunti. Dunque contare quante sono le differenti terne (A, B, C), equivale a contare il numero di funzioni possibili tra l'insieme $\mathbb{N}_n$, e l'insieme delle tre *etichette* $\{A,\ B,\ C\}$. Sappiamo già quante sono queste terne: 3^n.
(2) In questo secondo caso, vogliamo contare le terne (A, B, C) la cui unione è $\mathbb{N}_n$, senza imporre che i tre insiemi siano a due a due disgiunti (per cui questo numero deve essere necessariamente maggiore o uguale del numero al punto (1)). Si tratta dunque, per ogni elemento i di $\mathbb{N}_n$, di scegliere se sta in A, se sta in B, se sta in C, con la condizione che in almeno uno dei tre deve stare (per ipotesi l'unione di A, B, C è tutto $\mathbb{N}_n$). Scegliere questo equivale ad associare, ad ogni elemento di $\mathbb{N}_n$, una terna ordinata (a, b, c) dove a, b, c variano tra 0 (non appartiene a) e 1 (appartiene a). Per ogni elemento di $\mathbb{N}_n$ dunque si può scegliere tra 7 possibilità (le terne possibili di 0 e 1 sono in totale 8, ma noi dobbiamo escludere dalle scelte possibili quella tutta di 0). Dunque la cardinalità cercata è uguale al numero di funzioni da $\mathbb{N}_n$ alle 7 scelte possibili, che sappiamo essere 7^n.

4. Principio di inclusione-esclusione

In questo paragrafo vogliamo affrontare la questione di contare il numero di elementi (la cardinalità) dell'unione di n insiemi finiti, conoscendo la cardinalità dei singoli insiemi e delle loro mutue intersezioni.

Prima di affrontare il problema nella sua generalità, cominciamo ad affrontare dei casi particolari con n piccolo e fissato.
$\mathbf{n = 2}$. Dati due insiemi A_1 e A_2 di cardinalità finita, vogliamo determinare la cardinalità di $A_1 \cup A_2$. Osserviamo che se sommiamo $|A_1|$ e $|A_2|$, contiamo due volte gli elementi che appartengono ad $A_1 \cap A_2$ (dunque, in generale, $|A_1| + |A_2| \geq |A_1 \cup A_2|$). Da questa osservazione segue che:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Esercizio 3.31. *Sia m un numero naturale. Determinare il numero dei divisori di 10^{2m} che nella scrittura decimale terminano con un numero pari di zeri.*

Svolgimento. I divisori di $n = 10^{2m} = 2^{2m} \cdot 5^{2m}$ sono gli elementi dell'insieme $D = \{d \in \mathbb{N} | d = 2^\alpha \cdot 5^\beta,\ 0 \leq \alpha \leq 2m,\ 0 \leq \beta \leq 2m\}$. Quali di questi finiscono con un numero pari di zeri? Dato d in D, sia k quel numero per cui d è multiplo di 10^k, ma non di 10^{k+1}. k è il numero di zeri con cui finisce d, dunque ci interessano quei d per cui k è pari. E a cosa corrisponde k? k è semplicemente (provate a spiegare perché) il minimo tra α e β.

A questo punto possiamo procedere in diversi modi per rispondere alla domanda. Contiamo prima i d in D per cui $\alpha \leq \beta$. Fissato α pari, qualsiasi β maggiore di α e minore di $2m$ restituisce un d in D (di tali β dunque ce ne sono $2m - \alpha + 1$, una volta fissato α). Ovvero i d in D con $\alpha \leq \beta$ sono:

$$\sum_{\substack{\alpha \text{ pari}, \\ 0 \leq \alpha \leq 2m}} (2m - \alpha + 1)$$

Quella sopra è la somma dei primi $m + 1$ numeri dispari, che è $(m + 1)^2$. Simmetricamente i d in D con $\alpha \geq \beta$ saranno sempre $(m + 1)^2$.

Ci rimane da contare quanti sono i d in D con $\alpha = \beta$, ma questo è facile: sono i diversi numeri pari da 0 a $2m$, ovvero $m+1$. Il numero di elementi di D che termina con un numero pari di zeri è dunque $(m+1)^2 + (m+1)^2 - (m+1)$.

n = 3. Questo caso lo trattiamo con più calma, perché è *rivelatore* di quel che accade nel caso generale.

Anche nel caso di 3 insiemi finiti A_1, A_2, A_3, osserviamo che sommando le rispettive cardinalità contiamo più volte le mutue intersezioni. Potrebbe venire in mente che, come nel caso precedente, $|A \cup B \cup C|$ si ottenga togliendo, alla somma delle singole cardinalità dei tre insiemi, le cardinalità delle intersezioni prese a due a due ($|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3|$). Vediamo che così non è.

Gli elementi di $A_1 \cup A_2 \cup A_3$ possono essere elementi che appartengono: **a**) ad uno solo dei tre insiemi e non agli altri due, **b**) a due degli insiemi e non al terzo, **c**) a tutti e tre gli insiemi. Affinché $|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3|$ sia uguale a $|A_1 \cup A_2 \cup A_3|$, deve contare gli elementi di tutti e tre i tipi esattamente una volta.

Gli elementi del tipo **a** sono effettivamente contati esattamente una volta. Infatti consideriamo ad esempio un elemento che stia solo in A_1. Questo viene contato una volta in $|A_1|$ e poi *non appare più* nel conteggio in quanto non appartiene a nessuno dei seguenti insiemi A_2, A_3, $A_1 \cap A_2$, $A_1 \cap A_3$, $A_2 \cap A_3$.

Anche gli elementi del tipo **b** sono contati esattamente una volta. Infatti, un elemento che ad esempio sta in $A_1 \cap A_2$, ma non in A_3, nella formula considerata viene contato una volta in $|A_1|$, una volta in $|A_2|$ e una volta, ma con segno meno, in $|A_1 \cap A_2|$.

Il problema sorge per gli elementi del tipo **c**. Se infatti un elemento appartiene ad $A_1 \cap A_2 \cap A_3$, allora esso viene prima contato 3 volte (appartiene ad A_1, A_2 e A_3), e poi tolto 3 volte (appartiene ad $A_1 \cap A_2$, $A_2 \cap A_3$ e $A_1 \cap A_3$).

Si tratta dunque di contare anche questi elementi, aggiungendo, alla formula da cui eravamo partiti, la cardinalità dell'intersezione dei tre insiemi. Perciò:

(4.1)
$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

A questo punto siamo pronti ad enunciare il risultato generale.

Teorema 3.32 (Principio d'inclusione-esclusione)**.** *Dati $A_1, \ldots, A_n$ finiti si ha che:*

$$|A_1 \cup \ldots \cup A_n| = \sum_{m=1}^{n} ((-1)^{m-1} \sum_{1 \le i_1 < \ldots < i_m \le n} |\bigcap_{j=1}^{m} A_{i_j}|) \tag{4.2}$$

Prima di dimostrare il teorema cerchiamo di capire cosa dice la formula presente nell'enunciato. Si tratta di sommare tra loro n addendi ($\sum_{m=1}^{n}$), con segno alternato ($(-1)^{m-1}$), ognuno dei quali conta una certa cardinalità. La parte più difficile da capire della formula è probabilmente proprio quella finale

$$\sum_{1 \le i_1 < \ldots < i_m \le n} |\bigcap_{j=1}^{m} A_{i_j}|$$

In realtà è più semplice di quello che si possa pensare: si tratta di considerare tutti i modi possibili di scegliere m indici distinti (questo essendo ogni indice strettamente

minore del successivo) dall'insieme $\mathbb{N}_n$, e dunque di sommare le cardinalità di tutte le possibili intersezioni tra m insiemi diversi scelti tra gli A_i.

Cerchiamo di esemplificare la formula 4.2, nel caso $n = 3$ già discusso, per ritrovare la formula 4.1:

$$|A_1 \cup A_2 \cup A_n| = \sum_{m=1}^{3}((-1)^{m-1} \sum_{1\leq i_1<\ldots<i_m\leq 3} |\bigcap_{j=1}^{m} A_{i_j}|)$$

Consideriamo gli addendi della prima sommatoria uno alla volta.

Se $m = 1$, nella seconda sommatoria dobbiamo scegliere un solo indice (i_1 appunto) da $\mathbb{N}_3$, lo possiamo fare in tre modi diversi: $i_1 = 1$, $i_1 = 2$, $i_1 = 3$. A questo punto si tratta di calcolare

$$\sum_{i_1\in\{1,2,3\}} |\bigcap_{j=1}^{1} A_{i_1}|$$

In questo caso può creare un po' di confusione il fatto che ci sia il simbolo di intersezione: cosa significa fare l'intersezione di un solo insieme? L'insieme stesso. Considerare, con questa convenzione, intersezioni tra insiemi, ma anche sommatorie e produttorie tra numeri, anche nel caso di un solo elemento, è utile proprio dal punto di vista notazionale, ci permette di scrivere formule *compatte*. Dunque, se $m = 1$ otteniamo, come *contributo alla sommatoria*, il numero $|A_1| + |A_2| + |A_3|$.

Se $m = 2$, dobbiamo scegliere due indici (i_1, i_2) da $\mathbb{N}_3$. Anche in questo caso abbiamo 3 modi per farlo (le possibili scelte di 2 elementi da un insieme di 3 elementi), e otteniamo dunque:

$$(-1)^{2-1} \sum_{1\leq i_1<i_2\leq 3} |\bigcap_{j=1}^{2} A_{i_j}| = -(|A_1 \cap A_2| + |A_2 \cap A_3| + |A_1 \cap A_3|)$$

Infine se $m = 3$, dobbiamo scegliere tre indici da $\mathbb{N}_3$ e abbiamo un solo modo per farlo, che ci restituisce la cardinalità dell'intersezione tra i 3 insiemi. Abbiamo dunque, come ci aspettavamo, ritrovato la formula 4.1 del caso particolare $n = 3$.

A questo punto, dopo la necessaria spiegazione della notazione, passiamo alla dimostrazione vera e propria del teorema di inclusione-esclusione (il cui nome è significativo del processo di conteggio a cui si arriva alla formula finale).

Dimostrazione. Dobbiamo dimostrare che ogni elemento di $A_1 \cup \ldots \cup A_n$ è contato esattamente una volta dalla formula 4.2. Sia x un elemento dell'unione: x apparterrà ad alcuni A_i. Essendo l'unione tra insiemi commutativa, non è restrittivo supporre x appartenente ai primi k insiemi A_i, e dunque $x \in A_1 \cap \ldots \cap A_k$ e $x \notin A_{k+1} \cup \ldots \cup A_n$. Nell'uguaglianza 4.2, x viene contato, con il primo termine della sommatoria (ovvero $m = 1$), k volte (una volta per ognuno degli A_i a cui appartiene). Nelle intersezioni tra due degli A_i, x compare solo tra quelle tra i primi k insiemi. Quindi per $m = 2$, x viene contato $|\wp_2(\mathbb{N}_k)|$ volte (i modi diversi in cui possiamo scegliere due indici j, t da $\mathbb{N}_k$ per cui x appartenga ad $A_j \cap A_t$). Più in generale, per $m = s$ ($s \leq k$ in quanto l'intersezione di $k + 1$ tra gli A_i, non conterrà mai x), l'elemento x sarà contato $|\wp_s(\mathbb{N}_k)|$ volte. Dunque l'elemento x è contato esattamente:

$$\sum_{i=1}^{k}(-1)^{i-1} \left(\begin{array}{c} k \\ i \end{array} \right) \text{ volte} \tag{4.3}$$

Per dimostrare il teorema bisogna dimostrare che la sommatoria in 4.3 è uguale a 1. Questo è vero infatti:

$$\sum_{i=1}^{k}(-1)^{i-1}\left(\begin{array}{c} k \\ i \end{array}\right) - 1 = \sum_{i=0}^{k}(-1)^{i}\left(\begin{array}{c} k \\ i \end{array}\right) \underbrace{=}_{ese.3.28} (1-1)^k = 0$$

□

Usiamo il Teorema 3.32 per calcolare quante sono le funzioni surgettive da un insieme A con m elementi ad un insieme B con n elementi.

Sappiamo che tutte le funzioni da A in B sono n^m, contando il numero t delle funzioni non surgettive da A a B avremo che la cardinalità dell'insieme delle funzioni surgettive da A a B è uguale a $n^m - t$. Sia $B = \{x_1, \ldots, x_n\}$ e consideriamo i seguenti n sottoinsiemi (al variare di i tra 1 e n) dell'insieme delle funzioni da A a B:

$$X_i = \{f | f : A \to B \text{ e } i \notin f(A)\}$$

In pratica le funzioni f appartenenti a X_i sono tante quante le f da A a $B \setminus \{i\}$.

Esercizio 3.33. *Dimostrare che, con le notazioni sopra introdotte, scelti k insiemi $X_{i_1}, \ldots, X_{i_k}$ distinti tra gli X_i, si ha:*

$$|\cap_{j=1}^{k} X_{i_j}| = (n-k)^m$$

Le funzioni da A a B non surgettive sono quelle che stanno nella unione degli insiemi X_i al variare di i tra 1 e n. La cardinalità delle funzioni surgettive da A a B sarà dunque:

$$n^m - |\bigcup_{i=1}^{n} X_i|$$

Dal Teorema 3.32, e dall'esercizio 3.33 segue:

Teorema 3.34. *La cardinalità dell'insieme delle funzioni surgettive da A di cardinalità m a B di cardinalità n è:*

$$n^m - \sum_{i=1}^{n}(-1)^{i-1}\left(\begin{array}{c} n \\ i \end{array}\right)(n-i)^m = \sum_{i=0}^{n}(-1)^{i}\left(\begin{array}{c} n \\ i \end{array}\right)(n-i)^m$$

Esercizio 3.35. *Calcolare il numero di soluzioni (x, y, x) in $\mathbb{N}^3$ del sistema:*

$$\begin{cases} x + y + z = 100 \\ 0 \leq x \leq 50 \\ 2 \leq y \leq 40 \\ 10 \leq z \leq 50 \end{cases}$$

Svolgimento. Sappiamo che il numero di terne (x, y, z) di numeri naturali che sono soluzione dell'equazione $x+y+z = 100$ è $\left(\begin{array}{c} 102 \\ 2 \end{array}\right) = \frac{102 \cdot 101}{2} = 5151$. Ora vogliamo contare il numero di soluzioni (non risolverla) della stessa equazione imponendo ulteriori vincoli su x, y, z. Il primo passo, per eludere le limitazioni sul tetto minimo, è quello di cambiare variabili, e porre $s = y - 2$ e $t = z - 10$. Il nuovo sistema, con numero di soluzioni invariato rispetto a quello di partenza, è:

$$\begin{cases} x + s + t = 88 \\ 0 \leq x \leq 50 \\ 0 \leq s \leq 38 \\ 0 \leq t \leq 40 \end{cases}$$

Sappiamo già (Esercizio 3.29) che la cardinalità di S, l'insieme delle soluzioni di $x+s+t=88$ (senza ulteriori vincoli), è $\binom{90}{2}$. Per rispondere alla domanda iniziale, dobbiamo trovare il numero N delle soluzioni di $x+s+t=88$ che non rispettano i vincoli introdotti. Introduciamo le seguenti notazioni:

$$S_x=\{(x,s,t)\in S|x\geq 51\},\ S_s=\{(x,s,t)\in S|s\geq 39\},\ S_t=\{(x,s,t)\in S|t\geq 41\}$$

Il numero N cercato è la cardinalità di $S_x\cup S_t\cup S_s$. Per cui, usando il teorema di inclusione-esclusione si ha:

$$N=|S_x|+|S_s|+|S_t|-|S_x\cap S_s|-|S_x\cap S_t|-|S_s\cap S_t|+|S_x\cap S_s\cap S_t|$$

A questo punto si tratta di calcolare le cardinalità che intervengono nella uguaglianza precedente. Osserviamo che, passando al complementare dell'insieme cercato, abbiamo *trasformato* i vincoli superiori sulle variabili, in vincoli inferiori (vincoli che abbiamo già visto come trattare).

Cominciamo dalla cardinalità degli insiemi S_x, S_s, S_t. Ad esempio, S_x è il numero di soluzioni di $x+s+t=88$ la cui variabile x verifica il vincolo $x\geq 51$. Analogamente a quanto fatto sopra, procediamo con un cambio di variabile e poniamo $x=x_0+51$. Si ottiene $x_0+51+s+t=88$ (con il vincolo su x_0, sempre verificato, $x_0\geq 0$). $|S_x|$ è dunque uguale al numero di soluzioni in $\mathbb{N}^3$ dell'equazione $x_0+s+t=37$. Ovvero $|S_x|=\binom{39}{2}$. Procedendo in maniera del tutto analoga sui vincoli per s e t, si trova che $\binom{51}{2}$ e $\binom{49}{2}$ sono la cardinalità rispettivamente di S_s e S_t.

Si procede allo stesso modo per calcolare l'intersezione tra due dei tre insiemi S_x, S_s e S_t: si tratterà di togliere due vincoli inferiori. Ad esempio, se vogliamo calcolare $|S_x\cap S_s|$, poniamo $x=x_0+51$ e $s=s_0+39$, e otteniamo l'equazione $x_0+s_0+t+90=88$. Tale equazione non ha soluzioni in $\mathbb{N}$ e dunque $S_x\cap S_s$ è l'insieme vuoto. Analogamente, ponendo $x=x_0+51$ e $t=t_0+41$, otteniamo l'equazione $x_0+s+t_0+92=88$, anch'essa senza soluzioni in $\mathbb{N}$. Dunque anche $S_x\cap S_t$ è l'insieme vuoto. Infine ponendo $s=s_0+39$ e $t=t_0+41$ otteniamo l'equazione $x+s_0+t_0+80=88$, ovvero $x+s_0+t_0=8$. Questa equazione ha $\binom{10}{2}=45$ soluzioni in $\mathbb{N}$, perciò $|S_s\cap S_t|=45$.

Infine osserviamo che sappiamo già che $|S_x\cap S_s\cap S_t|=0$, in quanto S_x non ha nessun elemento in comune con gli altri due insiemi (bastava non avesse elementi in comune con uno dei due insiemi).

Dunque il numero di soluzioni del sistema iniziale è:

$$\underbrace{\binom{90}{2}}_{4005}-\left[\underbrace{\binom{39}{2}}_{780}+\underbrace{\binom{51}{2}}_{1275}+\underbrace{\binom{49}{2}}_{1176}\right]+\underbrace{\binom{10}{2}}_{45}=819$$

CAPITOLO 4

L'insieme $\mathbb{Z}$ dei numeri interi relativi

1. Introduzione e definizione formale

L'insieme dei numeri interi è sicuramente noto a tutti gli studenti, che hanno lavorato ed eseguito operazioni con interi fin dalla scuola primaria. L'idea intuitiva di insieme dei numeri interi è quella di unione di due copie disgiunte dei numeri naturali (senza lo zero) e dello 0: $\mathbb{Z} = \mathbb{N}^- \sqcup \{0\} \sqcup \mathbb{N}^+$, dove con $\mathbb{N}^-$ e $\mathbb{N}^+$ indichiamo rispettivamente gli interi negativi e positivi. Questa idea intuitiva, accompagnata dalle regole di calcolo (tra cui la *famigerata* regola dei segni), permette di operare sui numeri interi senza grossi problemi. In questo paragrafo introduttivo però vogliamo dare una possibile costruzione più formale dei numeri interi a partire dai numeri naturali. Questo perché tale costruzione coinvolge la nozione di insieme quoziente che abbiamo introdotto nel primo capitolo e con cui è importante prendere familiarità. Cercheremo, seppur brevemente, di mostrare anche come la costruzione formale sia in un certo senso *guidata* dallo scopo con cui sono stati introdotti i numeri interi.

I numeri interi rispondono all'esigenza pratica di introdurre quantità negative (esigenza tipicamente sorta con gli scambi commerciali e con la nascita dei debiti) e all'esigenza teorica di permettere sempre la sottrazione tra numeri naturali.

Come abbiamo osservato introducendo i numeri naturali non è possibile all'interno di essi eseguire la sottrazione $m - n$ se n è maggiore di m. Proprio questa osservazione è la chiave per la costruzione formale dei numeri interi: vogliamo che l'insieme dei numeri interi contenga tutte e solo le differenze tra numeri naturali. L'idea potrebbe essere quella di definire $\mathbb{Z}$ come l'insieme delle coppie di naturali (a, b): per esempio la coppia $(3, 5)$ rappresenterebbe l'intero che solitamente indichiamo con -2 (la differenza tra un *credito* di 3 e un *debito* di 5). In questo modo otteniamo un insieme che *contiene*[1] $\mathbb{N}$ e che rappresenta l'idea intuitiva di $\mathbb{Z}$: i numeri negativi saranno quelli che hanno la seconda componente maggiore della prima.

L'unico problema dell'identificazione di $\mathbb{Z}$ con gli elementi di $\mathbb{N} \times \mathbb{N}$, è che coppie diverse possono rappresentare la stessa differenza (ovvero quello che vorremmo fosse lo stesso numero intero): per esempio la coppia $(3, 5)$ e la coppia $(4, 6)$ (e in generale tutte le coppie $(c, 2 + c)$ con $c \in \mathbb{N}$). È il tipico caso in cui si vuole identificare elementi diversi, ovvero considerare classi di equivalenza. In questo caso si tratta di capire quando vogliamo che due elementi di $\mathbb{N} \times \mathbb{N}$ siano equivalenti e la risposta è che vogliamo che $(a, b) \sim (c, d)$ quando $a - b = c - d$ in $\mathbb{N}$. D'altra parte in $\mathbb{N}$ non sempre è possibile eseguire la sottrazione, quindi si tratta di esprimere la stessa

[1] In realtà $\mathbb{Z}$ qui è presentato come $\mathbb{N} \times \mathbb{N}$, dunque non contiene propriamente $\mathbb{N}$, ma un immagine di $\mathbb{N}$. Ovvero esiste una funzione iniettiva da $\mathbb{N}$ in $\mathbb{N} \times \mathbb{N}$, per esempio quella che associa a $n \in \mathbb{N}$ la coppia $(n, 0)$.

relazione attraverso l'addizione $+_{\mathbb{N}}$ già definita su $\mathbb{N}$:

$$(a,b) \sim (c,d) \overset{def}{\Leftrightarrow} a +_{\mathbb{N}} d = b +_{\mathbb{N}} c$$

Esercizio 4.1. *Dimostrare che la relazione $\sim$ appena introdotta sulle coppie di naturali è di equivalenza.*

A questo punto possiamo definire $\mathbb{Z}$ come l'insieme quoziente $\mathbb{N}\times\mathbb{N}/_{\sim}$ e indicare con $[(a,b)]$ la classe di equivalenza di (a,b). Se ci pensiamo bene è quello che succede per i numeri razionali, i quali già dalla scuola superiore vengono presentati come insiemi di frazioni equivalenti. Indicando con F l'insieme delle frazioni:

$$F = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} | b \neq 0\}$$

e con $\sim$ la relazione di equivalenza su F definita da:

$$\underbrace{(a,b)}_{\frac{a}{b}} \sim_F \underbrace{(c,d)}_{\frac{c}{d}} \overset{def}{\Leftrightarrow} a \cdot d = b \cdot c$$

l'insieme $\mathbb{Q}$ dei numeri razionali è definito come l'insieme delle classi di equivalenza:

$$\mathbb{Q} = F/_{\sim_F}$$

Tornando a $\mathbb{Z}$, identificando $\mathbb{N}$ con le classi di equivalenza delle coppie (a,b) con $a \geq b$, si ha che $\mathbb{N} \subset \mathbb{Z}$[2].

Osserviamo che, a questo punto, si possono definire le operazioni in $\mathbb{Z}$ a partire da quelle definite in $\mathbb{N}$. L'idea per definirle è quella di considerare la coppia (a,b) proprio come $a-b$ e imporre che continuino a valere le proprietà che valevano in $\mathbb{N}$ (per esempio la distributiva):

Definizione 4.2. Dati $[(a,b)], [(c,d)] \in \mathbb{Z}$ definiamo **addizione** $+_{\mathbb{Z}}$ e **moltiplicazione** $\cdot_{\mathbb{Z}}$ a partire da addizione $+_{\mathbb{N}}$ e moltiplicazione $\cdot_{\mathbb{N}}$ di $\mathbb{N}$ come segue:

- **Addizione:** $[(a,b)] +_{\mathbb{Z}} [(c,d)] = [(a +_{\mathbb{N}} c, b +_{\mathbb{N}} d)]$.
- **Moltiplicazione:** $[(a,b)] \cdot_{\mathbb{Z}} [(c,d)] = [(a \cdot_{\mathbb{N}} c + b \cdot_{\mathbb{N}} d, a \cdot_{\mathbb{N}} d + b \cdot_{\mathbb{N}} c)]$.

Esercizio 4.3. *Dimostrare che addizione e moltiplicazione su $\mathbb{Z}$ sono ben definite, ovvero non dipendono dai rappresentanti delle classi $[(a,b)]$ e $[(c,d)]$ scelti.*

Esercizio 4.4. *Dimostrare che addizione e moltiplicazione su $\mathbb{Z}$ ristretti ad $\mathbb{N}$ (cioè alle coppie con primo elemento maggiore o uguale del secondo) coincidono con addizione e moltiplicazione su $\mathbb{N}$.*

Come conseguenza di questo possiamo indicare le operazioni su $\mathbb{N}$ e su $\mathbb{Z}$ con lo stesso simbolo omettendo il riferimento ad $\mathbb{N}$ e $\mathbb{Z}$.

Esercizio 4.5. *Dimostrare che addizione e moltiplicazione su $\mathbb{Z}$ godono delle proprietà associativa, commutativa, esistenza dell'elemento neutro ($[(0,0)]$ per la addizione e $[(1,0)]$ per la moltiplicazione, distributiva della moltiplicazione rispetto alla addizione.*

Esercizio 4.6. *Verificare che, l'argomentazione usata in $\mathbb{N}$ per dimostrare l'unicità degli elementi neutri di addizione e moltiplicazione continua a valere in $\mathbb{Z}$. Dunque gli elementi neutri di addizione e moltiplicazione in $\mathbb{Z}$ sono unici.*

[2]In pratica, possiamo considerare l'immagine della funzione da $\mathbb{N}$ in $\mathbb{Z}$ che ad ogni $n \in \mathbb{N}$ associa la classe $[(n,0)] \in \mathbb{Z}$.

In $\mathbb{Z}$ si può estendere anche l'ordinamento definito in $\mathbb{N}$:

Definizione 4.7. Dati $z_1, z_2 \in \mathbb{Z}$ si dice che z_1 è maggiore o uguale di z_2 e si scrive $z_1 \geq_{\mathbb{Z}} z_2$ se esiste $z \in \mathbb{N}$ tale che $z_1 = z_2 + z$.

Esercizio 4.8. *Dimostrare che $\geq_{\mathbb{Z}}$ è una relazione d'ordine su $\mathbb{Z}$ e che ristretta a $\mathbb{N}$ coincide con $\geq_{\mathbb{N}}$ di $\mathbb{N}$.*

Per concludere, e tornare alle notazioni più usuali con cui eravamo abituati a trattare gli interi, osserviamo che è possibile scegliere, per ogni classe di equivalenza che individua un intero, un ben preciso rappresentante. Dato l'elemento $[(a, b)]$ di $\mathbb{Z}$ se $a > b$ (ricordiamo che a, b sono numeri naturali) diremo che $[(a, b)]$ è un numero intero positivo e se $b > a$ diremo che $[(a, b)]$ è un numero intero negativo. In particolare nel primo caso (a, b) è equivalente a $(a - b, 0)$, dunque $[(a, b)] = [(a - b, 0)]$ ed indicheremo tale intero con $a - b$ e nel secondo caso (a, b) è equivalente a $(0, b - a)$ e indicheremo tale intero con il simbolo $-(b - a)$.

Esempio 4.9. La coppia di naturali $(5, 3)$ è equivalente, rispetto a $\sim$, alla coppia $(2, 0)$. Indicheremo la classe di equivalenza con il simbolo 2.

La coppia di naturali $(3, 5)$ è equivalente, rispetto a $\sim$, alla coppia $(0, 2)$. Indicheremo la classe di equivalenza con il simbolo -2.

Definizione 4.10. Dato $z \in \mathbb{Z}$ un elemento $w \in \mathbb{Z}$ tale che $z + w = 0$ si dice **inverso** di z rispetto alla addizione. Un elemento $q \in \mathbb{Z}$ tale che $z \cdot q = 1$ si dice **inverso** di z rispetto alla moltiplicazione. L'elemento z si dice **invertibile** per la addizione (moltiplicazione) se esiste un inverso per la addizione (moltiplicazione).

Esercizio 4.11. *Dimostrare che l'inverso di un intero per la addizione (per la moltiplicazione), nel caso esista è unico.*

Esercizio 4.12. *Dimostrare che ogni intero è invertibile per la addizione, mentre gli unici interi invertibili per la moltiplicazione sono 1 e -1 ed hanno come inverso rispettivamente 1 e -1 stessi.*

L'Esercizio 4.12 ci dice che in $\mathbb{Z}$, dati a, b qualsiasi, è sempre risolubile l'equazione $a + x = b$, mentre in $\mathbb{N}$ l'equazione è risolvibile se e solo se $b \geq a$.

Esercizio 4.13. *Dati $a, b \in \mathbb{Z}$, dimostrare che $a \cdot b = 0$ se e solo se $a = 0$ oppure $b = 0$.*

Esercizio 4.14 (Legge di cancellazione in $\mathbb{Z}$)**.** *Dimostrare che dati $a, b, c \in \mathbb{Z}$ con $c \neq 0$, $a \cdot c = b \cdot c$ se e solo se $a = b$.*

Esercizio 4.15. *Dati a, b in $\mathbb{Z} \setminus \{0\}$, dimostrare che $a = a \cdot b$ se e solo se $b = 1$.*

Osservazione 4.16. Si potrebbe pensare che non ci sia bisogno di dimostrare quanto chiesto, in quanto sappiamo dall'Esercizio 4.6 che l'elemento neutro della moltiplicazione è unico e che è 1. In questo caso però stiamo dicendo qualcosa di diverso, ovvero che l'unico elemento che lascia fisso un qualsiasi elemento di $\mathbb{Z} \setminus \{0\}$ (e non tutti) rispetto alla moltiplicazione è 1.

2. La divisione euclidea, il massimo comun divisore e il minimo comun multiplo tra interi

Abbiamo visto che in $\mathbb{Z}$ è possibile trovare l'inverso rispetto alla addizione di qualsiasi elemento: questo permette di definire la differenza su $\mathbb{Z}$. Non è possibile

invece definire l'operazione di divisione su $\mathbb{Z}$: si può effettuare tra a e b solo se a è un multiplo di b.

Quello che possiamo fare però è definire l'algoritmo di divisione con resto che, dati due interi a e b, restituisce un quoziente e un resto con le proprietà descritte dal seguente teorema.

Teorema 4.17 (Divisione con resto o euclidea)**.** *Dati $a, b \in \mathbb{Z}$ con $b \neq 0$, esistono e sono unici due interi q, r tali che:*

$$a = q \cdot b + r, \quad 0 \leq r < |b|$$

Dimostrazione. **Esistenza.** Consideriamo la progressione geometrica infinita di termine iniziale a e ragione b: $A = \{a - x \cdot b | x \in \mathbb{Z}\}$. Sia $S = A \cap \mathbb{N}$. Abbiamo già mostrato (Teorema 2.36) che esiste r minimo di S della forma $a - q \cdot b$ per un certo $q \in \mathbb{Z}$. Resta da provare che r è minore di $|b|$. Se r fosse maggiore o uguale di $|b|$, allora $r - |b|$ sarebbe un elemento di S minore di r, assurdo perché r è il minimo di S.

Unicità. Supponiamo che esistano $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ con $r_1 \geq r_2$ tali che:

$$\begin{aligned} a &= q_1 \cdot b + r_1 \quad 0 \leq r_1 < |b| \\ a &= q_2 \cdot b + r_2 \quad 0 \leq r_2 < |b| \end{aligned}$$

Possiamo dunque scrivere $q_1 \cdot b + r_1 = q_2 \cdot b + r_2$, e, portando a primo membro i termini con b e raccogliendo a fattore b stesso ottenere $b(q_2 - q_1) = r_1 - r_2$. Da questo segue che $|b||q_2 - q_1| = |r_1 - r_2|$. A questo punto, sapendo che $|b| > r_1 \geq r_2 \geq 0$, abbiamo in particolare che $|b| > r_1 - r_2 \geq 0$, ovvero $|b| > |r_1 - r_2|$ (abbiamo solo usato il fatto che essendo $r_1 - r_2 \geq 0$ è uguale al suo valore assoluto).

Ora se q_2 fosse diverso da q_1 allora $|b||q_2 - q_1|$ sarebbe maggiore di $|b|$ (in quanto la differenza in valore assoluto tra due numeri interi è maggiore o uguale a 1), ma questo non può essere perché abbiamo osservato che $|r_1 - r_2| < |b|$. Dunque necessariamente $q_1 = q_2$ da cui $r_1 - r_2 = 0$ e quindi $r_1 = r_2$. □

Esempio 4.18. Se a e b sono rispettivamente -16 e -3, allora i q, r del Teorema 4.17 sono $q = 6$ e $r = 2$: $-16 = 6 \cdot (-3) + 2$.

Ricordando la definizione di divisore data nel caso generale per un insieme A su cui sia definita un'operazione $*$, si introduce la definizione di divisore in $\mathbb{Z}$ riferendosi all'operazione di moltiplicazione tra interi.

Definizione 4.19. Dati a, b in $\mathbb{Z}$ si dice che a **divide** b (o equivalentemente b è **multiplo** di a) se e solo se esiste c in $\mathbb{Z}$ tale che $b = a \cdot c$. Nel caso che a divida b, talvolta useremo la notazione $\dfrac{b}{a}$ per indicare il c tale che $b = a \cdot c$.

Corollario 4.20. *Siano a, b in $\mathbb{Z}$. a divide b se e solo se il resto della divisione euclidea di b con a è zero.*

Dimostrazione. Segue dal Teorema 4.17. □

Osservazione 4.21. Lo 0 divide solo se stesso, infatti, per ogni c in $\mathbb{Z}$, si ha $c \cdot 0 = 0$. Viceversa ogni intero z è divisore dello zero, infatti basta scegliere l'intero $c = 0$ per avere $0 = c \cdot z$.

Notiamo inoltre che -1 e 1 sono divisori di ogni numero intero z, infatti, scegliendo rispettivamente $c_1 = -z$ e $c_2 = z$, si ottiene $z = -1 \cdot c_1$ e $z = 1 \cdot c_2$.

Proposizione 4.22. *Siano $a, b, c \in \mathbb{Z}$. Se c divide sia a che b, allora divide una qualsiasi loro combinazione lineare (ovvero ogni intero della forma $k \cdot a + h \cdot b$ con k, h interi).*

DIMOSTRAZIONE. Per ipotesi esistono s, t tali che $a = s \cdot c$ e $b = t \cdot c$, quindi $k \cdot a + h \cdot b = h \cdot s \cdot c + k \cdot t \cdot c$ e raccogliendo c possiamo scrivere la combinazione lineare di a e b come $c \cdot (h \cdot s + k \cdot t)$. □

Osservazione 4.23. La relazione di divisibilità sugli interi non è una relazione totale in quanto esistono coppie di interi a, b per cui non vale né che $a|b$ né che $b|a$ (ad esempio $a = 5$, $b = 21$).

Bisogna stare attenti anche al fatto che solitamente la relazione di divisibilità, e le definizioni di divisore e multiplo incontrate a scuola, sono state introdotte nei numeri naturali e in $\mathbb{N}$ hanno proprietà che non hanno nel caso degli interi. Ad esempio il fatto che un multiplo b di a debba essere più grande o uguale di a, vera nell'insieme dei naturali, ovviamente non vale nell'insieme dei numeri interi ($5|-15$ ma $5 > -15$).

Quanto osservato in 4.23, come mostrato dalla prossima proposizione, non è la sola differenza tra la divisibilità in $\mathbb{Z}$ e quella in $\mathbb{N}$.

Proposizione 4.24. *La relazione di divisibilità sugli interi gode delle proprietà riflessiva e transitiva ma non della proprietà antisimmetrica, dunque non definisce un ordinamento su $\mathbb{Z}$.*

DIMOSTRAZIONE. La validità della proprietà riflessiva di $|$ segue dal fatto che, per ogni $a \in \mathbb{Z}$, si ha $a \cdot 1 = a$, perciò $a \mid a$. Per la transitività basta osservare che l'ipotesi $a|b$ e $b|c$ equivale a dire che esistono $h, k \in \mathbb{Z}$ tali che $b = a \cdot h$ e $c = b \cdot k$, dunque:

$$c = (a \cdot h) \cdot k \underbrace{=}_{prop.assoc.} a \cdot (h \cdot k)$$

Supponiamo adesso che a, b siano interi non nulli tali che a divide b e b divide a. Questo equivale al fatto che esistono $h, k \in \mathbb{Z}$ con $b = h \cdot a$ e $a = k \cdot b$, da cui $b = h \cdot k \cdot b$ ovvero $b \cdot (1 - h \cdot k) = 0$. Essendo $b \neq 0$ questo implica $h \cdot k = 1$, e dall'Esercizio 4.12 segue che può essere $k = h = 1$ ovvero $a = b$, ma anche $k = h = -1$, ovvero $a = -b$. Abbiamo cioè trovato che se a divide b e b divide a allora $a = \pm b$ (e non necessariamente $a = b$, come vorrebbe la proprietà antisimmetrica). □

Osservazione 4.25. Se b è un intero diverso da zero allora l'insieme dei suoi divisori è finito.

Definizione 4.26. Siano $a, b \in \mathbb{Z}$ non entrambi nulli[3], $d \in \mathbb{Z}$ si dice **un massimo comun divisore** di a e b se:

- d divide sia a che b.
- Per ogni c in $\mathbb{Z}$ che divide sia a che b, si ha che c divide d.

Proposizione 4.27. *Siano a, b interi non entrambi nulli. Se esiste $d = (a, b)$, allora tutti e soli i massimi comun divisori di a, b sono d e $-d$.*

[3]Osserviamo che, se a, b fossero entrambi nulli, l'insieme dei divisori comuni di a e b coinciderebbe con $\mathbb{Z}$.

DIMOSTRAZIONE. Abbiamo già osservato, dimostrando che | non è antisimmetrica, che se d divide d' e d' divide d allora $d = d'$ oppure $d = -d'$. Quindi se d è un massimo comun divisore, solo $-d$ può essere un massimo comun divisore diverso da d. È facile provare che (e lo lasciamo per esercizio), se d è massimo comun divisore, allora effettivamente anche $-d$ lo è sempre. □

Stabiliamo per convenzione di chiamare **il** massimo comun divisore tra a e b il valore positivo tra d e $-d$. Con questa convenzione abbiamo appunto l'unicità del massimo comun divisore tra due numeri e possiamo parlare **del** massimo comun divisore (e useremo la notazione (a, b) per indicarlo). Inoltre abbiamo che un divisore comune d di a, b è massimo comun divisore (secondo la Definizione 4.26) se e solo se è il massimo di tutti i divisori comuni.

Esercizio 4.28. *Dimostrare che d divisore comune di a e b (non entrambi nulli) è uguale a (a, b) se e solo se per ogni divisore comune c di a e b si ha $c \leq d$.*

A questo punto ci chiediamo per quali coppie di interi a, b non nulli esiste il massimo comun divisore. Il teorema seguente fornisce una risposta definitiva alla questione, inoltre, la dimostrazione dello stesso, suggerisce una interessante caratterizzazione di massimo comun divisore tra due numeri interi come minimo di un particolare insieme.

Teorema 4.29. *Per ogni $a, b \in \mathbb{Z}$ non entrambi nulli esiste (a, b).*

DIMOSTRAZIONE. Dati $a, b \in \mathbb{Z}$ non entrambi nulli, consideriamo l'insieme delle combinazioni a coefficienti interi di a, b positive, ovvero:

$$S = \{a \cdot m + b \cdot n | m, n \in \mathbb{Z} \text{ e } a \cdot m + b \cdot n > 0\}$$

Essendo a, b non entrambi nulli S non è vuoto, infatti se $a \neq 0$ basta considerare $m = a$ e $n = 0$ per avere $a \cdot m + b \cdot n = a^2 > 0$ e se $a = 0$ basta prendere m qualsiasi e $n = b$. Per l'assioma del buon ordinamento S ha un minimo d che sarà quindi un elemento della forma $a \cdot k + b \cdot h$ con k, h interi. Vogliamo dimostrare che d è il massimo comun divisore tra a e b.

Proviamo che d divide a. Effettuiamo la divisione euclidea tra a e d e troviamo $q, r \in \mathbb{Z}$ tali che $a = q \cdot d + r$ e $0 \leq r < d$. Sostituendo l'espressione di d in termini di a e b si ottiene $a = q \cdot (a \cdot k + b \cdot h) + r$, da cui si può ricavare r: $r = a(1 - q \cdot k) - b \cdot (h \cdot q)$. Ora, se r fosse diverso da zero, apparterrebbe a S e sarebbe minore del minimo d, dunque $r = 0$. Ma $r = 0$ significa proprio che d divide a. Analoga dimostrazione prova che d divide b e quindi che è un divisore comune di a e b.

Sia c un divisore comune di a e b, ovvero esistono w, z interi tali che $a = c \cdot w$ e $b = c \cdot z$, allora si ha $d = a \cdot k + b \cdot h = c \cdot w \cdot k + c \cdot z \cdot h$ e, raccogliendo c, $d = c \cdot (w \cdot k + z \cdot h)$. Cioè c divide d. □

Dalla dimostrazione del Teorema 4.29, avendo caratterizzato il massimo comun divisore tra a e b come il minimo delle combinazioni a coefficienti intere positive di a e b, segue immediatamente il seguente importante risultato.

Corollario 4.30 (Identità di Bézout)**.** *Dati a, b interi non entrambi nulli esistono k, h interi tali che:*

$$(a, b) = a \cdot k + b \cdot h$$

Esercizio 4.31. *Siano a, b interi non entrambi nulli. Dimostrare che $(a, b) = a$ se e solo se $a \mid b$.*

Esercizio 4.32. *Siano a, b interi non entrambi nulli, dimostrare che $(a, b) = (|a|, |b|)$.*

Definizione 4.33. Due numeri interi a e b non entrambi nulli si dicono **relativamente primi** o anche **coprimi** se $(a, b) = 1$.

Esercizio 4.34. *Siano a, c, b interi con $(a, c) = 1$ e c che divide $a \cdot b$. Provare che c divide b.*

Svolgimento. Per ipotesi esiste $z \in \mathbb{Z}$ tale che $a \cdot b = c \cdot z$. L'identità di Bézout ci dice che esistono h, k interi tali che $a \cdot k + c \cdot h = 1$. Moltiplicando entrambi i membri di questa identità per b otteniamo: $a \cdot b \cdot k + c \cdot h \cdot b = b$. Da cui, sostituendo $c \cdot z$ con $a \cdot b$ $c \cdot z \cdot k + c \cdot h \cdot b = b$. Ora, raccogliendo c, si ottiene la tesi.

Osservazione 4.35. Osserviamo che, nell'Esercizio 4.34, l'ipotesi che a e c siano coprimi è necessaria. L'idea del teorema è che non avendo fattori in comune a e c, e con c che divide $a \cdot b$, i fattori di c si "ritrovano" tutti in b. Quando invece a e c non sono coprimi, può essere che a e b singolarmente non siano divisi da c, ma il loro prodotto sì. Basta considerare ad esempio $c = 6$, $a = 2$ e $b = 9$.

Esercizio 4.36. *Siano $a, b, c \in \mathbb{Z}$ tali che $a \mid c$, $b \mid c$ e $(a, b) = 1$, provare che $(a \cdot b) \mid c$.*

Svolgimento. Per ipotesi esistono $r, s \in \mathbb{Z}$ tali che $c = a \cdot r$ e $c = b \cdot s$. In particolare $b \mid a \cdot r$ e dall'Esercizio 4.34 segue che $b \mid r$. Ovvero esiste $k \in \mathbb{Z}$ tale che $r = b \cdot k$, dunque $c = a \cdot r = a \cdot b \cdot k$. Cioè $a \cdot b \mid c$.

Esercizio 4.37. *Siano $a, b \in \mathbb{Z}$ non entrambi nulli e $d = (a, b)$. Allora:*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Svolgimento. Per ipotesi esistono $a_1, b_1 \in \mathbb{Z}$ tali che $a = d \cdot a_1$ e $b = d \cdot b_1$. Indichiamo con h il massimo comun divisore tra a_1 e b_1: vogliamo provare che $h = 1$. Per definizione di massimo comun divisore esistono $a_2, b_2 \in \mathbb{Z}$ tali che $a_1 = h \cdot a_2$ e $b_1 = h \cdot b_2$ da cui $a = d \cdot h \cdot a_2$ e $b = d \cdot h \cdot b_2$. Quindi $d \cdot h$ è un divisore comune di a e b e perciò deve dividere il massimo comun divisore tra a e b che è d ($d \cdot h \mid d$). Questo implica $h = 1$ (ricordiamo che h è maggiore di zero, altrimenti la relazione precedente potrebbe implicare anche $h = -1$).

Definizione 4.38. Siano $a, b \in \mathbb{Z}$ non entrambi nulli, $m \in \mathbb{Z}$ si dice **un minimo comun multiplo** di a e b se:

- m è un multiplo sia di a che di b.
- Per ogni c in $\mathbb{Z}$ multiplo sia di a e di b, si ha che m divide c.

Esercizio 4.39. *Dimostrare che per ogni coppia di interi a, b non entrambi nulli, esiste un minimo comun multiplo.*

Esercizio 4.40. *Se m è un minimo comun multiplo tra a e b allora anche $-m$ lo è, e non ci sono altri minimi comun multipli di a, b diversi da m e $-m$.*

Stabiliamo per convenzione che **il** minimo comun multiplo, che indicheremo con $[a, b]$, è il valore maggiore di zero tra m e $-m$. Una interessante proprietà che lega il massimo comun divisore e il minimo comun multiplo è la seguente:

Proposizione 4.41. *Per ogni $a, b \in \mathbb{Z}$ non entrambi nulli si ha*

$$[a, b] \cdot (a, b) = a \cdot b$$

DIMOSTRAZIONE. Sia $d = (a, b)$, allora esistono $a_1, b_1 \in \mathbb{Z}$ tali che $a = d \cdot a_1$, $b = d \cdot b_1$. Dall'Esercizio 4.37 sappiamo che $(a_1, b_1) = 1$. Vogliamo provare che $[a, b]$ è uguale a $fraca \cdot bd$, che indichiamo con h:

$$h = \frac{a_1 \cdot d \cdot b_1 \cdot d}{d} = a_1 \cdot b_1 \cdot d$$

Osserviamo che h è multiplo di $a = a_1 \cdot d$ e $b = b_1 \cdot b$, mostriamo adesso che per ogni intero t multiplo comune di a e b si ha che $h \mid t$. Essendo la relazione di divisibilità $\mid$ transitiva da $d \mid a$ e $a \mid t$ segue che $d \mid t$ ovvero che esiste $t_1 \in \mathbb{Z}$ tale che $t = d \cdot t_1$. Ora $a \mid t$ equivale a $a_1 \cdot d \mid t_1 \cdot d$, ovvero $a_1 \mid t$ e analogamente $b_1 \mid t$. Dall'Esercizio 4.36 segue che $a_1 \cdot b_1 | t_1$ e questo implica che $h = a_1 \cdot b_1 \cdot d$ divide $t_1 \cdot d = t$. □

3. I numeri primi e la ϕ di Eulero

Diamo di seguito le due definizioni distinte, nell'insieme $\mathbb{Z}$ degli interi, di numero primo e numero irriducibile e dimostriamo che in realtà sono equivalenti, cioè che da una si ricava l'altra come conseguenza e viceversa.

Definizione 4.42. Un numero $p \in \mathbb{Z}$, $p \neq 0, 1, -1$ si dice **primo** se $p|ab$ implica che $p|a$ o $p|b$.

Definizione 4.43. Un numero $p \in \mathbb{Z}$, $p \neq 0, 1, -1$ si dice **irriducibile** se i suoi unici divisori sono ± 1 e $\pm p$.

Proposizione 4.44. *Un numero $p \in \mathbb{Z}$ è primo se e solo se è irriducibile (ovvero le definizioni 4.42 e 4.43 sono equivalenti).*

DIMOSTRAZIONE. $\Rightarrow$) Siano p primo e d un divisore di p, questo significa che esiste $c \in \mathbb{Z}$ tale che $p = d \cdot c$. In particolare $p \mid d \cdot c$, dunque, per definizione di numero primo, o $p \mid d$ oppure $p \mid c$. Nel primo caso, dalla dimostrazione della Proposizione 4.24, segue che $d = \pm p$; nel secondo caso esiste h intero tale che $c = h \cdot p$. Ovvero $c = h \cdot d \cdot c$. Dall'Esercizio 4.15 segue che $h \cdot d = 1$ ovvero $d = \pm 1$.

$\Leftarrow$) Sia p irriducibile e supponiamo che $p \mid a \cdot b$. Dalla definizione di irriducibilità segue che (a, p) è uguale a p o a 1 (il massimo comun divisore deve essere un divisore comune, e p e 1 sono gli unici divisori di p). Nel primo caso $p \mid a$, nel secondo, dall'Esercizio 4.34 segue che $p \mid b$. □

Osservazione 4.45. $n \in \mathbb{N}$ è primo se e solo se ha esattamente due divisori distinti in $\mathbb{N}$.

Esercizio 4.46. *Siano $n > 2$, p primo, $a_1, \ldots, a_n \in \mathbb{Z}$. Supponiamo $p| \prod_{i=1}^{n} a_i$, allora esiste $1 \leq i \leq n$ tale che $p|a_i$.*

Suggerimento: procedere per induzione sul numero n di fattori.

Solitamente per insieme dei numeri primi (senza nessun'altra specificazione) si intende il sottoinsieme di $\mathbb{Z}$ degli elementi primi positivi. Nonostante che tutto possa essere generalizzato a primi in $\mathbb{Z}$ secondo la definizione data, da ora in poi quando parleremo di primi, senza ulteriori specifiche, intenderemo primi positivi (ovvero in $\mathbb{N}$).

Iniziamo con un risultato così importante da essere chiamato teorema fondamentale dell'aritmetica.

Teorema 4.47 (Teorema fondamentale dell'aritmetica)**.** *Sia $n \in \mathbb{N}$ maggiore di 1, allora n si scrive in modo unico (a meno dell'ordine) come prodotto di fattori primi.*

Il teorema in questa forma considera come prodotto di primi anche il prodotto di un solo primo, potremmo riformularlo dicendo $n > 1$ è primo o si scrive in modo unico come prodotto di primi, ma in matematica usualmente si preferiscono gli enunciati *compatti*, con meno eccezioni possibili.

Dimostrazione. **Esistenza.** Procediamo per induzione su n.
Passo base. Se $n = 2$, allora n è primo e quindi verifica l'enunciato.
Passo induttivo. Supponiamo la tesi vera per ogni $k < n$ e dimostriamo che questo implica che n è primo o prodotto di primi. Se n è primo non c'è niente da dimostrare, se n non è primo, per l'equivalenza con l'irriducibilità, n si scompone in $a \cdot b$ con $1 < a < n$ e $1 < b < n$. Per ipotesi induttiva sia a che b si scrivono come prodotto di primi:

$$a = \prod_{i=1}^{k} p_i \quad b = \prod_{j=1}^{h} q_j$$

Dunque n sarà il prodotto dei p_i e q_j:

$$n = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_h$$

Unicità. Nell'insieme di tutte le fattorizzazioni in primi di n (che sappiamo non essere vuoto perché abbiamo appena provato l'esistenza di una fattorizzazione per tutti gli n maggiori di 1) sia k il numero minimo di fattori che compongono queste fattorizzazioni. Supponiamo dunque che esista una fattorizzazione $n = \prod_{i=1}^{k} p_i$ e che ne esista anche un'altra $n = \prod_{j=1}^{h} q_j$ con p_i e q_j primi e $h \geq k$ (k è il minimo). Per mostrare che in realtà esiste un'unica fattorizzazione procediamo per induzione su k.
Passo base. Se $k = 1$, si ha $n = p_1 = \prod_{j=1}^{h} q_j$, allora dall'Esercizio 4.46 sappiamo che esiste $1 \leq t \leq h$ tale che $p_1 | q_t$. Per definizione di primo questo implica che $p_1 = q_t$ e dunque che $\prod_{j \neq t} q_j = 1$. Ma questa identità in $\mathbb{N}$ ha come unica soluzione $q_j = 1$ per ogni $j \neq t$, dunque $h = 1$ (perché $q_j = 1$ non è primo per definizione) e la fattorizzazione è unica in questo caso.
Passo induttivo. Supponiamo che tutti i naturali che ammettono una fattorizzazione con meno di k primi abbiano un'unica fattorizzazione e consideriamo n che ha k come minimo numero di fattori nelle sue fattorizzazioni in primi. Da $n = \prod_{i=1}^{k} p_i = \prod_{j=1}^{h} q_j$ segue che p_k divide $\prod_{j=1}^{h} q_j$. Analogamente a quanto detto precedentemente, questo equivale al fatto che esiste t ($1 \leq t \leq h$) tale che $p_k = q_t$.

Consideriamo adesso $m = \frac{n}{p_k} = \prod_{i=1}^{k-1} p_i = \prod_{j \neq t} q_j$. Per ipotesi induttiva m ha un'unica fattorizzazione come prodotto di primi e di conseguenza $k = h$, inoltre, per ogni i ($1 \leq i < k$), esiste j ($j \in \mathbb{N}_h$ e $j \neq t$) tale che $p_i = q_j$. □

Useremo spesso la notazione $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ per indicare la fattorizzazione in primi di un generico n. In questa notazione usualmente i p_i rappresentano primi distinti, dunque k è il numero di primi distinti presenti nella fattorizzazione, gli α_i (appartenenti a $\mathbb{N}$) sono gli esponenti in cui i primi p_i compaiono nella fattorizzazione di n.

Esercizio 4.48. *Se t, s sono due numeri naturali e t divide s, allora tutti i primi che compaiono nella fattorizzazione in primi di t, compaiono anche nella fattorizzazione di s. Inoltre, se p è un primo in comune alle due fattorizzazioni,*

l'esponente di p nella fattorizzazione di t è minore o uguale all'esponente di p nella fattorizzazione di s.

Osservazione 4.49. Il viceversa dell'Esercizio 4.48, ovvero che se t e s sono due numeri naturali e nella fattorizzazione in primi di t compaiono solo primi presenti nella fattorizzazione in s, tutti con esponente non maggiore del corrispondente in s allora t divide s, è ovviamente vero, perché, per ipotesi, s si può scrivere come t per *quello che manca*.

Osservazione 4.50. In particolare, dall'Esercizio 4.48 segue che, se t divide s, possiamo pensare t e s come prodotto degli stessi primi. Se infatti la fattorizzazione di s è $s = \prod_{i=1}^{k} p_i^{\alpha_i}$, possiamo scrivere t come $t = \prod_{i=1}^{k} p_i^{\beta_i}$, ammettendo che i β_i possano essere anche nulli (perdendo dunque l'unicità della fattorizzazione, perché includiamo anche degli 1).

Esempio 4.51. Sia $t = 20$ e $s = 700$. La scomposizione in fattori primi di s è $s = 2^2 \times 5^2 \times 7^1$. Possiamo scrivere t come $t = 2^2 \times 5^1 \times 7^0$.

Trovare la scomposizione in fattori primi di un numero intero n è *computazionalmente* molto complicato[4]. D'altra parte la scomposizione in fattori primi, se conosciuta, fornisce molte indicazioni importanti.

Proposizione 4.52 (Numero di divisori positivi)**.** *Sia $n > 1$ un intero di cui conosciamo la scomposizione in primi $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Allora il numero di divisori positivi di n è $\prod_{i=1}^{k}(\alpha_i + 1)$.*

Dimostrazione. Abbiamo visto (Esercizio 4.48) che un numero naturale h divide n se e solo se $h = \prod_{i=1}^{k} p_i^{\beta_i}$, con $0 \leq \beta_i \leq \alpha_i$. Dunque il numero di divisori di n è uguale al numero di stringhe $(\beta_1, \ldots, \beta_k)$ differenti. Visto che le possibili scelte per ogni β_i sono $\alpha_i + 1$, il numero di divisori positivi di n è proprio $\prod_{i=1}^{k}(\alpha_i + 1)$. □

Osservazione 4.53. Dalla Proposizione 4.52 segue che, se conosciamo la scomposizione in fattori primi di due numeri naturali m e n, allora il loro massimo comun divisore è il numero che si ottiene moltiplicando tra loro i fattori primi in comune tra m e n presi con l'esponente minore.

Esempio 4.54. Consideriamo $n = 3^5 \cdot 5^2 \cdot 11^2$ e $m = 2^4 \cdot 5 \cdot 11^7 \cdot 19$. Il massimo comun divisore tra n e m è $(n, m) = 5 \cdot 11^2$.

Esercizio 4.55. *Dati a, b, c interi, provare che c è coprimo con a e con b se e solo se è coprimo con $a \cdot b$.*

Svolgimento. Se c ha un fattore in comune maggiore di 1 con a o con b allora evidentemente ha un fattore in comune con $a \cdot b$. Dunque se $(a \cdot b, c) = 1$ allora $(a, c) = (b, c) = 1$.

Viceversa supponiamo che $(a \cdot b, c) = d > 1$, allora d si scompone in fattori primi. Sia p uno di tali fattori: da d divide $a \cdot b$ e d divide c segue che p è un fattore comune (maggiore di 1) di $a \cdot b$ e c. Per definizione di primo p divide $a \cdot b$ implica che p divide a o b ma entrambe le possibilità contraddicono l'ipotesi perché p sarebbe un fattore comune maggiore di 1 di a e c oppure di a e b. Dunque d deve essere uguale a 1.

[4] I metodi crittografici moderni si basano proprio sul fatto che moltiplicare tra loro numeri primi grandi è *poco costoso*, ma ritrovare i numeri primi a partire dal loro prodotto è *molto difficile*.

Conoscere la fattorizzazione in primi di un numero intero n maggiore di 1, vedremo tra poco, permette di calcolare quanti sono i numeri in $\mathbb{N}_n$ coprimi con n.

Definizione 4.56 (funzione ϕ di Eulero)**.** La funzione $\phi : \mathbb{N} \setminus \{0,1\} \longrightarrow \mathbb{N}$ che ad ogni naturale n maggiore di 1 associa la cardinalità dell'insieme:

$$\{m \in \mathbb{N}_n | (m,n) = 1\}$$

è detta **funzione ϕ di Eulero**.

Esempio 4.57. $\phi(10) = 4$, infatti i numeri coprimi con 10 in $\mathbb{N}_{10}$ sono $1, 3, 5, 7$. $\phi(6) = 2$ infatti, tra i numeri naturali compresi tra 1 e 6, solo 1 e 5 sono coprimi con 6.

Come anticipato, vediamo ora come la conoscenza della scomposizione in fattori primi di un intero n maggiore di 1, permetta di calcolare $\phi(n)$.

Esercizio 4.58. *Se p è primo allora $\phi(p) = p - 1$.*

Osserviamo inoltre che, l'Esercizio 4.55 *riletto* in termini di funzione di Eulero, ci dice che, se m e n sono interi maggiori di 1 e coprimi, allora:

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n)$$

Da questa osservazione segue che, se troviamo una formula per calcolare la ϕ di Eulero per numeri della forma p^k con p primo e $k \in \mathbb{N}^+$, allora per ogni m intero maggiore di 1 di cui conosciamo la fattorizzazione in primi distinti sappiamo calcolare $\phi(m)$.

Lemma 4.59. *Sia p primo e $k \in \mathbb{N}^+$, allora:*

$$\phi(p^k) = (p-1) \cdot p^{k-1}$$

Dimostrazione. Sia $a \in \mathbb{N}$ minore o uguale di p^k. a e p^k hanno un fattore in comune se e solo se p è un fattore di a, ovvero p divide a. Dunque gli $a \leq p^k$ non coprimi con p^k sono della forma $p \cdot t$ con $t \in \mathbb{N}$ che varia da 1 a p^{k-1}, ovvero in tutto sono p^{k-1}. Quindi:

$$\phi(p^k) = |\{n \in \mathbb{N} | 1 \leq n \leq p^k\}| - |\{p \cdot t | 1 \leq t \leq p^{k-1}\}| = p^k - p^{k-1}$$

□

A questo punto, mettendo insieme tutti i risultati trovati, possiamo enunciare il teorema per il calcolo della funzione di Eulero a partire dalla fattorizzazione in primi.

Teorema 4.60. *Sia m un intero maggiore di 1. Se la fattorizzazione in primi distinti di m è $\prod_{i=1}^{k} {p_i}^{\alpha_i}$ allora:*

$$\phi(m) = \prod_{i=1}^{k} ({p_i}^{\alpha_i} - {p_i}^{\alpha_i - 1}) = m \cdot \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

Cominciamo ad intuire l'importanza dei numeri primi, sorge dunque abbastanza spontaneo chiedersi se l'insieme dei numeri primi sia finito o meno. La risposta a questo quesito era nota più di 2000 anni fa: Euclide diede una dimostrazione dell'infinità dei primi ancora oggi considerata un capolavoro per la genialità dell'idea e la semplicità degli strumenti usati.

Teorema 4.61 (Teorema d'Euclide)**.** *Esistono infiniti numeri primi.*

DIMOSTRAZIONE. Supponiamo che l'insieme dei primi $P = \{p_1, \ldots, p_n\}$ sia finito e consideriamo il numero $N = (\prod_{i=1}^{n} p_i) + 1$. Tale numero è maggiore di 1 dunque, per il teorema fondamentale dell'aritmetica, o N è primo o è diviso da qualche primo (in quanto è prodotto di primi). Osserviamo che N è strettamente maggiore di tutti i p_i, dunque N non appartiene a P e non può essere primo, d'altra parte N non è multiplo di nessun p_i di P in quanto, per come è definito, il resto della divisione euclidea di N con qualsiasi p_i di P è sempre 1. Dunque l'assunzione P insieme dei primi finito, porta ad un assurdo. □

Pur essendo infiniti i numeri primi sembrano susseguirsi in modo del tutto casuale. Molti sono stati i tentativi infruttuosi di trovare successioni che avessero come valori solo numeri primi. Uno di questi tentativi piuttosto famoso è quello di Fermat che ipotizzò che i numeri della forma $2^{2^n}+1$ (che vengono chiamati **numeri di Fermat**) al variare di n tra i naturali fossero tutti primi. Sfortunatamente Eulero mostrò che, già per $n = 5$, si ottiene un numero molto grande 4294967297 che è scomponibile in 641 per 6700417, quindi non primo. Un aspetto interessante è che da allora non si è ancora trovato un numero di Fermat, con $n \geq 5$, che sia primo ed oggi la congettura di Fermat è stata completamente *ribaltata*: si suppone che per $n > 4$ nessun numero di Fermat sia primo. I numeri di Fermat hanno una loro importanza anche perché Gauss mostrerà un inaspettato legame tra essi e la possibilità di costruire poligoni regolari utilizzando riga e compasso.

Un altro tentativo interessante alla ricerca di una successione di interi primi, fu quello portato avanti da Padre Marin Mersenne (1588-1648). Mersenne, frate dell'ordine dei Minimi, attraverso una fitta rete di contatti epistolari tra gli studiosi dell'epoca, fu un importante divulgatore della conoscenza scientifica. Mersenne si incuriosì, anche per motivi religiosi, ai cosiddetti numeri perfetti, definiti nel Libro VII degli Elementi di Euclide (definizione nr. 23) come segue: "il numero perfetto è quello uguale alle sue parti".

Definizione 4.62. Un numero naturale a si dice **perfetto** se è uguale alla somma dei suoi divisori minori di a o, equivalentemente, se la somma di tutti i suoi divisori è uguale a $2a$.

Osservando i primi numeri perfetti si possono notare alcune regolarità. Consideriamo ad esempio gli unici 4 numeri perfetti minori di 10000: $6, 28, 498, 8128$. Sono tutti

N	$6 = 2 \cdot 3$	$28 = 2^2 \cdot 7$	$498 = 2^4 \cdot 31$	$8128 = 2^6 \cdot 127$
Somma esponenti	$1 + 1 = 2$	$2 + 1 = 3$	$4 + 1 = 5$	$6 + 1 = 7$
Fattore dispari $+1$	$3 + 1 = 2^2$	$7 + 1 = 2^3$	$31 + 1 = 2^5$	$127 + 1 = 2^7$

Abbiamo dunque che i primi 4 perfetti sono della forma $2^{p-1} \cdot (2^p - 1)$ con p primo. Se proviamo con $p = 11$ otteniamo un numero che non è perfetto, ma si può notare che $2^{11} - 1$ non è primo (è $23 \cdot 89$), mentre nei primi 4 numeri perfetti non solo p era primo, ma lo è anche $2^p - 1$.

Che un numero della forma $2^{p-1} \cdot (2^p - 1)$, con p e $2^p - 1$ primi, fosse perfetto era già noto ai tempi di Euclide. Nella Proposizione 36, del IX Libro degli Elementi si trova: "Se a partire dall'unità, si prende un numero a piacere di numeri successivamente proporzionali in ragione doppia, fino a che la loro somma sia un numero primo, il prodotto di tale somma per l'ultimo numero sarà un numero perfetto". Circa 2000 anni dopo, Eulero dimostra che se un numero pari è perfetto deve essere della forma citata.

Teorema 4.63. *Un numero pari n è perfetto se e solo se è della forma $2^{p-1} \cdot (2^p - 1)$ con p e $(2^p - 1)$ primi.*

DIMOSTRAZIONE. $\Leftarrow$) Se n è della forma $2^{p-1} \cdot (2^p - 1)$, e indichiamo con q il fattore dispari $2^p - 1$, allora i $2p$ divisori di n sono della forma $2^i \cdot q$ o della forma 2^i con $0 \leq i \leq p-1$. Consideriamo la somma S dei divisori di n della forma 2^i:

$$S = \sum_{i=0}^{p-1} 2^i = 2S - S = 2^p - 1 = q$$

Dunque la somma di tutti i divisori di n è:

$$\sum_{i=0}^{p-1} 2^i + \sum_{i=0}^{p-1} 2^i \cdot q = \underbrace{\sum_{i=0}^{p-1} 2^i}_{q} + q \cdot \underbrace{\sum_{i=0}^{p-1} 2^i}_{q} = q + q^2$$

Ora osserviamo che:

$$q + q^2 = q(q+1) = (2^p - 1)2^p = 2 \cdot 2^{p-1}(2^p - 1) = 2n$$

$\Rightarrow$) Sia $n = 2^{k-1}q$, con q dispari e $k > 1$ (in quanto n per ipotesi è pari), perfetto. Indichiamo con $\sigma(n)$ la funzione che ad un numero naturale n associa la somma dei divisori positivi di n.

Esercizio 4.64. *Dati $a, b \in \mathbb{N}$ con $(a, b) = 1$ si ha $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.*

Con la notazione introdotta, e per l'ipotesi n perfetto, si ha dunque:

$$2n = 2^k q = \sigma(n) = \sigma(2^{k-1}) \cdot \sigma(q)$$

Abbiamo già visto che $\sigma(2^{k-1})$ è uguale a $2^k - 1$, dunque:

$$\sigma(q) = \frac{\overbrace{2^k q}^{=2n}}{\underbrace{2^k - 1}_{=\sigma(2^{k-1})}} = \frac{(2^k - 1)q + q}{2^k - 1} = q + \frac{q}{2^k - 1}$$

Quanto trovato ci dice che:

- $2^k - 1$ divide q, in quanto $\sigma(q)$ è ovviamente un numero intero. Di conseguenza $\dfrac{q}{2^k - 1}$ è anch'esso un divisore di q.
- q e $\dfrac{q}{2^k - 1}$ sono gli unici divisori di q, in quanto $\sigma(q)$ per definizione è la somma dei divisori di q, ed essendo essi stessi divisori non ce ne possono essere altri.

Da questo segue che *a*) q è primo, *b*) $q = 2^k - 1$. Ci rimane da dimostrare che k è primo, e questo segue proprio da *a*) e *b*). Se infatti k non fosse primo, esisterebbero t, h naturali maggiori di 1 tali che $k = th$. Ma allora:

$$q = 2^k - 1 = 2^{th} - 1 = (2^h)^t - 1 = (2^h - 1) \underbrace{\sum_{i=0}^{t-1} (2^h)^i}_{=s}$$

con $2^h - 1$ e s entrambi maggiori di 1, e dunque q non sarebbe primo. Perciò k è un numero primo. □

Osservazione 4.65. Il Teorema 4.63 caratterizza i numeri perfetti pari, e quelli dispari? Non ne sono stati trovati, e la congettura di Sylvester (1814-1897) è che non ne esistano.

Mersenne studia i numeri della forma $2^p - 1$ con p primo, interessato a capire, per quanto visto sui numeri perfetti, quali di essi siano primi. Mersenne stila una lista (incompleta e con qualche errore) dei primi numeri della forma $2^p - 1$ con p primo che sono primi, e congettura che di tali numeri primi ce ne siano in quantità finita. Nonostante gli errori presenti nella sua lista, il lavoro di Mersenne è sicuramente ragguardevole per l'epoca (lavorando tra l'altro con numeri molto grandi senza l'aiuto di calcolatori), per questo i numeri della forma $2^p - 1$ con p primo, vengono ora chiamati **numeri di Mersenne**.

La cosa interessante è che non solo al giorno d'oggi la congettura sui numeri di Mersenne si è ribaltata (si pensa che i numeri di Mersenne primi siano infiniti), ma la ricerca di numeri primi *grandi* avviene attraverso la ricerca di numeri di Mersenne primi. Il GIMPS (Great Internet Mersenne Prime Search) si occupa proprio della *caccia* a numeri di Mersenne sempre più grandi.

4. Algoritmo di Euclide

Stabilito che il massimo comun divisore tra due interi a, b non entrambi nulli esiste sempre, e che trovare la fattorizzazione in primi è un compito difficile (a volte proibitivo), come si può fare a calcolare il massimo comun divisore senza passare dalla fattorizzazione di a e b? Per rispondere a questa domanda, cominciamo mostrando una semplice, ma significativa, proprietà del massimo comun divisore tra due numeri interi.

Proposizione 4.66. *Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Per ogni intero k si ha $(a, b) = (a, b - k \cdot a)$.*

Dimostrazione. Dimostreremo la proposizione facendo vedere che l'insieme dei divisori comuni di a e b, che indicheremo con T, è uguale all'insieme dei divisori comuni di a e $b - k \cdot a$ qualsiasi sia k, che indicheremo con R_k.

Sia $t \in T$, vogliamo mostrare che t divide a (lo sappiamo) e che t divide $b - k \cdot a$ qualsiasi sia k. Per ipotesi $t \mid a$ e $t \mid b$, cioè esistono $h, j \in \mathbb{Z}$ tali che $a = t \cdot h$ e $b = t \cdot j$. Quindi $b - k \cdot a = t \cdot j - k \cdot t \cdot h$, e raccogliendo a fattore t otteniamo che $b - k \cdot a$ è uguale a $t \cdot (j - k \cdot h)$. Cioè t appartiene ad R_k per ogni k. Abbiamo quindi che $T \subseteq R_k$.

Viceversa se $t \in R_k$, vogliamo far vedere che $t \in T$ cioè che $R_k \subseteq T$ e quindi concludere che $T = R_k$. Dobbiamo mostrare che da $t \mid a$ e $t \mid b - k \cdot a$ segue che $t \mid b$. Per ipotesi esistono $h, j \in \mathbb{Z}$ tali che $a = t \cdot h$ e $b - k \cdot a = t \cdot j$. Perciò $b = k \cdot a + t \cdot j = k \cdot t \cdot h + t \cdot j$, e raccogliendo t, si trova che b è uguale a t per un intero $(k \cdot h + j)$. □

Esercizio 4.67. *Calcolare al variare di $n \in \mathbb{Z}$, $(4n+3, 8n-5)$ e $(4n+2, 8n-16)$.*

Svolgimento. Dalla Proposizione 4.66 sappiamo che $(a, b) = (a, b - k \cdot a)$ per ogni k intero. Usiamo questa proprietà per trovare un massimo comun divisore (a, b) uguale a $(4n + 3, 8n - 5)$, ma con uno tra a e b non dipendente da n (e che quindi saremo in grado di fattorizzare):

$$(4n + 3, 8n - 5) = (4n + 3, 8n - 5 - 2 \cdot (4n + 3)) = (4n + 3, -11)$$

Ora i divisori positivi di -11 sono 1 e 11 perciò abbiamo due casi possibili:

$$\begin{cases} 4n+3 = 11 \cdot k \Rightarrow (4n+3, 8n-5) = 11 \\ \text{altrimenti} \Rightarrow (4n+3, 8n-5) = 1 \end{cases}$$

Concludendo possiamo dire che: se $4n+3$ è un multiplo di 11 allora il massimo comun divisore è 11, altrimenti è 1. Nel seguito riusciremo a stabilire per quali n in $\mathbb{Z}$ si ha che $4n+3$ è un multiplo di 11.

$$(4n+2, 8n-16) = (4n+2, 8n-16-2\cdot(4n+2)) = (4n+2, -20)$$

I divisori positivi di 20 sono 1, 2, 4, 5, 10 e 20 quindi la discussione è un po' più articolata di quella vista nel caso precedente:

$$\begin{cases} 4n+2 = 20 \cdot k \Rightarrow (4n+2, 8n-16) = 20 \\ 4n+2 = 10 \cdot k \text{ e } (2,k) = 1 \Rightarrow (4n+2, 8n-16) = 10 \\ 4n+2 = 5 \cdot k \text{ e } (4,k) = 1 \Rightarrow (4n+2, 8n-16) = 5 \\ 4n+2 = 4 \cdot k \text{ e } (5,k) = 1 \Rightarrow (4n+2, 8n-16) = 4 \\ 4n+2 = 2 \cdot k \text{ e } (10,k) = 1 \Rightarrow (4n+2, 8n-16) = 2 \\ \text{altrimenti} \Rightarrow (4n+2, 8n-16) = 1 \end{cases}$$

La Proposizione 4.66 è la chiave per definire un algoritmo per il calcolo del massimo comun divisore tra due interi. Per semplificare le notazioni, e visto l'Esercizio 4.32, definiremo l'algoritmo per coppie di numeri naturali. L'algoritmo, basato sulla ripetizione di divisioni euclidee, è noto come **algoritmo di Euclide**.

Teorema 4.68 (Algoritmo di Euclide)**.** *Dati a, b naturali non entrambi nulli, con $b \leq a$, per calcolare (a, b) si può procedere iterando i seguenti passaggi:*

(1) *Se $b = 0$ allora $(a, 0) = a$.*
(2) *Se $b \neq 0$ calcoliamo la divisione con resto tra a e b:*

$$a = b \cdot q_1 + r_1 \quad 0 \leq r_1 < b$$

(3) *Ripete la procedura dal punto (1) sostituendo b ad a e r_1 a b.*

Dimostrazione. In pratica l'algoritmo di Euclide è una successione di divisioni euclidee che termina al passo n quando il resto r_n della divisione euclidea è zero, e restituisce come massimo comun divisore tra a e b, l'ultimo resto non nullo (r_{n-1}). Dimostriamo che *i*) l'algoritmo di Euclide termina qualsiasi sia la coppia di naturali a, b non entrambi nulli; *ii*) effettivamente il risultato dell'algoritmo di Euclide è il massimo comun divisore tra a e b.
i) L'algoritmo termina qualsiasi sia la coppia a, b (diversa dalla coppia $(0, 0)$) di partenza, in quanto la successione dei resti r_n delle divisione euclidee, è una successione decrescente di numeri naturali, e sappiamo (forma equivalente del principio del buon ordinamento) che non esistono successioni decrescenti infinite di numeri naturali.
Per quanto dimostrato nella Proposizione 4.66, vale la seguente catena di uguaglianze:

$$(a, b) = (b, r_1) = \ldots = (r_i, r_{i+1}) = \ldots (r_{n-1}, \underbrace{r_n}_{=0}) = r_{n-1}$$

□

Osservazione 4.69. Dalla Proposizione 4.41 segue che, l'algoritmo di Euclide per il calcolo del massimo comun divisore tra a e b, permette di calcolare il minimo comun multiplo (basta dividere il prodotto ab per (a, b)).

Vediamo ora un esempio di applicazione dell'algoritmo di Euclide, esempio che mostrerà come, attraverso l'algoritmo stesso, è possibile calcolarsi anche una coppia di coefficienti k, h che risolve l'identità di Bézout $(a, b) = a \cdot k + b \cdot h$.

Esempio 4.70. Determiniamo con l'algoritmo di Euclide il massimo comun divisore tra 450 e 126.

$$\begin{aligned} 450 &= 126 \cdot \underbrace{3}_{q_1} + \underbrace{72}_{r_1} \\ 126 &= 72 \cdot \underbrace{1}_{q_2} + \underbrace{54}_{r_2} \\ 72 &= 54 \cdot \underbrace{1}_{q_3} + \underbrace{18}_{r_3} \\ 54 &= 18 \cdot \underbrace{3}_{q_4} + \underbrace{0}_{r_4} \end{aligned}$$

Perciò il massimo comun divisore tra 450 e 126 è 18. La catena di uguaglianze tra massimi comun divisori che è alla base dell'algoritmo di Euclide è la seguente:

$$(\underbrace{450}_{a}, \underbrace{126}_{b}) = (\underbrace{126}_{b}, \underbrace{72}_{r_1}) = (\underbrace{72}_{r_1}, \underbrace{54}_{r_2})$$

$$(\underbrace{72}_{r_1}, \underbrace{54}_{r_2}) = (\underbrace{54}_{r_2}, \underbrace{18}_{r_3}) = (\underbrace{18}_{r_3}, \underbrace{0}_{r_4}) = 18$$

Risalendo l'algoritmo di Euclide è possibile anche trovare una coppia di interi k, h che risolve l'identità di Bézout, ovvero tale che $a \cdot h + b \cdot k = (a, b)$.

Vediamo come fare sull'esempio appena proposto tra 450 e 126. Dall'algoritmo di Euclide otteniamo che:

$$\begin{aligned} 72 &= 450 - 126 \cdot 3 \\ 54 &= 126 - 72 \cdot 1 \\ 18 &= 72 - 54 \cdot 1 \end{aligned}$$

Per cui partendo a sostituire dall'ultima equazione:

$$\begin{aligned} 18 &= 72 - 54 = 72 - (126 - 72) = 2 \cdot 72 - 126 = \\ &= 2 \cdot (450 - 126 \cdot 3) - 126 = 2 \cdot 450 - 7 \cdot 126 \end{aligned}$$

Quindi $h = 2$ e $k = -7$ sono due valori interi tali che $18 = 450 \cdot h + 126 \cdot k$.

Il metodo di *risalire* l'algoritmo di Euclide è piuttosto laborioso e anche inutile visto che i calcoli li abbiamo già fatti una volta. Possiamo usare un algoritmo (chiamato *algoritmo di Euclide esteso*) che calcola contemporaneamente massimo comun divisore tra a e b e due interi k, h che soddisfano l'identità di Bézout. Vediamo come fare con un esempio numerico. Calcoliamo il massimo comun divisore tra 153 e 253

in questo modo:

$$\begin{array}{lll}
v_1 & \begin{pmatrix} 253 & 1 & 0 \end{pmatrix} & \\
v_2 & \begin{pmatrix} 153 & 0 & 1 \end{pmatrix} & 253 = 153 \cdot 1 + 100 \\
v_1 - v_2 = v_3 & \begin{pmatrix} 100 & 1 & -1 \end{pmatrix} & 153 = 100 \cdot 1 + 53 \\
v_2 - v_3 = v_4 & \begin{pmatrix} 53 & -1 & 2 \end{pmatrix} & 100 = 53 \cdot 1 + 47 \\
v_3 - v_4 = v_5 & \begin{pmatrix} 47 & 2 & -3 \end{pmatrix} & 53 = 47 \cdot 1 + 6 \\
v_4 - v_5 = v_6 & \begin{pmatrix} 6 & -3 & 5 \end{pmatrix} & 47 = 6 \cdot 7 + 5 \\
v_5 - 7 \cdot v_6 = v_7 & \begin{pmatrix} 5 & 23 & -38 \end{pmatrix} & 6 = 5 \cdot 1 + 1 \\
v_6 - v_7 = v_8 & \begin{pmatrix} 1 & -26 & 43 \end{pmatrix} &
\end{array}$$

Quello che abbiamo trovato è che il massimo comun divisore tra 253 e 153 è 1 e che $k = -26$ e $h = 43$ soddisfano l'identità di Bézout, ovvero:

$$\underbrace{253 \cdot (-26)}_{-6578} + \underbrace{153 \cdot 43}_{6579} = 1$$

Ma cerchiamo di capire perché e come questo algoritmo funziona. Il tutto si basa sul calcolo di vettori v_i di tre componenti, la prima delle quali *esegue* l'algoritmo di Euclide. Se $v_i = (x_i, y_i, z_i)$, $v_{i+1} = (x_{i+1}, y_{i+1}, z_{i+1})$ e la divisione euclidea tra x_i e x_{i+1} (le due prime coordinate) è data da $x_i = q \cdot x_{i+1} + r$ allora definiamo v_{i+2} uguale a $v_i - q \cdot v_{i+1}$. Volendo calcolare il massimo comun divisore tra a, b con $a \geq b$ e partendo con $v_1 = (a, 1, 0)$ e $v_2 = (b, 0, 1)$ ci si ferma all'ultimo vettore v_j con prima componente x_j diversa da zero: tale x_j è il massimo comun divisore tra a e b (infatti sulla prima componente dei v_i, come detto, non abbiamo fatto altro che eseguire l'algoritmo di Euclide). Quello che rimane da capire è perché la seconda e terza componente y_j e z_j di v_j soddisfano l'identità di Bézout. Basta osservare che per ogni i (nei casi iniziali $i = 1$ e $i = 2$ per definizione) le tre componenti x_i, y_i, z_i del vettore v_i sono tali che $x_i = a \cdot y_i + b \cdot z_i$.

Esercizio 4.71. *Dimostrare, esibendo un controesempio, che non è vero che, per ogni n in $\mathbb{N}$ si ha $(33n + 22, 2n + 5) = 1$.*

Svolgimento. Indichiamo con d il massimo comun divisore $(33n+22, 2n+5)$. Dalla Proposizione 4.66 sappiamo che:

$$d = (\underbrace{33n + 22}_{a} + (\underbrace{-16}_{k} \underbrace{(2n + 5)}_{b}), \underbrace{2n + 5}_{b}) = (n - 58, 2n + 5)$$

Usando sempre la Proposizione 4.66, riusciamo a scrivere d in modo che sia il massimo comun divisore di due numeri, di cui uno non dipende da n:

$$d = (n - 58, 2n + 5) = (n - 58, 2n + 5 - 2(n - 58)) = (n - 58, 121)$$

Osservando che $121 = 11^2$ si ha che d può essere 1, 11 o 121. Scegliendo n in modo che $n - 58$ sia uguale ad 11, ovvero $n = 69$, si ha $d = 11$.

5. Equazioni diofantee

Definizione 4.72. Dati a, b, c interi l'equazione $a \cdot x + b \cdot y = c$ nelle incognite x, y si dice **equazione diofantea**. Una coppia (r, s) di interi per cui vale $a \cdot r + b \cdot s = c$ si dice una **soluzione dell'equazione diofantea**.

Vogliamo studiare per quali valori a, b, c in $\mathbb{Z}$, l'equazione $a \cdot x + b \cdot y = c$ ha soluzione. La risposta a questo interrogativo è fornita dal prossimo teorema.

Teorema 4.73. *Dati $a, b, c \in \mathbb{Z}$ l'equazione diofantea $a \cdot x + b \cdot y = c$ nelle variabili x, y ha una soluzione (r, s) (con r, s interi) se e solo se $d = (a, b) \mid c$.*

Dimostrazione. $\Rightarrow$) Per ipotesi esistono r e s tali che $a \cdot r + b \cdot s = c$. Sappiamo inoltre, per definizione di massimo comun divisore, che esistono a_1 e b_1 interi tali che $a = d \cdot a_1$ e $b = d \cdot b_1$ per cui $c = (d \cdot a_1) \cdot r + (d \cdot b_1) \cdot s$ e, raccogliendo a fattore d si trova $c = d \cdot (a_1 \cdot r + b_1 \cdot s)$, ovvero $d \mid c$.

$\Leftarrow$) Per ipotesi esiste $k \in \mathbb{Z}$ tale che $c = d \cdot k$. Inoltre per Bézout sappiamo che esistono w, z tali che $d = a \cdot w + b \cdot z$. Moltiplicando entrambi i membri per k si ottiene:

$$\underbrace{d \cdot k}_{=c} = a \cdot \underbrace{w \cdot k}_{=r} + b \cdot \underbrace{z \cdot k}_{=s}$$

E dunque la coppia (r, s) è una soluzione della diofantea. □

Corollario 4.74. *Due numeri interi a, b sono coprimi se e solo se esistono $r, s \in \mathbb{Z}$ tali che $a \cdot r + b \cdot s = 1$.*

Dimostrazione. $\Rightarrow$) Lo abbiamo già dimostrato in generale per il massimo comun divisore di qualsiasi coppia a, b di interi, in questo caso per ipotesi $(a, b) = 1$.

$\Leftarrow$) Dal Teorema 4.73 segue che d è un intero positivo che divide 1, dunque $d = 1$. □

A questo punto siamo interessati, nel caso $(a, b) \mid c$, a capire quante sono le soluzioni dell'equazione diofantea $a \cdot x + b \cdot y = c$ e come fare a determinarle tutte. Due fondamentali proprietà per rispondere alla nostra domanda sono descritte nelle prossime due proposizioni.

Proposizione 4.75. *Date (x_1, y_1) e (x_2, y_2) soluzioni dell'equazione diofantea $a \cdot x + b \cdot y = c$, la coppia differenza $(x_1 - x_2, y_1 - y_2)$ è soluzione di $a \cdot x + b \cdot y = 0$ (detta* **equazione omogenea associata***).*

Dimostrazione. Sostituendo $(x_1 - x_2, y_1 - y_2)$ a primo membro della diofantea al posto delle variabili x e y, si ha:

$$a \cdot (x_1 - x_2) + b \cdot (y_1 - y_2) = \underbrace{a \cdot x_1 + b \cdot y_1}_{=c} - (\underbrace{a \cdot x_2 + b \cdot y_2}_{=c}) = 0$$

□

Proposizione 4.76. *Se (r, s) è una soluzione della diofantea $a \cdot x + b \cdot y = c$, e (x_0, y_0) è una soluzione della diofantea omogenea associata, allora la coppia somma $(r + x_0, s + y_0)$ è ancora una soluzione della diofantea.*

Dimostrazione. Sostituendo $(r + x_0, s + y_0)$ a primo membro della diofantea al posto delle variabili x e y, si ha infatti che:

$$a \cdot (r + x_0) + b \cdot (s + y_0) = \underbrace{a \cdot r + b \cdot s}_{=c} + \underbrace{a \cdot x_0 + b \cdot y_0}_{=0} = c$$

□

Mettendo insieme i due risultati appena dimostrati, possiamo caratterizzare completamente l'insieme delle soluzioni di una diofantea.

Proposizione 4.77. *Siano $a, b, c \in \mathbb{Z}$ tali che $(a, b) \mid c$. Consideriamo la diofantea $a \cdot x + b \cdot y = c$ e sia (r, s) una soluzione particolare. Gli elementi dell'insieme A delle soluzioni della diofantea sono tutte e sole le coppie di interi ottenute sommando ad (r, s) una qualsiasi soluzione della equazione omogenea associata. Ovvero, indicando con A_0 l'insieme delle soluzioni dell'omogenea,*

$$A = \{(x, y) | (x, y) = (r, s) + (x_0, y_0) \quad \text{con} \quad (x_0, y_0) \in A_0\}$$

Proposizione 4.78. *Data l'equazione diofantea $ax + by = c$, se $d = (a, b)$ divide c (e quindi la diofantea ha soluzione), allora esistono infinite soluzioni.*

Dimostrazione. Vista la Proposizione 4.77, dobbiamo provare che l'insieme A_0 delle soluzioni dell'equazione omogenea associata, ha infinite soluzioni. Per ipotesi esistono a_1 e b_1 interi tali che $a = d \cdot a_1$, $b = d \cdot b_1$ (dall'Esercizio 4.37 sappiamo anche che $(a_1, b_1) = 1$). L'equazione omogenea associata ad $ax + by = c$ è dunque $(d \cdot a_1)x + (d \cdot b_1)y = 0$. Essendo $d \neq 0$ sappiamo che (Esercizio 4.13) questo equivale a $a_1 \cdot x + b_1 \cdot y = 0$. Dunque $a_1 \cdot x = -b_1 \cdot y$, ovvero $a_1 \mid b_1 \cdot y$. D'altra parte a_1 e b_1 sono coprimi, dunque (Esercizio 4.34) a_1 divide y, ovvero esiste t in $\mathbb{Z}$ tale che $a_1 t = y$. Sostituendo nell'uguaglianza sopra, e usando nuovamente l'Esercizio 4.13 ($a_1 \neq 0$) si ottiene $x = -b_1 \cdot t$. Le soluzioni dell'omogenea sono dunque le coppie $(-b_1 \cdot t, a_1 \cdot t)$ al variare di t in $\mathbb{Z}$. In particolare le soluzioni di un'equazione diofantea omogenea sono infinite. □

A questo punto dovrebbe essere chiara la strategia per risolvere l'equazione diofantea $a \cdot x + b \cdot y = c$ con $d = (a, b) \mid c$. Tale strategia è divisa in due passi:

(1) Ricerca di una soluzione particolare (r, s) di $a \cdot x + b \cdot y = c$.
(2) Ricerca dell'insieme di soluzioni dell'omogenea associata $a \cdot x + b \cdot y = 0$.

Passo 1: Determinazione di una soluzione particolare di $a \cdot x + b \cdot y = c$.
Dividendo c per d troviamo un intero k tale che $c = d \cdot k$. Abbiamo visto che con l'algoritmo di Euclide (esteso o *risalendo* l'algoritmo di Euclide standard) è possibile trovare r, s tali che $d = a \cdot r + b \cdot s$. Moltiplicando questa uguaglianza per k si ottiene $\underbrace{d \cdot k}_{=c} = a \cdot (r \cdot k) + b \cdot (s \cdot k)$. Dunque $(r \cdot k, s \cdot k)$ è una soluzione particolare della diofantea.

Esercizio 4.79. *Trovare, se esiste, una soluzione particolare dell'equazione diofantea $321 \cdot t + 27 \cdot k = 12$.*

Svolgimento. Calcoliamo il massimo comun divisore tra 321 e 27 con l'algoritmo di Euclide:

$$\begin{aligned} 321 &= 11 \cdot 27 + 24 \\ 27 &= 1 \cdot 24 + 3 \\ 24 &= 8 \cdot 3 + 0 \end{aligned}$$

Perciò $(321, 27) = 3$. 3 divide 12 e dunque la diofantea $321 \cdot t + 27 \cdot k = 12$ ha soluzione. Per trovare una soluzione particolare *risaliamo* l'algoritmo di Euclide:

$$\begin{aligned} 3 &= 27 - 24 \\ 24 &= 321 - 11 \cdot 27 \end{aligned} \quad \Rightarrow \quad 3 = 27 - (321 - 11 \cdot 27) = 12 \cdot 27 - 321$$

Moltiplicando per 4 (il risultato di $c = 12$ diviso $d = 3$) si ottiene:

$$12 = 48 \cdot 27 - 4 \cdot 321$$

Ovvero una soluzione particolare della diofantea data è $(-4, 48)$.

Esercizio 4.80. *Determinare, se esiste,* (x, y, z) *in* $\mathbb{Z}^3$ *tale che* $35x + 77y + 55z = 4$.

Svolgimento. Cerchiamo di ricondurci ad una equazione diofantea in due variabili. Riscriviamo la nostra equazione come segue: $77y+55z = 4-35x$. Se la consideriamo in y, z, sappiamo che questa equazione ha soluzione se e solo se $(77, 55) = 11$ divide $4 - 35x$. Dobbiamo dunque scegliere x in modo che $4 - 35x$ sia uguale a $11t$, ovvero risolvere la equazione diofantea $11t + 35x = 4$, nelle variabili x, t. Questa equazione ha soluzione perché $(11, 35) = 1$. È facile osservare, senza troppi calcoli, che scegliendo $x = 1$ e $t = -3$ si ottiene 2, dunque scegliendo $x = 2$ e $t = -6$ avremo come risultato 4. A questo punto vogliamo trovare una soluzione di $77y + 55z = 4 - 35 \cdot 2$, ovvero $77y + 55z = -66$. Dividendo per 11 si ottiene $7y + 5z = -6$. Si potrebbe usare l'algoritmo di Euclide, ma, visto che si tratta di numeri piccoli, anche osservare *ad occhio* che $y = -1$, $z = 1$ restituisce -2, e dunque $y = -3$ e $z = 3$ darà -6. Dunque una soluzione all'equazione iniziale è data dalla terna $(2, -3, 3)$, infatti:

$$35 \cdot 2 + 77 \cdot (-3) + 55 \cdot 3 = 70 - 231 + 165 = 235 - 231 = 4$$

Passo 2: Determinazione di tutte le soluzioni dell'omogenea.
Abbiamo visto, dalla dimostrazione della Proposizione 4.78, che l'equazione diofantea $ax + by = 0$ ha infinite soluzioni descritte dall'insieme:

$$A_0 = \{(\frac{-b}{(a,b)}t, \frac{a}{(a,b)}t) \in \mathbb{Z} \times \mathbb{Z} | t \in \ Z\}$$

Esercizio 4.81. *Determinare tutte le soluzioni della diofantea* $321t+27k = 12$.

Svolgimento. Abbiamo già calcolato la soluzione particolare $(-4, 48)$, dunque ci resta da determinare l'insieme A_0 delle soluzioni dell'omogenea. Dividiamo i due membri dell'equazione per 3 $((321, 27))$, e otteniamo $107t + 9k = 4$. Dunque A_0 è il seguente insieme:

$$A_0 = \{(-\underbrace{9}_{\frac{27}{3}} \cdot t, \underbrace{107}_{\frac{321}{3}} \cdot t) \in \mathbb{Z} \times \mathbb{Z} | t \in \mathbb{Z}\}$$

A questo punto, dalla Proposizione 4.77 segue chem tutte le soluzioni della diofantea sono descritte, al variare di t in $\mathbb{Z}$, dalle coppie:

$$(4, 48) + A_0 = (-4 - 9 \cdot t, 48 + 107 \cdot t)$$

6. Congruenze e insiemi $\mathbb{Z}/m\mathbb{Z}$

Introduciamo su $\mathbb{Z}$ la relazione binaria $\equiv_m$ definita come segue:

Definizione 4.82. Dati $a, b \in \mathbb{Z}$, $m > 1$ intero si definisce $a \equiv_m b$ se e solo se m divide $a - b$. La relazione $\equiv_m$ è detta **congruenza modulo** m e a, b si dicono **congrui** modulo m. Si scrive anche $a \equiv b\ (m)$ in luogo di $a \equiv_m b$.

Esempio 4.83. 1085 è congruo a 7 modulo 11 in quanto $1085 - 7 = 1078$ e 1078 è uguale a $11 \cdot 98$.

Proposizione 4.84. *Siano* $a, b \in \mathbb{Z}$ *e* m *intero maggiore di* 1. $a \equiv_m b$ *se e solo se* a *e* b *hanno lo stesso resto nella divisione per* n.

DIMOSTRAZIONE. Indichiamo con q_a, r_a e q_b, r_b il quoziente e resto della divisione euclidea rispettivamente di a e b per m, cioè $a = q_a \cdot m + r_a$ e $b = q_b \cdot m + r_b$.

$\Rightarrow$) Per ipotesi $m \mid (a-b)$, cioè esiste $k \in \mathbb{Z}$ tale che $a - b = k \cdot m$, ovvero $a = b + k \cdot m$. Dunque:

$$\underbrace{q_a \cdot m + r_a}_{=a} = \underbrace{q_b \cdot m + r_b}_{=b} + k \cdot m = (q_b + k) \cdot m + r_b$$

Per l'unicità di quoziente e resto della divisione euclidea si ha che $q_a = q_b + k$ e $r_a = r_b$.

$\Leftarrow$) Se $r_a = r_b$ allora $a - b = q_a \cdot m + r_a - (q_b \cdot m + r_b) = (q_a - q_b) \cdot m$. Cioè $m \mid (a-b)$. □

Proposizione 4.85 (Proprietà delle congruenze)**.** *Siano m intero maggiore di 1 e $a, b \in \mathbb{Z}$ tali che $a \equiv b\ (m)$, allora valgono le seguenti proprietà:*

(1) $(a, m) = (b, m)$,
(2) $\forall r \in \mathbb{Z}$, $r \cdot a \equiv r \cdot b\ (m)$,
(3) $\forall c, d \in \mathbb{Z}$, *se* $c \equiv d\ (m)$ *allora* $a + c \equiv b + d\ (m)$ *e* $a \cdot c \equiv b \cdot d\ (m)$,
(4) $\forall d \in \mathbb{Z}$, $d \mid m \Rightarrow a \equiv b\ (d)$,
(5) $\forall n \in \mathbb{Z}$, $a \equiv b\ (n) \Rightarrow a \equiv b\ ([m, n])$.

DIMOSTRAZIONE. Ipotesi comune a tutti gli enunciati che dobbiamo provare è che $a \equiv b\ (m)$, ovvero m divide $a - b$, cioè esiste $k \in \mathbb{Z}$ tale che $a - b = k \cdot m$, o equivalentemente $a = b + k \cdot m$.

(1) $(a, m) = (b + k \cdot m, m)$ e dalla Proposizione 4.66 segue che $(b + k \cdot m, m)$ è uguale a (b, m).
(2) $r \cdot a - r \cdot b = r \cdot (a - b) = r \cdot k \cdot m$, ovvero m divide $r \cdot a - r \cdot b$.
(3) Se esiste $h \in \mathbb{Z}$ tale che $c - d = h \cdot m$, allora si ha:

$$(a + c) - (b + d) = (a - b) + (c - d) = k \cdot m - h \cdot m = (k - h) \cdot m$$

Ovvero m divide $(a + c) - (b + d)$.
Analogamente se con h indichiamo $(a \cdot c) - (b \cdot d)$ si ha:

$$h = (b + k \cdot m) \cdot (d + h \cdot m) - b \cdot d = m \cdot (b \cdot h + k \cdot d + k \cdot h \cdot m)$$

il che dimostra: m divide $(a \cdot c) - (b \cdot d)$.
(4) Se esiste $t \in \mathbb{Z}$ tale che $m = t \cdot d$ allora:

$$a - b = k \cdot m = k \cdot t \cdot d$$

Ovvero d divide $a - b$.
(5) Se n divide $a - b$, allora $a - b$ è un multiplo comune di m e n, ovvero è un multiplo di $[m, n]$ cioè $[m, n]$ divide $a - b$.

□

Osservazione 4.86. Osserviamo che in generale per le congruenze modulo m non vale quella che chiamiamo *legge di cancellazione* (vedi anche Esercizio 4.14): dati a, b, c interi con $c \neq 0$ e $a \cdot c \equiv b \cdot c\ (m)$, in generale non possiamo concludere che $a \equiv b\ (m)$. Consideriamo per esempio $a = 1$, $b = 3$, $c = 3$ e $m = 6$, si ha che: $\underbrace{3}_{a \cdot c} \equiv \underbrace{9}_{b \cdot c}\ (6)$, ma 1 non è congruo a 3 modulo 6.

Proposizione 4.87. *Siano a, b, c in $\mathbb{Z}$ ($c \neq 0$) tali che $a \cdot c \equiv b \cdot c\ (m)$, allora $a \equiv b\ \left(\frac{m}{(m,c)}\right)$.*

DIMOSTRAZIONE. Sia $d = (m, c)$ allora, per l'Esercizio 4.37, esistono $m_1, c_1 \in \mathbb{Z}$ tali che $m = m_1 \cdot d$, $c = c_1 \cdot d$ e $(m_1, c_1) = 1$. Per ipotesi m divide $c \cdot (a - b)$, ovvero esiste $t \in \mathbb{Z}$ tale che $c \cdot (a - b) = t \cdot m$. Dividendo per d si ottiene $c_1 \cdot (a - b) = t \cdot m_1$, ovvero m_1 divide $c_1 \cdot (a - b)$. Essendo c_1 e m_1 coprimi questo implica che m_1 divide $a - b$ (osserviamo che m_1 è proprio $\frac{m}{(m,c)}$). □

Corollario 4.88. *Nelle ipotesi della proposizione precedente, se $(m, c) = 1$ allora da $a \cdot c \equiv b \cdot c\ (m)$ segue che $a \equiv b\ (m)$.*

A partire dalla relazione di congruenza modulo m, possiamo definire un nuovo insieme, ottenuto come quoziente di $\mathbb{Z}$. Dimostriamo infatti che la relazione di congruenza è di equivalenza.

Proposizione 4.89. *Per ogni m intero maggiore di 1 la relazione di congruenza modulo m è di equivalenza su $\mathbb{Z}$.*

DIMOSTRAZIONE. **Riflessiva.** Per ogni $z \in \mathbb{Z}$, m divide $z - z = 0$, ovvero $z \equiv_m z$.

Simmetrica. Per ogni $z, w \in \mathbb{Z}$, se m divide $z - w$ allora m divide $w - z$, cioè $z \equiv_m w$ implica $w \equiv_m z$.

Transitiva. Per ogni $z, w, x \in \mathbb{Z}$, se $z \equiv_m w$ (ovvero m divide $z - w$) e $w \equiv_m x$ (ovvero m divide $w - x$), allora esistono $t, r \in \mathbb{Z}$ tali che $z - w = t \cdot m$ e $w - x = r \cdot m$. Da questo segue che $z - x = (z - w) + (w - x) = t \cdot m + r \cdot m = m \cdot (t + r)$, dunque m divide $z - x$, cioè $z \equiv_m x$. □

Definizione 4.90. L'insieme quoziente $\mathbb{Z}/_{\equiv_m}$ di $\mathbb{Z}$ rispetto a $\equiv_m$ è detto insieme degli **interi modulo** m. Indicheremo tale insieme quoziente con $\mathbb{Z}/m\mathbb{Z}$ o anche con $\mathbb{Z}_m$.

Osservazione 4.91. Gli elementi di $\mathbb{Z}/m\mathbb{Z}$ sono le classi di equivalenza modulo m. In particolare abbiamo visto che due interi sono congrui modulo m se hanno lo stesso resto nella divisione per m. Quindi i resti possibili nella divisione euclidea per m possono essere scelti come insieme di rappresentanti. Tali resti sono m (infatti se r è resto allora $0 \leq r < m$) dunque $|\mathbb{Z}/m\mathbb{Z}| = m$ e:

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Esercizio 4.92. *Dimostrare che m interi consecutivi sono sempre un insieme di rappresentanti per la congruenza.*

Ci chiediamo: quali interi appartengono alla classe di $[a]_m$? Sappiamo che $b \in [a]_m$ (cioè $a \equiv_m b$) se e solo se m divide $a - b$, ovvero se e solo se esiste $k \in \mathbb{Z}$ tale che $a = b + k \cdot m$. Dunque alla classe $[a]_m$ appartengono tutti gli interi della progressione aritmetica di ragione m e base a:

$$[a]_m = \{a + k \cdot m | k \in \mathbb{Z}\}$$

Sull'insieme $\mathbb{Z}/m\mathbb{Z}$ possiamo definire due operazioni di somma $+_{\mathbb{Z}/m\mathbb{Z}}$ e prodotto $\cdot_{\mathbb{Z}/m\mathbb{Z}}$ *indotte*[5] dalle operazioni di $\mathbb{Z}$ come segue[6]:
Somma: Per ogni $[a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$ poniamo $[a]_m +_{\mathbb{Z}/m\mathbb{Z}} [b]_m = [a+b]_m$. Ovvero la somma di due classi in $\mathbb{Z}/m\mathbb{Z}$ è la classe della somma (in $\mathbb{Z}$) di due rappresentanti.
Prodotto: Per ogni $[a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$ poniamo $[a]_m \cdot_{\mathbb{Z}/m\mathbb{Z}} [b]_m = [a \cdot b]_m$. Ovvero il prodotto di due classi in $\mathbb{Z}/m\mathbb{Z}$ è la classe del prodotto (in $\mathbb{Z}$) di due rappresentanti.

Osservazione 4.93. Il fatto che queste definizioni siano *buone* definizioni, cioè il risultato non dipenda dalla scelta dei rappresentanti delle classi $[a]_m$ e $[b]_m$, è garantito dalla terza proprietà della Proposizione 4.85.

È inoltre facile provare (usando le proprietà di somma e prodotto in $\mathbb{Z}$) che la somma e il prodotto in $\mathbb{Z}/m\mathbb{Z}$ godono delle proprietà commutativa e associativa e vale la proprietà distributiva del prodotto rispetto alla somma. Inoltre per entrambe le operazioni esiste l'elemento neutro ($[0]_m$ per la somma e $[1]_m$ per il prodotto), e per la somma ogni elemento $[a]_m$ ha inverso $[-a]_m$. Si nota invece che in $\mathbb{Z}/m\mathbb{Z}$ non tutti gli elementi hanno inverso moltiplicativo: per esempio $[0]_m$ non ha inverso in quanto per ogni $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ il prodotto $[0]_m \cdot [a]_m$ è uguale a $[0 \cdot a]_m$ ovvero a $[0]_m$ che è diverso dalla classe $[1]_m$.

Proposizione 4.94 (Criteri di divisibilità per 2, 3, 5 e 11)**.** *Sia n un numero naturale la cui forma decimale è $a_k \dots a_1 a_0$, con $a_i \in \{0, \dots 9\}$ per ogni i e $a_k \neq 0$.*

(1) *n è divisibile per 2 se e solo se $a_0 \equiv 0$ (2),*
(2) *n è divisibile per 3 se e solo se $\sum_{i=0}^{k} a_i \equiv 0$ (3),*
(3) *n è divisibile per 5 se e solo se $a_0 \equiv 0$ (5).*
(4) *n è divisibile per 11 se e solo se $\sum_{i=0}^{k} (-1)^{i+1} a_i \equiv 0$ (11).*

Dimostrazione. Possiamo scrivere n anche nella forma $\sum_{i=0}^{k} 10^i \cdot a_i$. Dire che n è divisibile per m, significa che $[n]_m = [0]_m$. Dalle proprietà delle congruenze sappiamo che:

$$[\sum_{i=0}^{k} 10^i \cdot a_i]_m = \sum_{i=0}^{k} [10^i]_m \cdot [a_i]_m$$

(1) Se $m = 2$ si ha che $[10^i]_2$ è uguale a $[1]_2$ se i è uguale a 0, ed è uguale ad $[0]_2$ altrimenti. Dunque $[n]_2 = [a_0]_2$.
(2) Se $m = 3$ si ha $[10^i]_3 = [1]_3$ per ogni i. Dunque $[n]_3 = [\sum_{i=0}^{k} a_i]_3$.
(3) Se $m = 5$ si ha lo stesso risultato del caso $m = 2$ (non è un caso, visto che lavoriamo con la scrittura decimale, e 2 e 5 sono i fattori di 10). Dunque $[n]_5 = [a_0]_5$.
(4) Se $m = 11$, $[10^i]_{11}$ è uguale a $[1]_{11}$ se i è pari, ed a $[-1]_{11}$ se i è dispari. Dunque $[n]_{11} = [\sum_{i=0}^{k} (-1)^{i+1} a_i]_{11}$.

□

Esercizio 4.95. *Dimostrare che, per ogni numero intero $n \geq 0$, $7^{3^n} - 1$ è divisibile per 3^{n+1}.*

[5] In seguito vedremo che questo procedimento è generalizzabile a qualsiasi insieme quoziente.
[6] Nel seguito indicheremo $+_{\mathbb{Z}/m\mathbb{Z}}$ e $\cdot_{\mathbb{Z}/m\mathbb{Z}}$ rispettivamente con $+$ e $\cdot$, senza far riferimento a $\mathbb{Z}/m\mathbb{Z}$, e spesso, nel caso della moltiplicazione, ometteremo persino il $\cdot$, scrivendo ab in luogo di $a \cdot b$.

Svolgimento. Procediamo per induzione su n.
Passo base. Se $n = 0$, allora l'enunciato dice che $7^{3^0} - 1$ ovvero 6 è divisibile per 3^{0+1} ovvero 3, e questo è ovviamente vero.
Passo induttivo. Supponiamo l'enunciato vero per n, ovvero che esista $h \in \mathbb{N}$ tale che $7^{3^n} - 1 = h \cdot 3^{n+1}$, e dimostriamo che da questo segue che $7^{3^{(n+1)}} - 1$ è divisibile per $3^{(n+1)+1}$, ovvero che esiste $t \in \mathbb{N}$ tale che $7^{3^{(n+1)}} - 1 = t \cdot 3^{n+2}$. D'altra parte:

$$7^{3^{(n+1)}} - 1 = 7^{3^n \cdot 3} - 1 = (7^{3^n})^3 - 1 = (7^{3^n})^3 - 1^3$$

Abbiamo cioè scritto il termine che vorremmo fosse divisibile per 3^{n+2}, come differenza di cubi. Possiamo dunque usare la scomposizione del prodotto notevole $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$ per scrivere:

$$(7^{3^n})^3 - 1^3 = (7^{3^n} - 1)((7^{3^n})^2 + 7^{3^n} + 1)$$

Ora, per ipotesi induttiva possiamo scrivere:

$$(7^{3^n} - 1)((7^{3^n})^2 + 7^{3^n} + 1) = (h \cdot 3^{n+1})((7^{3^n})^2 + 7^{3^n} + 1)$$

Per completare la dimostrazione basta far vedere che $(7^{3^n})^2 + 7^{3^n} + 1$ è un multiplo di 3. Ma questo è vero perché $7 \equiv 1$ (3) e dunque:

$$\underbrace{(7^{3^n})^2}_{\equiv 1\ (3)} + \underbrace{7^{3^n}}_{\equiv 1\ (3)} + 1 \equiv 0\ (3)$$

Gli elementi $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ invertibili sono quelli per cui esiste $[x]_m \in \mathbb{Z}/m\mathbb{Z}$ tale che $[a]_m \cdot [x]_m = [1]_m$, ovvero $[a]_m$ è invertibile se e solo se esiste una soluzione intera, nell'incognita x, della congruenza $a \cdot x \equiv 1\ (m)$. Risponderemo alla questione di quali $[a]_m$ sono invertibili (per il prodotto) in $\mathbb{Z}/m\mathbb{Z}$ affrontando il problema più generale di discutere, dati $a, b \in \mathbb{Z}$, l'esistenza di soluzioni della generica congruenza nell'incognita x: $ax \equiv b\ (m)$.

Teorema 4.96. *Dati a, b, m interi la congruenza $ax \equiv b\ (m)$ (con $m > 1$) ha soluzione se e solo se $(a, m) \mid b$. In tal caso la congruenza ha esattamente (a, m) soluzioni.*

Dimostrazione. $ax \equiv b\ (m)$ se e solo se esiste $k \in \mathbb{Z}$ tale che $ax - b = mk$ ovvero se e solo ha soluzione nelle incognite x, k l'equazione diofantea $ax - mk = b$. Dal Teorema 4.73 segue che la congruenza è risolubile se e solo se $(a, m) \mid b$. In tal caso, indicando con (x_1, k_1) una soluzione particolare della diofantea, sappiamo che l'insieme S di tutte le soluzioni è descritto da:

$$S = \{\left(x_1 + \frac{m}{(a,m)}t, k_1 + \frac{a}{(a,m)}t\right) | t \in \mathbb{Z}\}$$

Dunque $ax \equiv b\ (m)$ se e solo se $x \equiv x_1\ (\frac{m}{(a,m)})$. Per elencare (e contare) il numero di soluzioni in $\mathbb{Z}/m\mathbb{Z}$ della congruenza, si deve dunque elencare (e contare) quanti sono le classi differenti in $\mathbb{Z}/m\mathbb{Z}$ che verificano $x \equiv x_1\ (\frac{m}{(a,m)})$. Ora basta osservare che le classi della forma:

$$\left[x_1 + t\frac{m}{(a,m)}\right]_m$$

al variare di t tra 0 e $(a, m) - 1$, sono (a, m) classi distinte che verificano la congruenza richiesta. □

Dal Teorema 4.96 seguono in particolare due risultati sugli inversi in $\mathbb{Z}/m\mathbb{Z}$.

Corollario 4.97. *Gli invertibili per il prodotto in $\mathbb{Z}/m\mathbb{Z}$ sono le classi $[a]_m$ con a e m coprimi.*

Corollario 4.98. *Se $[a]_m$ è invertibile in $\mathbb{Z}/m\mathbb{Z}$, allora il suo inverso è unico.*

Dimostrazione. Basta osservare che, dalle ipotesi e dal Teorema 4.96, l'equazione $ax \equiv 1\ (m)$ ha esattamente $(a, m) = 1$ soluzioni. □

Osservazione 4.99. Per la proprietà 1 della Proposizione 4.85, qualsiasi rappresentante b della classe di $[a]_m$ è tale che $(a, m) = (b, m)$. Quindi, come deve essere, la condizione presente nel Corollario 4.97 non dipende dal rappresentante scelto.

Osserviamo inoltre che la caratterizzazione degli invertibili di $\mathbb{Z}/m\mathbb{Z}$ fornita dal Corollario 4.97, ci dice che in $\mathbb{Z}/m\mathbb{Z}$ ci sono esattamente $\phi(m)$ (dove ϕ è la funzione di Eulero introdotta nella Definizione 4.56) elementi invertibili.

Vediamo, attraverso un esempio, come la dimostrazione del Teorema 4.96 fornisca un metodo di risoluzione per le congruenze.

Esempio 4.100. Cerchiamo di determinare tutte le soluzioni intere di $14 \cdot x \equiv 21\ (35)$.

Osserviamo che $(14, 35) = 7$ divide 21 quindi la congruenza ha soluzione. x è una soluzione intera della congruenza se e solo se esiste k intero tale che $14 \cdot x - 35 \cdot k = 21$. Dunque, le soluzioni intere x della congruenza, saranno le *prime* componenti di tutte le soluzioni (x, k) della diofantea $14 \cdot x - 35 \cdot k = 21$, soluzioni che abbiamo imparato a trovare.

Con l'algoritmo di Euclide troviamo che $14 \cdot (-2) - 35 \cdot (-1) = 7$. Perciò:

$$14 \cdot (-2) \cdot 3 - 35 \cdot (-1) \cdot 3 = 21$$

Dunque $(-6, -3)$ è una soluzione particolare della diofantea, e tutte le soluzioni della diofantea sono date da $(-6 + 5t, -3 + 2t)$ al variare di t in $\mathbb{Z}$.

Per ciò che abbiamo osservato, tutte le soluzioni intere della congruenza sono date da $x = -6 + 5t$. Tale insieme di soluzioni può essere anche descritto, con la notazione introdotta, come $x \equiv -6\ (5)$ ovvero $x \equiv 4\ (5)$ (in quanto $-6 \equiv 4\ (5)$). Osserviamo che la congruenza ha infinite soluzioni in $\mathbb{Z}$, una sola in $\mathbb{Z}_5$ (la classe $[4]_5$), e 7 in $\mathbb{Z}_{35}$ (tutte le classi distinte di interi modulo 35 che nella divisione per 5 danno resto 4, ovvero $[4]_{35}$, $[9]_{35}$, $[14]_{35}$, $[19]_{35}$, $[24]_{35}$, $[29]_{35}$, $[34]_{35}$).

Osservazione 4.101. Indicando con $\mathbb{Z}/m\mathbb{Z}^*$ il sottoinsieme di $\mathbb{Z}/m\mathbb{Z}$ degli invertibili rispetto al prodotto, ovvero $\mathbb{Z}/m\mathbb{Z}^* = \{[a]_m | (a, m) = 1\}$, la restrizione del prodotto di $\mathbb{Z}/m\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}^*$ è un'operazione in $\mathbb{Z}/m\mathbb{Z}^*$. Infatti il prodotto di due invertibili di $\mathbb{Z}/m\mathbb{Z}$ è un invertibile: questa è una immediata conseguenza dell'Esercizio 4.55. Dato $[a]_m \in \mathbb{Z}/m\mathbb{Z}^*$ indicheremo con ${[a]_m}^{-1}$ l'inverso di $[a]_m$ (a sua volta $[a]_m = ({[a]_m}^{-1})^{-1}$ dunque ${[a]_m}^{-1} \in \mathbb{Z}/m\mathbb{Z}^*$).

Per determinare l'inverso di $[a]_m \in \mathbb{Z}/m\mathbb{Z}^*$, possiamo risolvere $ax \equiv 1\ (m)$ con il procedimento mostrato sopra per una generica congruenza.

Proposizione 4.102. *In $\mathbb{Z}/m\mathbb{Z}^*$ vale la legge di cancellazione, ovvero per ogni $a, b, c \in \mathbb{Z}/m\mathbb{Z}^*$ si ha: $a \cdot c = b \cdot c \Leftrightarrow a = c$.*

Dimostrazione. Un'implicazione è la seconda proprietà della Proposizione 4.85, l'altra segue immediatamente dal corollario 4.88. □

Corollario 4.103. *Ogni equazione di primo grado in $\mathbb{Z}/m\mathbb{Z}^*$ ha una e una sola soluzione.*

DIMOSTRAZIONE. Per ogni $[a]_m, [b]_m$ in $\mathbb{Z}/m\mathbb{Z}^*$, possiamo considerare l'equazione $[a]_m[x]_m - [b]_m = 0$, ovvero cerchiamo in $\mathbb{Z}/m\mathbb{Z}^*$ elementi $[x]_m$ tali che $[a]_m[x]_m$ sia uguale a $[b]_m$. $[a]_m$ è invertibile per definizione di $\mathbb{Z}/m\mathbb{Z}^*$. Dalla Proposizione 4.102 si ha che $[a]_m[x]_m = [b]_m$ se e solo se $[a^{-1}]_m[a]_m[x]_m = [a^{-1}]_m[b]_m$, ovvero $[x]_m = [a^{-1}]_m[b]_m$. Dunque l'equazione ha unica soluzione $[a^{-1}]_m[b]_m$. □

Finora abbiamo introdotto $\mathbb{Z}/m\mathbb{Z}$, definendo le operazioni $+_{\mathbb{Z}/m\mathbb{Z}}$, $\cdot_{\mathbb{Z}/m\mathbb{Z}}$, e discutendo il problema della risolubilità (ovvero l'esistenza di soluzioni) e della risoluzione (ovvero la determinazione dell'insieme delle soluzioni) di equazioni di primo grado in $\mathbb{Z}/m\mathbb{Z}$. Nei prossimi paragrafi tratteremo il problema della risolubilità e della risoluzione dei sistemi di congruenze.

7. Teorema cinese del resto

Dati $a, b, c, d \in \mathbb{Z}$, m, n interi maggiori di 1, vogliamo discutere la risolubilità di un generico sistema di due congruenze:

$$\begin{cases} ax \equiv b \ (m) \\ cx \equiv d \ (n) \end{cases}$$

Una condizione necessaria affinché il sistema sia risolubile è che siano risolubili le singole congruenze, ovvero che $t = (a, m) \mid b$ e $h = (c, n) \mid d$. Siano a_1, b_1, m_1 i quozienti della divisione di a, b, m per t e c_1, d_1, n_1 i quozienti della divisione di c, d, n per h. Possiamo riscrivere il sistema iniziale come segue (ovvero i due sistemi sono equivalenti, hanno lo stesso insieme di soluzioni):

$$\begin{cases} a_1x \equiv b_1 \ (m_1) \\ c_1x \equiv d_1 \ (n_1) \end{cases}$$

Dall'Esercizio 4.37, sappiamo che $(a_1, m_1) = (c_1, n_1) = 1$, dunque esistono in $\mathbb{Z}/m_1\mathbb{Z}$ e $\mathbb{Z}/n_1\mathbb{Z}$ gli inversi moltiplicativi ${a_1}^{-1}$ e ${c_1}^{-1}$ rispettivamente di a e c. Possiamo dunque riscrivere il sistema come segue:

$$\begin{cases} x \equiv {a_1}^{-1}b_1 \ (m_1) \\ x \equiv {c_1}^{-1}d_1 \ (n_1) \end{cases}$$

Condizione necessaria affinché un sistema di congruenze di primo grado sia risolubile è che possa essere portato in questa forma, che chiameremo **forma normale**. Dunque per studiare la risolubilità di sistemi di congruenze possiamo limitarci a studiare sistemi in forma normale.

Ad ora abbiamo chiesto unicamente che le due congruenze presenti nel sistema fossero singolarmente risolubili, non che gli insiemi delle soluzioni delle due si intersecassero. Ed in effetti non tutti i sistemi del tipo trovato sono risolubili.

Esempio 4.104. Il sistema

$$\begin{cases} x \equiv 1 \ (7) \\ x \equiv 0 \ (7) \end{cases}$$

non è risolubile, in quanto per il teorema di divisione euclidea, il resto della divisione per un numero (in questo caso 7) è unico, dunque non esiste nessun intero x che diviso per 7 possa dare resto 0 e resto 1.

Torniamo dunque a studiare il caso generale, esplorando se esistono condizioni necessarie e sufficienti sui coefficienti del sistema per stabilirne la risolubilità.

$$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$$

Traducendo le congruenze in uguaglianze, si ha che il sistema è risolubile se e solo se esistono h, k interi tali che il sistema:

$$\begin{cases} x = a + mk \\ x = b + nh \end{cases}$$

sia risolubile. Questo equivale al fatto che sia risolubile in h, k l'equazione diofantea $mk - nh = b - a$. Sappiamo che condizione necessaria e sufficiente per la risolubilità di questa diofantea è che $(m, n) \mid (b - a)$. Se questa condizione è verificata e k_1, h_1 sono una soluzione particolare allora tutte le soluzioni della diofantea sono date, al variare di $r \in \mathbb{Z}$, dalle coppie:

$$(k_1 + \frac{n}{(m,n)} \cdot r, h_1 + \frac{m}{(m,n)} \cdot r)$$

Dunque (Prop. 4.41), le x che risolvono il sistema sono date, al variare di r in $\mathbb{Z}$ da:

$$x = a + m \cdot (k_1 + \frac{n}{(m,n)} \cdot r) = \underbrace{a + mk_1}_{sol.par.\ x_1} + [m, n]r$$

Ovvero in termini di congruenze le soluzioni sono descritte da $x \equiv x_1 \ ([m, n])$.

In particolare, il sistema è risolubile se e solo se $(m, n) | b - a$, ed in questo caso esistono (m, n) soluzioni modulo $m \cdot n$. Abbiamo cioè mostrato il seguente risultato, noto come teorema cinese del resto:

Teorema 4.105 (Teorema cinese del resto)**.** *Siano dati due numeri naturali m, n primi tra loro e siano dati due resti r, s (cioè $0 \leq r < m$ e $0 \leq s < n$), allora esiste un unico x con $0 \leq x < m \cdot n$ e tale che:*

- *Il resto della divisione di x per m è r.*
- *Il resto della divisione di x per n è s.*

Si può generalizzare l'enunciato del teorema cinese del resto al caso di un sistema di n congruenze di moduli m_i (con $1 \leq i \leq n$) a due a due coprimi.

Teorema 4.106. *Siano $a_1, \ldots, a_n \in \mathbb{Z}$ e $m_1, \ldots, m_n$ interi maggiori di 1 a due a due coprimi, allora il sistema:*

$$\begin{cases} x \equiv a_1 \ (m_1) \\ \quad \vdots \\ x \equiv a_n \ (m_n) \end{cases}$$

ammette un'unica soluzione modulo $\prod_{i=1}^{n} m_i$.

Esercizio 4.107. *Dimostrare il teorema precedente. (Suggerimento: procedere per induzione sul numero di congruenze. Il caso base $n = 2$ è l'enunciato del teorema cinese del resto).*

Esercizio 4.108. *Determinare l'insieme di soluzioni in $\mathbb{N}$ (eventualmente anche vuoto) del seguente sistema di congruenze:*

$$\begin{cases} 7x \equiv 4 \ \ (11) \\ x \equiv 3 \ \ (14) \end{cases}$$

Svolgimento. L'inverso di 7 in $\mathbb{Z}_{11}$ è 8, dunque il sistema è equivalente a:

$$\begin{cases} x \equiv 32 \ \ (11) \\ x \equiv 3 \ \ (14) \end{cases}$$

Ovvero:

$$\begin{cases} x \equiv 10 \ \ (11) \\ x \equiv 3 \ \ (14) \end{cases}$$

Essendo 11 e 14 primi tra loro, il sistema è risolvibile e, se troviamo una soluzione particolare x_1, tutte le soluzioni x in $\mathbb{Z}$ del sistema saranno descritte, al variare di h in $\mathbb{Z}$, da $x = x_1 + 154 \cdot h$ ($154 = [11, 14]$).

Riscrivendo il sistema in termini di equazioni diofantee, esistono $k, t \in \mathbb{Z}$ tali che:

$$\begin{cases} x = 10 + 11 \cdot t \\ x = 3 + 14 \cdot k \end{cases}$$

Cerchiamo una soluzione particolare della diofantea $14 \cdot k - 11 \cdot t = 7$. Osservando che $14 \cdot 4 - 11 \cdot 5 = 1$, si ha che:

$$14 \cdot 28 - 11 \cdot 35 = 7$$

Quindi una soluzione particolare della diofantea è data da $(\underbrace{28}_{k}, \underbrace{35}_{t})$. Una soluzione particolare del sistema è dunque data da

$$x_1 = 10 + 11 \cdot 35 = 3 + 14 \cdot 28 = 395$$

Tutte le soluzioni x in $\mathbb{Z}$ del sistema di congruenze sono dunque date, al variare di h in $\mathbb{Z}$, dalla formula $x = 395 + 154 \cdot h$, che può essere riscritta, in termini di congruenze, come segue: $x \equiv 87$ (154) ($395 \equiv 87$ (154)). L'esercizio però chiede le soluzioni in $\mathbb{N}$: il più piccolo valore in $\mathbb{N}$ soluzione del sistema è $x = 87$. Dunque tutte le soluzioni in $\mathbb{N}$ del sistema sono descritte, al variare di t in $\mathbb{N}$, da $x = 87 + 154 \cdot t$.

Teorema 4.109 (Teorema cinese - seconda forma)**.** *Siano m, n interi maggiori di 1 coprimi. La funzione:*

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

che ad ogni classe $[a]_{m \cdot n}$ associa la coppia $([a]_m, [a]_n)$ è ben definita e bigettiva.

Dimostrazione. φ è ben definita se

$$[a]_{m \cdot n} = [b]_{m \cdot n} \Rightarrow \ \varphi([a]_{m \cdot n}) = \varphi([b]_{m \cdot n})$$

Ovvero

$$[a]_{m \cdot n} = [b]_{m \cdot n} \Rightarrow \ ([a]_m, [a]_n) = ([b]_m, [b]_n)$$

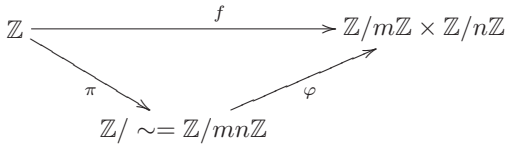
E questo è vero in quanto, se $m \cdot n$ divide $a - b$, allora sia m che n dividono $a - b$.

Il teorema cinese del resto implica che φ è una funzione surgettiva infatti ci dice per ogni intero a il sistema seguente ha una (unica) soluzione modulo $m \cdot n$:

$$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$$

La tesi segue, dal Teorema 3.10, osservando che $\mathbb{Z}/mn\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ hanno lo stesso numero di elementi. □

La tesi del teorema ci dice che il seguente diagramma commuta:



Corollario 4.110. *Dati $a \in \mathbb{Z}$ e m, n interi maggiori di 1 coprimi, la congruenza*

$$x \equiv a \ (m \cdot n)$$

è equivalente al sistema

$$\begin{cases} x \equiv a \ (m) \\ x \equiv a \ (n) \end{cases}$$

Corollario 4.111. *Nelle ipotesi e con le notazioni del Teorema 4.109, la restrizione di φ a $\mathbb{Z}/mn\mathbb{Z}^*$ è bigettiva su $\mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$.*

Dimostrazione. Dall'Esercizio 4.55 segue che:

$$[a]_{m\cdot n} \in \mathbb{Z}/mn\mathbb{Z}^* \Leftrightarrow \ \varphi([a]_{m\cdot n}) \in \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$$

□

Osservazione 4.112. Per ogni $m > 1$, si ha per definizione che $|\mathbb{Z}/m\mathbb{Z}^*| = \phi(m)$. Dal corollario 4.111 segue che se $(m, n) = 1$:

$$|\mathbb{Z}/mn\mathbb{Z}^*| = |\mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*| = |\mathbb{Z}/m\mathbb{Z}^*| \cdot |\mathbb{Z}/n\mathbb{Z}^*|$$

Abbiamo perciò una dimostrazione differente del fatto che: se $(m, n) = 1$ si ha $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Esercizio 4.113. *Dire per quali valori di $\alpha \in \mathbb{Z}$ il seguente sistema ha soluzioni:*

$$\Delta = \begin{cases} 6x \equiv \alpha \ (15) \\ 4x \equiv 1 \ (7) \end{cases}$$

Svolgimento. Poiché $[4]_7{}^{-1} = [2]_7$, moltiplicando entrambe i membri della seconda congruenza di Δ per 2, si ottiene la congruenza equivalente $x \equiv 2 \ (7)$.

Viceversa 6 non è invertibile in $\mathbb{Z}_{15}$, perché 6 e 15 non sono coprimi. La prima congruenza di Δ è risolubile se e solo se $(6, 15)$, cioè 3, divide α.

Dunque se α non è multiplo di 3, Δ non ha soluzione. Se invece $\alpha = 3\beta$, Δ è equivalente a:

$$\Delta_1 = \begin{cases} 2x \equiv \beta \ (5) \\ x \equiv 2 \ (7) \end{cases}$$

A questo punto 2 è invertibile modulo 5 (l'inverso è 3), dunque Δ_1 è equivalente a:

$$\Delta_2 = \begin{cases} x \equiv 3\beta \ (5) \\ x \equiv 2 \ (7) \end{cases}$$

Per il teorema cinese del resto Δ_2 è risolubile, perciò la condizione affinchè il sistema Δ sia risolubile è che α sia congruo a 0 modulo 3.

Risolviamo il sistema nel caso α sia modulo di 3. Sappiamo, sempre dal teorema cinese del resto, che le soluzioni del sistema saranno modulo $[5,7] = 35$. Cerchiamo una soluzione particolare del seguente sistema:

$$\begin{cases} x = 3\beta + 5k \\ x = 2 + 7h \end{cases}$$

Consideriamo dunque l'equazione diofantea $5k - 7h = 2 - 3\beta$. Una soluzione di $5k - 7h = 1$ è data da $k = 3, h = 2$, quindi una soluzione di $5k - 7h = 2 - 3\beta$ è data dalla coppia $(6 - 9\beta, 4 - 6\beta)$. Concludendo, una soluzione particolare del sistema Δ_2 (e dunque di Δ) è:

$$x = 3\beta + 5(6 - 9\beta) = -42\beta + 30$$

e tutte le soluzioni di Δ sono descritte da:

$$x \equiv -42\beta + 30 \equiv 30 - 7\beta \ (35)$$

Osservazione 4.114 (Metodo del sollevamento)**.** Descriviamo un metodo generale per risolvere sistemi di n congruenze con i moduli primi tra loro. Abbiamo già osservato che, se le singole congruenze del sistema sono risolvibili (condizione necessaria per la risolubilità del sistema), tutti i sistemi di congruenze di primo grado possono essere portati in forma normale, dunque consideriamo un sistema già in questa forma:

$$\begin{cases} x \equiv a_1 \ (m_1) \\ \dots \\ \dots \\ x \equiv a_n \ (m_n) \end{cases}$$

Dal teorema cinese del resto, sappiamo che un tale sistema ha una soluzione modulo il prodotto dei moduli. Consideriamo gli n sistemi σ_i:

$$\sigma_i = \begin{cases} x \equiv 0 \ (m_1) \\ \dots \\ x \equiv 1 \ (m_i) \\ \dots \\ x \equiv 0 \ (m_n) \end{cases}$$

Se x_i indica una soluzione del sistema σ_i, allora:

$$x \equiv \sum_{i=1}^{n} a_i x_i \ (\prod_{i=1}^{n} m_i)$$

è una soluzione del sistema originario. Infatti, per ogni j (con $1 \leq j \leq n$), si ha che:

$$x \equiv \sum_{i=1}^{n} a_i x_i \ (m_j) \Rightarrow x \equiv \sum_{i \neq j} a_i \cdot 0 + a_j \cdot 1 \equiv a_j \ (m_j)$$

Esercizio 4.115. *Descrivere le soluzioni intere del seguente sistema di congruenze:*

$$\begin{cases} 2x \equiv 1 \ (3) \\ 7x \equiv 3 \ (10) \\ 6x \equiv 2 \ (7) \end{cases}$$

Svolgimento. Essendo $2, 3, 6$ gli opposti rispettivamente di 2 in $\mathbb{Z}_3$, 7 in $\mathbb{Z}_{10}$, 6 in $\mathbb{Z}_7$, possiamo passare al sistema equivalente in forma normale:

$$\begin{cases} x \equiv 2 \ (3) \\ x \equiv 9 \ (10) \\ x \equiv 5 \ (7) \end{cases}$$

Per usare il metodo descritto, consideriamo i seguenti tre sistemi:

$$\begin{cases} x \equiv 1 \ (3) \\ x \equiv 0 \ (10) \\ x \equiv 0 \ (7) \end{cases} \quad \begin{cases} x \equiv 0 \ (3) \\ x \equiv 1 \ (10) \\ x \equiv 0 \ (7) \end{cases} \quad \begin{cases} x \equiv 0 \ (3) \\ x \equiv 0 \ (10) \\ x \equiv 1 \ (7) \end{cases}$$

Tali sistemi sono equivalenti ai seguenti:

$$\begin{cases} x \equiv 1 \ (3) \\ x \equiv 0 \ (70) \end{cases} \quad \begin{cases} x \equiv 0 \ (21) \\ x \equiv 1 \ (10) \end{cases} \quad \begin{cases} x \equiv 0 \ (30) \\ x \equiv 1 \ (7) \end{cases}$$

Le soluzioni dei tre sistemi sono modulo 210, ed è facile vedere che sono rispettivamente $x_1 \equiv 70 \ (210)$, $x_2 \equiv 21 \ (210)$ e $x_3 \equiv 120 \ (210)$. Quindi la soluzione del sistema originario è:

$$x \equiv 2 \cdot 70 + 9 \cdot 21 + 5 \cdot 120 \ (210)$$

Esercizio 4.116. *Determinare per quali valori di a in $\mathbb{N}$ è risolubile il seguente sistema di congruenze:*

$$\begin{cases} 7x \equiv -1 \ (12) \\ x \equiv 2a - 1 \ (3a) \end{cases}$$

Svolgimento. Osserviamo che $[7]_{12}$ è l'inverso di se stesso in $\mathbb{Z}/12\mathbb{Z}$. Dunque portiamo innanzitutto il sistema in forma normale, moltiplicando entrambi i membri della prima equazione per 7:

$$\begin{cases} x \equiv 5 \ (12) \\ x \equiv 2a - 1 \ (3a) \end{cases}$$

A questo punto la risolubilità del sistema dipende dal massimo comun divisore d tra 12 e $3a$ ($d = (12, 3a) = 3(4, a)$), che deve dividere $5 - (2a - 1)$, ovvero $6 - 2a$.

Per quello che abbiamo osservato, d può valere 3 (se a è dispari), 6 (se a è pari ma non multiplo di 4), 12 (se a è multiplo di 4). Studiamo separatamente i 3 casi.

- Se a è dispari (ovvero in termini di congruenze $a \equiv 1 \ (2)$), abbiamo osservato che $d = 3$ e dunque la condizione di risolubilità del sistema equivale a $6 - 2a \equiv 0 \ (3)$ (ovvero 3 divide $6 - 2a$). Riducendo i coefficienti della congruenza modulo 3 si ottiene $a \equiv 0 \ (3)$. Dunque il sistema iniziale ha soluzione se a è soluzione del sistema di congruenze seguente:

  $$\begin{cases} a \equiv 1 \ (2) \\ a \equiv 0 \ (3) \end{cases}$$

  Sistema che - dal teorema cinese del resto - sappiamo avere soluzione $a \equiv 3 \ (6)$.
- Se a è pari, ma non multiplo di 4, ovvero $a \equiv 2 \ (4)$, allora $d = 6$, e la condizione di risolubilità del sistema è $6 - 2a \equiv 0 \ (6)$. Questa congruenza è equivalente a $4a \equiv 0 \ (6)$, da cui si ricava (Proposizione 4.87) $2a \equiv 0 \ (3)$, ovvero (moltiplicando entrambi i membri per $[2]_3$ che è l'inverso di $[2]_3$)

$a \equiv 0\ (3)$. Dunque il sistema iniziale ha soluzione se a è soluzione del sistema di congruenze seguente:

$$\begin{cases} a \equiv 2\ (4) \\ a \equiv 0\ (3) \end{cases}$$

Sistema che - dal teorema cinese del resto - sappiamo avere soluzione $a \equiv 6\ (12)$.

- Se a è multiplo di 4, ovvero $a \equiv 0\ (4)$, allora $d = 12$ e la condizione di risolubilità del sistema equivale a 12 divide $6 - 2a$, ovvero $2a \equiv 6\ (12)$. Questa congruenza è equivalente (Proposizione 4.87) a $a \equiv 3\ (6)$. Dunque il sistema iniziale ha soluzione se a è soluzione del sistema di congruenze seguente:

$$\begin{cases} a \equiv 0\ (4) \\ a \equiv 3\ (6) \end{cases}$$

Sistema che - dal teorema cinese del resto - sappiamo non avere soluzioni (infatti $2 = (4, 6)$ non divide $3 - 0$). D'altra parte anche senza teorema cinese del resto si può osservare che i numeri congrui a 3 modulo 6 (ovvero della forma $3+6k$ con k intero) sono tutti dispari, e dunque non potranno mai essere multipli di 4.

Riassumendo abbiamo trovato che il sistema ha soluzione se a è congruo a 3 modulo 6 o se è congruo a 6 modulo 12. Cerchiamo di riscrivere tutto in un unico modulo, ovvero ci chiediamo: quali a in $\mathbb{Z}/12\mathbb{Z}$ sono congrui a 3 modulo 6? La risposta è $[3]_{12}$ e $[9]_{12}$.

Dunque i valori di a in $\mathbb{N}$ per cui il sistema è risolubile sono gli a della forma $t + 12k$, con t che varia nell'insieme $\{3, 6, 9\}$ e k che varia in $\mathbb{N}$.

8. Piccolo teorema di Fermat e teorema di Eulero

Proposizione 4.117. *Sia p un numero primo, per ogni $x, y \in \mathbb{Z}$ si ha:*

$$(x + y)^p \equiv x^p + y^p\ (p)$$

Dimostrazione. Dal Teorema 3.23 sappiamo che:

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i$$

Portando fuori dalla sommatoria il primo e l'ultimo termine (ovvero quelli corrispondenti rispettivamente a $i = 0$ e $i = p$) si ottiene:

$$(x + y)^p = \underbrace{\binom{p}{0}}_{=1} x^p + \underbrace{\binom{p}{1} x^{p-1} y + ... + \binom{p}{p-1} x y^{p-1}}_{A} + \underbrace{\binom{p}{p}}_{=1} y^p$$

Per concludere dobbiamo mostrare che A è un multiplo di p, perché, per definizione di congruenza, $(x + y)^p \equiv x^p + y^p\ (p)$ significa che $(x + y)^p$ e $x^p + y^p$ differiscono per un multiplo di p.

Osserviamo ch,e se p è un numero primo e $i < p$, allora p non divide $i!$, infatti tutti i fattori presenti nel fattoriale sono minori di p, quindi coprimi con p, e dunque anche il loro prodotto lo è (Esercizio 4.55). Da questo segue che il numero intero:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

è un multiplo di p, perché p divide il numeratore ma non il denominatore. Quindi A è somma di multipli di p, e perciò è anch'esso un multiplo di p. □

Teorema 4.118 (Piccolo teorema di Fermat)**.** *Sia p un numero primo, allora per ogni $x \in \mathbb{Z}$ si ha:*

$$x^p \equiv x \ (p)$$

Dimostrazione. Cominciamo dimostrando il teorema per $x \in \mathbb{N}$, procedendo per induzione.
Passo base. Se $x = 0$, l'enunciato equivale a $0^p \equiv 0 \ (p)$ che è banalmente vero.
Passo induttivo. Dobbiamo dimostrare che se $x^p \equiv x \ (p)$ allora $(x+1)^p \equiv (x+1) \ (p)$. Dalla Proposizione 4.117 segue che $(x+1)^p \equiv x^p + 1^p \ (p)$ e per ipotesi induttiva $x^p \equiv x \ (p)$. Dunque $(x+1)^p \equiv x + 1 \ (p)$.

Consideriamo ora il caso $x < 0$. L'ipotesi su x implica $-x > 0$ e, per quanto appena dimostrato, $(-x)^p \equiv -x \ (p)$, cioè $(-1)^p \cdot x^p \equiv -x \ (p)$. Se p è dispari abbiamo $x^p \equiv x \ (p)$, se $p = 2$ otteniamo $x^2 \equiv -x \ (2)$, ma $-x \equiv x \ (2)$. □

Curiosità [Il piccolo teorema di Fermat e i fili di perle].
Supponiamo di giocare a fare fili di perline colorate e di avere 3 colori diversi: il bianco (B), il rosso (R) e il giallo (G). Ci chiediamo quanti fili di 5 perle diversi (dove per diversi intendiamo anche diversi per l'ordine di inserimento delle perline) possiamo fare? La risposta la sappiamo ed è 3^5: tutte le funzioni da un insieme di 5 elementi (le *posizioni* sul filo di perle) ad un insieme di 3 elementi (i colori a nostra disposizione). Supponiamo adesso di domandarci la stessa cosa avendo n colori di perle e volendo fare fili di perle di lunghezza p con p primo (avendo, per ogni colore, almeno p perle di quel colore). La risposta sarà che possiamo fare n^p fili di perle distinti. A questo punto vogliamo trasformare i nostri fili di perle in delle belle collane, ma con l'idea di non considerare fili di perle tutti dello stesso colore perché troppo monotoni. Dunque in realtà lavoreremo su $n^p - n$ fili di perle (i fili di perle monocromatici sono n, tanti quanti i colori a nostra disposizione).

Per trasformare i nostri fili in collane, dobbiamo legare il filo. A questo punto ci domandiamo: da tutti i possibili fili di perle, quante collane diverse potremo fare? In questo caso supponiamo che il nodo al filo non si veda, coperto dalle perline, e dunque che una collana sia identificata dalla sequenza dei colori. Ad esempio, se consideriamo lunghezza 3, i fili di perle distinti (B, R, G), (R, G, B) e (G, B, R) andranno a formare la stessa collana.

Per rispondere alla domanda sul numero di collane differenti, bisogna perciò capire in generale quanti fili distinti di perle danno la stessa collana. L'esempio fatto suggerisce di *ribaltare* il punto di vista: data una collana (e quindi una volta scelta la sequenza dei colori, che può essere immaginata *chiusa* in cerchio), quanti fili di perle distinti la possono creare? Sicuramente tagliandola dopo qualsiasi perlina otteniamo un filo di perle che la genera. Il punto è: ogni taglio di questo tipo produce un filo di perle distinto? La risposta in generale è no, basta pensare ad esempio ad una collana con 4 perline di colore bianco e rosso alternati. Se tagliamo dopo una delle due perline rosse (o analogamente bianca) ottengo il filo di perle (B, R, B, R), ma la stessa cosa accade se taglio dopo l'altra perlina rossa. In questo caso dunque, due tagli diversi della collana danno lo stesso filo di perle.

Osservando l'esempio fatto notiamo che questo può accadere in generale se la collana è composta da una sequenza (ovvero una successione di più di una perlina) ripetuta: nell'esempio la sequenza (B, R) di lunghezza 2 è ripetuta due volte.

Osserviamo che, in questi casi, la lunghezza della collana è uguale al numero di volte che la sequenza è ripetuta per la lunghezza della sequenza. Dunque nel caso che ci interessa, ovvero collane di lunghezza p primo, le uniche sequenze ripetute possibili sono quelle di lunghezza p: ma queste corrispondono ai fili monocromatici che abbiamo escluso. Questo ci dice che, nel caso di lunghezza p primo, ogni taglio della collana dopo una perlina produce un filo di perline diverso dalla quale la collana *proviene*. Ovvero, ci sono p fili di perline (uno per ogni taglio possibile della collana) che vanno a formare la stessa collana. La risposta alla nostra domanda di calcolo combinatorio: "quante collane si possono formare dagli $n^p - n$ fili di perle distinti di lunghezza p?" è perciò $\frac{n^p - n}{p}$. Dovendo essere un numero intero, questo prova che p divide $n^p - n$, ovvero il piccolo teorema di Fermat.

Corollario 4.119. *Sia p primo. Per ogni $x \in \mathbb{Z}$, con $(x, p) = 1$, si ha:*

$$x^{p-1} \equiv 1 \ (p)$$

Dimostrazione. L'ipotesi equivale a $[x]_p \in \mathbb{Z}/p\mathbb{Z}^*$. Moltiplicando per l'inverso di $[x]_p$ l'identità fornita dal Teorema 4.118 otteniamo $x^{p-1} \equiv 1 \ (p)$. □

Corollario 4.120. *Dato $[x]_p \in \mathbb{Z}/p\mathbb{Z}^*$, il suo inverso è $[x^{p-2}]_p = [x]_p{}^{p-2}$.*

Esercizio 4.121. *Calcolare 19^{759} in $\mathbb{Z}_7$.*

Svolgimento. Intanto facciamo notare che 19 è congruo a 5 modulo 7, perciò:

$$19^{759} \equiv 5^{759} \ (7)$$

Inoltre, essendo 5 coprimo con 7, dal Corollario 4.119 sappiamo che 5^6 è congruo a 1 modulo 7. Eseguendo la divisione euclidea tra l'esponente 759 e 6 troviamo: $759 = 6 \cdot 126 + 3$. Dunque, dalle proprietà delle potenze segue che:

$$5^{759} = 5^{6 \cdot 126 + 3} = (5^6)^{126} \cdot 5^3$$

Per quanto osservato, $(5^6)^{126} \cdot 5^3 \equiv 5^3 \ (7)$. A questo punto si tratta di calcolare 5^3 modulo 7 che è 6.

Esercizio 4.122. *Risolvere la seguente congruenza polinomiale:*

$$x^9 + x^8 + 3x - 1 \equiv 1 \ (5)$$

Svolgimento. Un *algoritmo* solitamente dispendioso (ma in questo caso non troppo visto il modulo 5), ma sicuramente finito, per cercare le soluzioni di equazioni negli $\mathbb{Z}/m\mathbb{Z}$, è quello di provare tutti gli elementi di $\mathbb{Z}/m\mathbb{Z}$ (che appunto sono finiti).

Vogliamo però usare qualcosa di più ingegnoso (anche perché per moduli *grandi*, l'algoritmo per prova è finito ma può essere molto lungo...). Notiamo subito che x congruo a 0 modulo 5 non è soluzione, possiamo dunque usare il Corollario 4.119 e affermare che $x^4 \equiv 1 \ (5)$. L'equazione da risolvere è dunque equivalente a:

$$x^9 + x^8 + 3x - 1 \equiv x + 1 + 3x - 1 \equiv 1 \ (5)$$

Ovvero ci siamo ridotti a risolvere la congruenza di primo grado $4x \equiv 1 \ (5)$. Osservando che $[4]_5$ è l'inverso di $[4]_5$, si ottiene, moltiplicando entrambi i membri della congruenza per $[4]_5$: $x \equiv 4 \ (5)$.

Osservazione 4.123. Se $x^r \equiv a \ (p)$ e $(r, p-1) = 1$ allora esiste s tale che $r \cdot s \equiv 1 \ (p-1)$. Elevando alla s entrambi i membri della congruenza si ottiene $(x^r)^s \equiv a^s \ (p)$, ovvero $x \equiv a^s \ (p)$. Se eleviamo ora alla r ri-otteniamo la congruenza

di partenza $x^r \equiv a\ (p)$. Perciò l'operazione di elevazione a potenza per un numero primo con $p-1$ è invertibile in $\mathbb{Z}/p\mathbb{Z}$. Ovvero le congruenze che ne risultano sono equivalenti (hanno gli stessi insiemi delle soluzioni).

Esercizio 4.124. *Risolvere la congruenza* $3761 \cdot x^{56} \equiv 7x^3\ (17)$

Svolgimento. Innanzitutto osserviamo che $[0]_{17}$ è ovviamente soluzione della congruenza: infatti sostituendo a x la classe 0 si ottiene $0 \equiv 0\ (17)$.
Detto questo andiamo a cercare se ci sono altre soluzioni tra le classi di $\mathbb{Z}_{17}$ diverse da $[0]_{17}$, ovvero in $\mathbb{Z}_{17}^*$ (dato che 17 è primo). Possiamo dunque moltiplicare entrambi i membri per x^{-3}, ovvero l'inverso di x^3, e ottenere:

$$3761 \cdot x^{53} \equiv 7\ (17)$$

A questo punto riduciamo 3761 ($3761 = 17 \cdot 221 + 4$) e dividiamo 53 per la cardinalità di $\mathbb{Z}_{17}^*$ ($53 = 16 \cdot 3 + 5$). La congruenza si può dunque riscrivere come:

$$4 \cdot x^{16 \cdot 3 + 5} \equiv 7\ (17)$$

da cui:

$$4 \cdot x^5 \equiv 7\ (17)$$

A questo punto va trovato l'inverso di 4 in $\mathbb{Z}_{17}$ (si può fare con l'algoritmo di Euclide ma è piuttosto facile in questo caso notare che -4 è tale che $4 \cdot (-4) = -16$ è congruo a 1 modulo 17). Moltiplicando per l'inverso di 4 (ovvero -4) entrambi i membri della congruenza si ottiene:

$$x^5 \equiv 7 \cdot (-4) \equiv 6\ (17)$$

A questo punto potremmo calcolarci tutte le potenze quinte in $\mathbb{Z}_{17}^*$ e vedere se ce ne sono di uguali a 6. Un metodo migliore si ottiene però usando l'Osservazione 4.123. Eleviamo i due membri della congruenza per l'inverso di 5 modulo 16. È facile vedere che la classe di -3 è l'inversa di $[5]_{16}$, ma scegliamo un rappresentante positivo per non dover poi calcolare di nuovo inversi:

$$(x^5)^{13} \equiv 6^{13}\ (17)$$

Abbiamo appunto che:

$$(x^5)^{13} = x^{16 \cdot 4 + 1} = (x^{16})^4 \cdot x \underbrace{\equiv}_{teo.Fermat} x\ \ (17)$$

Ovvero:

$$x \equiv 6^{13}\ (17)$$

Non rimane altro che calcolare 6^{13} in $\mathbb{Z}_{17}$. Si ha che $6^2 = 36 \equiv 2\ (17)$ e perciò $6^4 \equiv 4\ (17)$ da cui $6^8 = -1\ (17)$ e infine:

$$6^{13} = 6^8 \cdot 6^4 \cdot 6 \equiv -24 \equiv 10\ \ (17)$$

Si ha dunque che, oltre alla soluzione 0 già trovata, si ha $x \equiv 10\ (17)$.

Concludiamo il paragrafo con la generalizzazione del corollario 4.119 ad un modulo non necessariamente primo. Il piccolo teorema di Fermat poteva essere ottenuto come corollario del seguente risultato.

Teorema 4.125 (Teorema di Eulero)**.** *Sia* $m \in \mathbb{Z}$ *maggiore di* 1 *allora per ogni* $x \in \mathbb{Z}$ *tale che* $(x, m) = 1$ *si ha:*

$$x^{\phi(m)} \equiv 1\ (m)$$

DIMOSTRAZIONE. Indichiamo con $[a_i]_m$ per $1 \leq i \leq \phi(m)$ i $\phi(m)$ elementi di $\mathbb{Z}/m\mathbb{Z}^*$. Per ogni $x \in \mathbb{Z}$ tale che $(x, m) = 1$, l'applicazione

$$\varphi_x : \mathbb{Z}/m\mathbb{Z}^* \longrightarrow \mathbb{Z}/m\mathbb{Z}^*$$

che ad ogni $[a_i]_m$ associa $[x]_m \cdot [a_i]_m$ è bigettiva. Per dimostrarlo basta osservare che se $[x]_m \cdot [a_i]_m = [x]_m \cdot [a_j]_m$, moltiplicando per l'inverso di $[x]_m$ (che esiste in quanto $(x, m) = 1$), si ha $[a_i]_m = [a_j]_m$. Ovvero φ_x è iniettiva tra due insiemi della stessa cardinalità.

Questo dimostra che, per ogni $x \in \mathbb{Z}$ con $(x, m) = 1$, l'insieme

$$\{[x]_m \cdot [a_1]_m, [x]_m \cdot [a_2]_m, \ldots, [x]_m \cdot [a_{\phi(m)}]_m\}$$

è uguale a $\mathbb{Z}/m\mathbb{Z}^*$ (contenendo tutti e soli gli elementi di $\mathbb{Z}/m\mathbb{Z}^*$). Perciò:

$$\prod_{i=1}^{\phi(m)} [x]_m \cdot [a_i]_m = \prod_{i=1}^{\phi(m)} [a_i]_m$$

Moltiplicando per l'inverso di $\prod_{i=1}^{\phi(m)} [a_i]_m$ (che esiste perché il prodotto di elementi di $\mathbb{Z}/m\mathbb{Z}^*$ è un elemento di $\mathbb{Z}/m\mathbb{Z}^*$) si ottiene:

$$[x^{\phi(m)}]_m = [1]_m$$

□

Corollario 4.126. *Dato $[x]_m \in \mathbb{Z}/m\mathbb{Z}^*$, il suo inverso è $[x]_m{}^{\phi(m)-1}$.*

Parte II

Strutture algebriche

CAPITOLO 5

I gruppi

1. Definizione e prime proprietà

In matematica riconoscere strutture è sicuramente uno degli aspetti più importanti. In particolare noi considereremo insiemi su cui siano definite una o più operazioni, che verificano certe proprietà, le quali - di volta in volta - definiscono la struttura studiata. In particolare, in questo capitolo, tratteremo la struttura di gruppo, partendo dalla definizione di strutture *intermedie*.

Definizione 5.1. $(G, *)$, dove G è un insieme non vuoto e $*$ una operazione su G è chiamato **magma**.

Definizione 5.2. Un magma $(G, *)$ per cui $*$ sia associativa, ovvero tale che per ogni $a, b, c \in G$: $(a * b) * c = a * (b * c)$, si dice **semigruppo**.

Definizione 5.3. Un semigruppo $(G, *)$ con identità, ovvero esiste in G un elemento e tale che per ogni g in G: $e * g = g * e = g$, detto neutro rispetto a $*$, si dice **monoide**.

Definizione 5.4. Un monoide $(G, *)$ per cui tutti gli elementi hanno inverso si dice **gruppo**. Un gruppo con un numero finito di elementi si dice **finito**.

Esempio 5.5. $(\mathbb{N}, *)$ dove $*$ è l'operazione definita da $a * b = a^b$ è un magma, e non è un semigruppo in quanto l'operazione $*$ non è associativa. Basta osservare che per esempio:

$$64 = (2^3)^2 = (2 * 3) * 2 \neq 2 * (3 * 2) = 2^9 = 512$$

Esercizio 5.6. *Mostrare che* $(\mathbb{Z}, -)$ *è un magma, ma non un semigruppo.*

Esempio 5.7. $(\mathbb{N} \setminus \{0\}, +)$ è un semigruppo, ma non è un monoide (abbiamo tolto proprio l'identità della somma dall'insieme considerato).

Esempio 5.8. $(\wp(A), \cap)$, ovvero l'insieme delle parti di A con l'operazione di intersezione, è un monoide, ma non è un gruppo.

Come detto, in questo capitolo, ci interessiamo in particolare della struttura di gruppo, dunque riassumiamo nella definizione che segue le proprietà che la coppia $(G, *)$, con G insieme non vuoto, e $*$ operazione su G, deve rispettare per essere un gruppo.

Definizione 5.9. $(G, *)$ si dice un **gruppo** se sono verificate le seguenti proprietà:

(1) $*$ è associativa in G:

$$\forall a, b, c \in G \quad (a * b) * c = a * (b * c)$$

(2) Esiste in G un elemento neutro (o identità) per $*$:

$$\exists e \in G, \forall x \in G \quad e * x = x * e = x$$

(3) Ogni elemento di G possiede un inverso $*$:

$$\forall x \in G, \exists y \in G \quad x * y = y * x = e$$

Osservazione 5.10. Ricordiamo che per stabilire che $(G, *)$ è un gruppo (come una qualsiasi delle altre strutture definite precedentemente), dobbiamo assicurarci che $*$ sia una operazione su G secondo la definizione data in 1.42. Ovvero, per ogni a, b in G, $a * b$ deve essere un elemento di G.

Definizione 5.11. Un gruppo $(G, *)$ si dice **abeliano** se l'operazione $*$ è commutativa in G, ovvero per ogni $x, y \in G$ si ha che $x * y = y * x$.

Esempio 5.12. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m\mathbb{Z}, +)$ sono esempi di gruppi abeliani (detti *additivi* per indicare l'operazione corrispondente).

Se indichiamo con $\mathbb{Q}^*$ l'insieme degli invertibili di $\mathbb{Q}$ rispetto alla moltiplicazione (che coincide con $\mathbb{Q}$ senza lo 0, così come per $\mathbb{R}$ e $\mathbb{C}$, e a differenza di $\mathbb{Z}/m\mathbb{Z}$) e usiamo analoga notazione per gli altri insiemi numerici è facile provare che $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ sono gruppi abeliani (*moltiplicativi*).

Dato $n \in \mathbb{N}$, se con Ξ_n indichiamo il sottoinsieme di $\mathbb{C}$ delle radici n-esime dell'unità ($\Xi_n = \{x \in \mathbb{C} | x^n = 1\}$), allora $(\Xi_n, \cdot)$ è un gruppo con n elementi.

Esercizio 5.13. *Provare che dato un insieme X (con $|X| > 2$) indicando con $S(X)$ l'insieme delle funzioni bigettive da X in se stesso e con $\circ$ l'operazione di composizione tra funzioni, $(S(X), \circ)$ è un gruppo non abeliano.*

Svolgimento. Proviamo qui solamente la non commutatività di $\circ$ in $S(X)$, e lasciamo al lettore la prova del fatto che $(S(X), \circ)$ è un gruppo.

Siano $a, b, c \in X$, e consideriamo i seguenti due elementi σ_1, σ_2 di $S(X)$:

$$\sigma_1(x) = \begin{cases} a \text{ se } x = b \\ b \text{ se } x = a \\ x \text{ altrimenti} \end{cases} \qquad \sigma_2(x) = \begin{cases} c \text{ se } x = b \\ b \text{ se } x = c \\ x \text{ altrimenti} \end{cases}$$

In pratica σ_1 scambia a con b e lascia fissi tutti gli altri elementi di X, analogamente σ_2 scambia b con c e lascia fisso tutto il resto. Allora si ha che:

$$(\sigma_1 \circ \sigma_2)(x) = \begin{cases} b \text{ se } x = a \\ c \text{ se } x = b \\ a \text{ se } x = c \\ x \text{ altrimenti} \end{cases} \qquad (\sigma_2 \circ \sigma_1)(x) = \begin{cases} c \text{ se } x = a \\ a \text{ se } x = b \\ b \text{ se } x = c \\ x \text{ altrimenti} \end{cases}$$

Da cui segue che $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$.

Esercizio 5.14. *Provare (per chi conosce le matrici) che $(GL_n(\mathbb{R}), \cdot)$, noto come* **gruppo lineare** *di ordine n è un gruppo non abeliano, dove con $GL_n(\mathbb{R})$ abbiamo indicato l'insieme delle matrici quadrate di ordine n con determinante diverso da 0 (ovvero invertibili), e con $\cdot$ il prodotto riga per colonna tra matrici.*

Esempio 5.15 (Gruppo diedrale)**.** Indichiamo con D_n l'insieme delle isometrie del piano $\mathbb{R}^2$ che mandano un poligono regolare di n lati in sé. Vogliamo mostrare che $(D_n, \circ)$ è un gruppo, non commutativo con $2 \cdot n$ elementi.

Osserviamo che ogni elemento di D_n deve lasciare fisso il baricentro del poligono e deve mandare vertici in vertici (basta ricordarsi che gli elementi di D_n sono isometrie).

Dunque in D_n ci sono sicuramente le n rotazioni r_i di centro il baricentro del poligono e di angolo $i \cdot \frac{2\pi}{n}$ al variare di i tra 1 e n: è facile osservare che r_i si ottiene componendo i volte r_1, ovvero $r_i = {r_1}^i$.

Inoltre, avendo ogni poligono regolare di n lati n assi di simmetria, in D_n ci saranno le n simmetrie rispetto a questi assi che indicheremo con $S_1, ..., S_n$. Se n è dispari gli assi sono le n rette distinte che congiungono gli n vertici al baricentro, se n è pari gli assi sono le $n/2$ rette distinte che congiungono i vertici al baricentro (infatti ognuna di queste rette passa per due vertici) e le $n/2$ rette distinte che congiungono i punti medi dei lati con il baricentro (anche in questo caso ogni retta passa per due punti medi distinti).

Abbiamo dunque trovato $2 \cdot n$ elementi distinti di D_n. Per concludere che questi sono tutti gli elementi di D_n basta osservare che, fissato un vertice V del poligono, una isometria che lascia fisso tale poligono è completamente determinata una volta stabilita l'immagine V' di V (e abbiamo n possibilità: il numero dei vertici) e l'immagine di un vertice adiacente a V (e in questo caso abbiamo 2 possibilità: uno dei due vertici adiacenti a V'). Dunque D_n ha proprio $2 \cdot n$ elementi che sono quelli da noi individuati.

Ora ci rimane da mostrare che D_n è un gruppo.
$\circ$ *è una operazione su* D_n. Componendo due isometrie che lasciano fisso un poligono P otteniamo un'isometria che lascia fisso il poligono P.

Possiamo dire anche qualcosa di più: indichiamo con r la rotazione r_1 e scegliamo una delle simmetrie S di D_n. Sappiamo già che per ogni j si ha $r_j = r^j$, ora mostriamo che, per ogni i, esiste k tale che $S_i = S \circ r^k$. Osserviamo che la composizione di due simmetrie rispetto a due rette incidenti è una rotazione di centro il punto di intersezione e angolo il doppio dell'angolo formato dalle due rette. In particolare si ha che $S \circ S_i$ sarà uguale ad una certa r_k (ovvero r^k) di D_n. Da questo segue che $S_i = S^{-1} \circ r^k$ ma l'inversa di una simmetria assiale S è S stessa, dunque $S_i = S \circ r^k$. Concludendo, fissata una simmetria $S \in D_n$, si ha che:

$$D_n = \{S^t \circ r^j | 0 \leq j \leq n-1,\ 0 \leq t \leq 1\}$$

Esercizio 5.16. *Studiare la legge di composizione tra due elementi generici* $S^t \circ r^j$ *e* $S^h \circ r^i$ *di* D_n *e mostrare che non vale la proprietà commutativa.*

$\circ$ *è associativa.* La composizione di funzioni è in generale associativa, dunque lo è se ci restringiamo al sottoinsieme delle isometrie dal piano in sé.
Esiste in D_n *l'elemento neutro per* $\circ$. L'identità del piano è un'isometria (usando le nostre notazioni, corrisponde alla rotazione r_n di centro il baricentro del poligono e di angolo 2π) che per definizione (lascia fissi tutti i punti) verifica le proprietà di elemento neutro per $\circ$.
Per ogni elemento di D_n *esiste l'inverso.* Fissata una qualsiasi simmetria S in D_n basta far vedere che $S \circ r^k$ ha inverso per ogni k. È facile mostrare che tale inverso è $r^{n-k} \circ S$.

Definizione 5.17. Il gruppo $(D_n, \circ)$ è detto **gruppo diedrale**.

Dopo aver visto alcuni esempi di gruppo, cominciamo a mostrare alcune delle proprietà che caratterizzano la struttura di gruppo.

Proposizione 5.18. *L'elemento neutro e di un gruppo $(G, *)$ è unico.*

DIMOSTRAZIONE. Supponiamo che e ed e' siano due elementi neutri in $(G, *)$ gruppo. Allora:

$$e' \underbrace{=}_{e \text{ è elemento neutro}} e' \cdot e \underbrace{=}_{e' \text{ è elemento neutro}} e$$

□

Proposizione 5.19. *Sia $(G, *)$ un gruppo. Per ogni $a \in G$ esiste un unico inverso.*

DIMOSTRAZIONE. Sia $a \in G$. Che esista un inverso di a lo sappiamo per definizione di gruppo, dobbiamo quindi dimostrare l'unicità. Supponiamo b e c siano due inversi di a allora abbiamo:

$$c = e * c \underbrace{=}_{b \text{ é inverso di } a} (b * a) * c \underbrace{=}_{prop.associativa} b * (a * c) \underbrace{=}_{c \text{ é inverso di } a} b * e = b$$

□

Notazioni: vista l'unicità dell'inverso di un elemento a di un gruppo $(G, *)$, possiamo indicare tale inverso con il simbolo a^{-1} (cioè facendo riferimento solo all'elemento a di cui è inverso). Inoltre per un generico gruppo $(G, *)$, useremo la notazione moltiplicativa, scrivendo x^n (con $n \in \mathbb{N}^+$) per indicare l'elemento:

$$\underbrace{x * \ldots * x}_{n \text{ volte}}$$

e scrivendo x^{-n} per indicare l'elemento:

$$\underbrace{x^{-1} * \ldots * x^{-1}}_{n \text{ volte}}$$

Per convenzione poniamo inoltre $x^0 = e$.

Solo quando l'operazione di un gruppo G sia esplicitamente l'addizione, indicheremo l'inverso dell'elemento x di G con il simbolo $-x$, scrivendo $n \cdot x$ in luogo di x^n.

Corollario 5.20. *Sia $(G, *)$ un gruppo. Per ogni $a \in G$, $(a^{-1})^{-1} = a$.*

Esercizio 5.21. *Con le notazioni introdotte dimostrare che:*

(1) *L'inverso di x^n è uguale all'inverso di x elevato alla n, ovvero:*

$$(x^n)^{-1} = (x^{-1})^n$$

(2) *Valgono le usuali proprietà di calcolo delle potenze, ovvero:*

$$\begin{cases} x^m \cdot x^n = x^{m+n} \\ (x^m)^n = x^{m \cdot n} \end{cases}$$

Proposizione 5.22. *Sia $(G, *)$ un gruppo. Dati $a, b \in G$ l'inverso di $a * b$ è l'elemento $b^{-1} * a^{-1}$.*

DIMOSTRAZIONE. Per dimostrare questo risultato basta verificare che:

$$(a * b) * (b^{-1} * a^{-1}) = e$$

Usando la proprietà associativa di $*$ abbiamo che:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e$$

□

Esercizio 5.23. *Sia $(G,*)$ un gruppo. Dati $a_1,\dots,a_n \in G$ l'inverso di $a_1 * \dots * a_n$ è l'elemento ${a_n}^{-1} * \dots * {a_1}^{-1}$.*

I seguenti esercizi forniscono proprietà caratterizzanti i gruppi abeliani.

Esercizio 5.24. *Sia $(G,*)$ un gruppo, dimostrare che è abeliano se e solo se per ogni $a,b \in G$, si ha che $(a*b)^{-1} = a^{-1} * b^{-1}$.*

Esercizio 5.25. *Sia $(G,*)$ un gruppo, dimostrare che è abeliano se e solo se $\forall a,b \in G$ si ha che $(a*b)^2 = a^2 * b^2$.*

Svolgimento. Se $(G,*)$ è abeliano per ogni a,b in G si ha che:

$$(a*b)^2 = (a*b)*(a*b) \underbrace{=}_{prop.ass.} a*(b*a)*b \underbrace{=}_{prop.com.} a*(a*b)*b \underbrace{=}_{prop.ass.} a^2*b^2$$

Viceversa se per ogni $a,b \in G$ vale che:

$$\underbrace{a*a*b*b}_{a^2*b^2} = \underbrace{a*b*a*b}_{(a*b)^2}$$

allora moltiplicando entrambe i membri a sinistra per a^{-1} e a destra per b^{-1} si ha:

$$a^{-1}*(a*a*b*b)*b^{-1} = a^{-1}*(a*b*a*b)*b^{-1}$$

ovvero $a*b = b*a$, cioè G è abeliano.
Un'altra proprietà molto importante, comune a tutti i gruppi, è la seguente:

Proposizione 5.26 (Legge di cancellazione)**.** *Sia $(G,*)$ un gruppo, allora per ogni a,b,c di G si ha:*

$$a*b = a*c \Leftrightarrow b = c \Leftrightarrow b*a = c*a$$

Dimostrazione. Da $b=c$ segue che $a*b = a*c$ e $b*a = c*a$ (**attenzione** non è vero in generale che, se G non è commutativo, $a*b$ sia uguale a $c*a$).

Viceversa dimostriamo che se $a*b = a*c$ allora $b=c$ (la dimostrazione che da $b*a = c*a$ segua $b=c$ è del tutto analoga). Consideriamo a^{-1} inverso di a in G, abbiamo che:

$$b = e*b = (a^{-1}*a)*b = a^{-1}*(a*b) \underbrace{=}_{ipotesi} a^{-1}*(a*c) = (a^{-1}*a)*c = e*c = c$$

□

Osservazione 5.27. Abbiamo incontrato degli insiemi in cui la legge di cancellazione non vale. Consideriamo per esempio il prodotto in $\mathbb{Z}_6$, è vero che $[2]_6 \cdot [3]_6$ è uguale a $[4]_6 \cdot [3]_6$, ma non è vero che $[2]_6 = [4]_6$. Osserviamo che $(\mathbb{Z}_6,*)$ non è un gruppo e, *incidentalmente ma non troppo*, che $[3]_6$ non è invertibile in $\mathbb{Z}_6$. *Non troppo* in quanto, se $[3]_6$ fosse stato invertibile, avremmo potuto procedere come nella dimostrazione della Proposizione 5.26.

Corollario 5.28. *Dati $a,b \in G$ gruppo, esiste sempre, ed è unico, un elemento x di G tale che $a*x = b$.*

Dimostrazione. Per l'esistenza basta osservare che l'elemento $x = a^{-1}*b$ di G soddisfa l'uguaglianza $a*x = b$. Dalla legge di cancellazione segue che se x e y in G sono tali che $a*x = b = a*y$, allora $x = y$. □

Esercizio 5.29. *Un monoide $(E,*)$ per cui valga la proprietà descritta nel Corollario 5.28 è un gruppo.*

Svolgimento. Infatti se indichiamo con e l'elemento neutro di E, per ogni $a \in E$ si può considerare l'uguaglianza $a * x = e$. Per ipotesi esiste un (unico) elemento in E che soddisfa l'uguaglianza, ovvero ogni $a \in E$ ha inverso.

2. Sottogruppi

Abbiamo introdotto insiemi G su cui sia definibile una struttura di gruppo, siamo interessati, nel caso di sottoinsiemi H di G, alla possibilità di *ritrovare* in essi tale struttura.

Definizione 5.30. Dato un gruppo $(G, *)$, un sottoinsieme non vuoto H di G si dice un **sottogruppo** di $(G, *)$ (e scriveremo $(H, *) < (G, *)$) se $(H, *)$ è esso stesso un gruppo. Se H è diverso da G il sottogruppo $(H, *)$ è detto **proprio**.

Notazione: finora abbiamo insistito con la notazione che ricorda come un gruppo sia una coppia formata da un insieme e un'operazione definita su di esso avente alcune proprietà. D'ora innanzi, proprio con l'intenzione di non appesantire la notazione, ometteremo il riferimento all'operazione laddove non ci sembri ambigua tale omissione. Con questa convenzione, laddove non si creino ambiguità, per indicare che $(H, *)$ è un sottogruppo di $(G, *)$ useremo la notazione $H < G$.

Esempio 5.31. Sia G un gruppo, è facile osservare che G e l'insieme $\{e\}$, contenente solo l'elemento neutro di G, sono sempre sottogruppi di G. Tali sottogruppi vengono chiamati **sottogruppi banali** di G.

Esempio 5.32. $(S(\mathbb{R}^2), \circ)$, con $S(\mathbb{R}^2)$ insieme delle bigezioni dal piano in se stesso, è un gruppo (caso particolare dell'Esercizio 5.13). Descriviamone alcuni sottogruppi non banali:

(1) Abbiamo già osservato (Esempio 5.15) che D_n è un gruppo, essendo contenuto strettamente in $S(\mathbb{R}^2)$, è un suo sottogruppo non banale.
(2) Il sottoinsieme H di $S(\mathbb{R}^2)$ delle traslazioni f_v di vettore v è un sottogruppo di $S(\mathbb{R}^2)$. Infatti: la traslazione di vettore 0 è l'identità; la composizione di due traslazioni f_v, f_w è una traslazione ($f_v \circ f_w = f_{w+v}$ dove $+$ è la somma componente per componente di $\mathbb{R}^2$); l'operazione di composizione[1] di traslazioni è associativa (lo è in generale la composizione di funzioni); per ogni traslazione, esiste un inverso in H (l'inverso di f_v è f_{-v}).
(3) Il sottoinsieme H di $S(\mathbb{R}^2)$ delle rotazioni f_θ di angolo θ è un sottogruppo di $S(\mathbb{R}^2)$. Infatti: la rotazione di angolo $\theta = 0$ è l'identità; la composizione di due rotazioni, di angolo rispettivamente α e β, è una rotazione di angolo $\alpha + \beta$; come per le traslazioni, la composizione è associativa; l'inverso di una rotazione f_θ è la rotazione $f_{2\pi-\theta}$.

Osservazione 5.33. In generale, non è vero che un generico sottoinsieme H di un gruppo G è un sottogruppo di G. Innanzitutto perché, per ogni coppia di elementi a, b in H è definito $a * b \in G$, ma non è assicurato che $a * b$ sia in H, ovvero la restrizione di $*$ ad H potrebbe non essere una operazione su H.

Esempio 5.34. Sia $G = \{\mathbb{Z}, +\}$. Il sottoinsieme $H = \{-3, -2, -1, 0, 1, 2, 3\}$, pur contenendo l'elemento neutro rispetto al $+$, e contenendo per ogni suo elemento il rispettivo inverso, non è chiuso per l'operazione $+$ e quindi non è un sottogruppo. Infatti, ad esempio, $3 + 2$ non è un elemento di H.

[1] Facciamo notare una ambiguità di linguaggio: abbiamo usato il termine *composizione* sia per indicare l'operazione considerata, sia per indicare il risultato della composizione tra due elementi.

Definizione 5.35. Dato un insieme G su cui è definita una operazione $*$, un sottoinsieme H di G per cui la restrizione di $*$ agli elementi di H sia una operazione per H (ovvero per ogni g, r in H, $g * r$ appartiene ad H), si dice **chiuso rispetto all'operazione** $*$. Se ogni elemento di H ha l'inverso in H rispetto a $*$, H si dice **chiuso per l'inverso**.

Osservazione 5.36. Dato $(G, *)$ gruppo, se è vero come abbiamo osservato che la restrizione di $*$ ad un sottoinsieme H di G può non essere una operazione su H, è vero anche però che se lo è, sicuramente è associativa. La proprietà associativa infatti vale per tutti gli elementi di G, dunque *a maggior ragione* vale per tutti gli elementi di H che sono un sottoinsieme di quelli di G.

Questa osservazione ci fa intuire come, per provare che un sottoinsieme H non vuoto di un gruppo G è un sottogruppo, non sia necessario verificare tutte le proprietà riportate nella Definizione 5.9 di gruppo (perché alcune saranno conseguenza del fatto che H è contenuto in G).

Lemma 5.37. *Un sottoinsieme non vuoto H di un gruppo $(G, *)$ è un sottogruppo di G se e solo se:*

$$a, b \in H \Rightarrow a * b \in H \tag{2.1}$$

$$a \in H \Rightarrow a^{-1} \in H. \tag{2.2}$$

Dimostrazione. Per definizione se $H < G$, ovvero è un gruppo di per se stesso, allora valgono le condizioni 2.1 e 2.2.

Viceversa se valgono 2.1 e 2.2 per provare che H verifica tutte le proprietà di gruppo rimane da mostrare che $e \in H$ (del fatto che l'operazione continui ad essere associativa in H abbiamo già detto). Per ipotesi H è non vuoto, quindi esiste $a \in H$. La condizione 2.2 ci dice che $a^{-1} \in H$, e dalla condizione 2.1 segue che $e = a * a^{-1} \in H$. □

Esercizio 5.38. *Provare che, se $(G, *)$ è un gruppo finito, un sottoinsieme H di G è un sottogruppo se e solo se è chiuso per l'operazione $*$.*

Svolgimento. Una implicazione è ovvia: se H è un sottogruppo, per definizione è chiuso per l'operazione. Viceversa supponiamo H sia un sottoinsieme di G chiuso per $*$, per dimostrare la tesi (dal lemma 5.37) basta verificare che per ogni a di H, a^{-1} appartiene ad H. Consideriamo il sottoinsieme $S = \{a^i | i \in \mathbb{Z}\}$ delle potenze intere di a. S è contenuto in H, ed ovviamente è finito (essendo l'intero G finito). Dunque devono esistere due interi distinti $i > j$ tali che $a^i = a^j$ (fossero tutte diverse le potenze intere di a, S non sarebbe finito). Allora si ha che $a^{i-j} = e$, ovvero:

$$a^{i-j-1} * a = e$$

Dunque a^{i-j-1} è l'inverso di a e sta in H.

Lemma 5.39. *Un sottoinsieme H non vuoto di un gruppo $(G, *)$ è un sottogruppo se e solo se per ogni x, y in H l'elemento $x * y^{-1}$ è un elemento di H.*

Dimostrazione. Se H è un sottogruppo di G allora, per definizione, H è chiuso per l'operazione $*$ e per ogni elemento esiste l'inverso in H. Dunque per ogni $x, y \in H$ anche $y^{-1} \in H$ e di conseguenza $x * y^{-1}$ appartiene ad H.

Viceversa mostriamo che, se per ogni x, y di H l'elemento $x * y^{-1}$ sta ancora in H, allora H è chiuso per l'operazione $*$, e per ogni x in H esiste l'inverso in H.

H non è vuoto, dunque esiste un elemento x appartenente ad H. Considerando la *coppia* (x, x) si ha per ipotesi che $x * x^{-1} = e$ è un elemento di H, e considerando la coppia di elementi (e, x) di H si ha che $e * x^{-1} = x^{-1}$ sta in H.

Per concludere ci resta da mostrare che $*$ è una operazione su H. Osserviamo che, per ogni coppia x, y di elementi di H, $y^{-1} \in H$ (appena dimostrato). Dunque considerando la coppia x, y^{-1} di H si ottiene che $x * (y^{-1})^{-1} = x * y$ è in H. □

Definizione 5.40. Sia $(G, *)$ un gruppo, l'insieme $Z(G)$ degli elementi g di G che commutano con ogni elemento di G si dice **centro** di G.

$$Z(G) = \{g \in G | \forall x \in G \; x * g = g * x\}$$

Esercizio 5.41. *Provare che $Z(G)$ è un sottogruppo di G.*

Svolgimento. Osserviamo che $Z(G)$ non è mai vuoto, perché l'elemento neutro e appartiene a $Z(G)$ qualsiasi sia il gruppo G.

Siano $x, y \in Z(G)$, vogliamo provare (Lemma 5.39) che $x * y^{-1}$ è un elemento di $Z(G)$, ovvero per ogni g di G deve essere $g * (x * y^{-1}) = (x * y^{-1}) * g$. Sappiamo che, per ogni g in G, vale $g * (x * y) = (x * y) * g$. Moltiplicando questa uguaglianza, a sinistra e a destra, per l'inverso y^{-1} di y, si ottiene:

$$y^{-1} * g * (x * y) * y^{-1} = y^{-1} * (x * y) * g * y^{-1}$$

Sfruttando la proprietà associativa e il fatto che x e y commutano con qualsiasi elemento di G si ottiene a primo membro $(x * y^{-1}) * g$, ed a secondo membro $(x * y^{-1}) * g$.

Facciamo ora un primo esempio, importante, di caratterizzazione completa dei sottogruppi di uno specifico gruppo: $(\mathbb{Z}, +)$.

Teorema 5.42. *I sottogruppi di $(\mathbb{Z}, +)$ sono tutti e soli gli insiemi $n\mathbb{Z}$ definiti, al variare di n in $\mathbb{N}$, come segue:*

$$n\mathbb{Z} = \{n \cdot t | t \in \mathbb{Z}\}$$

Dimostrazione. Lasciamo come esercizio la dimostrazione del fatto che gli insiemi $n\mathbb{Z}$ con $n \in \mathbb{N}$ sono effettivamente sottogruppi di $(\mathbb{Z}, +)$, e mostriamo che se H è un sottogruppo di $(\mathbb{Z}, +)$ allora esiste $n \in \mathbb{N}$ tale che $H = n\mathbb{Z}$.

Se $H = \{0\}$ allora $H = 0\mathbb{Z}$, altrimenti esiste in H un elemento a diverso da 0 e di conseguenza esiste in H un elemento maggiore di zero: infatti H come sottogruppo se contiene a contiene anche $-a$, e uno tra a e $-a$ è positivo. Dunque l'insieme $H^+ = H \cap \mathbb{N}^+$ è non vuoto e, per il principio del buon ordinamento, ha un minimo n. Vogliamo dimostrare che $H = n\mathbb{Z}$.

$n\mathbb{Z}$ è contenuto in H, infatti $n \in H$, e H è, per ipotesi, un sottogruppo e dunque è chiuso per addizione ripetuta di addendi uguali a n.

Viceversa se $h \in H$ e facciamo la divisione euclidea tra h e n otteniamo $h = q \cdot n + r$ con $0 \leq r < n$. Osservando che h e $q \cdot n$, e dunque $r = h - q \cdot n$, stanno in H, si ha che r non può essere positivo, altrimenti apparterrebbe ad H^+ e sarebbe minore di n. Dunque $r = 0$ e h è un multiplo di n, cioè appartiene a $n\mathbb{Z}$. □

Esercizio 5.43. *Siano $H = n\mathbb{Z}$ e $K = m\mathbb{Z}$ due sottogruppi di $(\mathbb{Z}, +)$. H è contenuto in K se e solo se $m|n$.*

Svolgimento. Se m divide n, cioè esiste t in $\mathbb{Z}$ tale che $n = m \cdot t$, allora ogni elemento h di H, che è del tipo $n \cdot s$ per un certo s in $\mathbb{Z}$, si può scrivere anche $m \cdot (t \cdot s)$. Ovvero ogni h in H è anche elemento di K.

Viceversa se H è contenuto in K (ovvero, essendo gruppi, è un sottogruppo di K), allora ogni elemento di H si può scrivere come multiplo di m. In particolare n è un elemento di H e dunque, esiste t in $\mathbb{Z}$ tale che $n = m \cdot t$.

Proposizione 5.44. *Siano H e K sottogruppi del gruppo $(G, *)$ allora l'insieme $H \cap K$ è un sottogruppo di G, ed è il più grande sottogruppo di G contenuto sia in H che in K.*

Dimostrazione. Essendo H e K sottogruppi, l'elemento neutro e di G appartiene sia ad H che a K, e dunque ad $H \cap K$ che risulta essere non vuoto. Ora, se x, y appartengono ad $H \cap K$, allora x, y e y^{-1} appartengono sia ad H che a K, quindi anche $x * y^{-1}$ appartiene ad entrambe i sottogruppi, ovvero ad $H \cap K$. Abbiamo perciò dimostrato che $H \cap K$ è un sottogruppo.

Per concludere basta osservare insiemisticamente che se T è un insieme contenuto sia in H che in K allora $T \subset H \cap K$. □

Esercizio 5.45. *Dati m, n in $\mathbb{Z} \setminus \{0\}$, provare che $n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z}$.*

Svolgimento. Dalla Proposizione 5.44 sappiamo che l'intersezione H tra i due sottogruppi $n\mathbb{Z}$ e $m\mathbb{Z}$ di $\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$, e dal Teorema 5.42 sappiamo che H è della forma $d\mathbb{Z}$ con $d \in \mathbb{Z}$. Vogliamo dimostrare che d è il minimo comun multiplo tra n e m. Per far questo facciamo vedere che ogni elemento di H si può scrivere come $[n, m] \cdot t$ con t intero, e viceversa che ogni elemento di questo tipo (ovvero appartenente a $[n, m]\mathbb{Z}$) è un elemento di H.

Sia $h \in H$, ovvero h è un multiplo intero sia di n che di m, allora, per definizione di minimo comun multiplo, è un multiplo intero di $[n, m]$. Perciò $h \in [n, m]\mathbb{Z}$.

Viceversa sia $z \in [n, m]\mathbb{Z}$, cioè della forma $[n, m] \cdot t$ con t intero. z è un multiplo di n (dunque appartiene a $n\mathbb{Z}$), ed è un multiplo intero di m (dunque appartiene a $n\mathbb{Z}$), ovvero z appartiene a $n\mathbb{Z} \cap m\mathbb{Z}$.

Possiamo generalizzare il risultato della Proposizione 5.44 anche ad intersezioni di famiglie infinite di sottogruppi.

Proposizione 5.46. *Sia $(G, *)$ un gruppo e $\{G_i\}_{i \in I}$ una famiglia di sottogruppi di G (con I anche infinito), allora $\mathcal{G} = \bigcap_{i \in I} G_i$ è il più piccolo sottogruppo di G contenuto in tutti i G_i.*

Dalla Proposizione 5.46 segue che, dato un sottoinsieme S di $(G, *)$, esiste sempre il più piccolo sottogruppo di $(G, *)$ che contiene S.

Proposizione 5.47. *Per ogni sottoinsieme non vuoto S di G esiste un sottogruppo K di G che: contiene l'insieme S, e tale che ogni sottogruppo di G che contiene S, contiene anche K.*

Dimostrazione. Consideriamo l'insieme $\Im$ dei sottogruppi di G che contengono l'insieme S. Sicuramente $\Im$ non è vuota, in quanto $G \in \Im$. Consideriamo l'insieme $K = \bigcap_{T \in \Im} T$: esso contiene S per definizione. Dalla Proposizione 5.46 segue la tesi. □

Definizione 5.48. Sia S un sottoinsieme non vuoto di un gruppo $(G, *)$. Chiamiamo **sottogruppo generato da** S il più piccolo sottogruppo di G che contiene S, e useremo la notazione $< S >$ per indicarlo.

Esempio 5.49. Abbiamo dimostrato che, dati H e K sottogruppi di un gruppo $(G, *)$, $H \cap K$ è il più grande sottogruppo contenuto sia in H che in K. Ci chiediamo adesso se esiste, e quale sia, il più piccolo sottogruppo T contenente sia H che K.

Se $H \cup K$ fosse un sottogruppo di G allora $H \cup K$ sarebbe il sottogruppo che cerchiamo, ma in generale non è vero che l'unione di sottogruppi è un sottogruppo. Consideriamo per esempio il gruppo $(\mathbb{Z}, +)$ e i sottogruppi H e K rispettivamente dei multipli interi di 3 e dei multipli interi di 5. Osserviamo ad esempio che l'elemento 8, somma di due elementi dell'unione (3 e 5), non è un elemento dell'unione in quanto non è un multiplo né di 3, né di 5.

L'esempio appena fatto mostra che, in generale, l'unione di due sottogruppi non è chiusa per l'operazione del gruppo. La seguente proposizione ci dice che l'unione di due sottogruppi è un sottogruppo solo in un caso particolare.

Proposizione 5.50. *Siano H, K sottogruppi di $(G, *)$. Allora $H \cup K < G$ se e solo se $H \subseteq K$ oppure $K \subseteq H$.*

Dimostrazione. $\Leftarrow$) Se $H \subseteq K$, allora $H \cup K = K$ che per ipotesi è un sottogruppo di G. Analogamente se $K \subseteq H$, allora $H \cup K = H$ che anch'esso è un sottogruppo di G.
$\Rightarrow$) Viceversa, supponiamo che H e K non siano uno contenuto nell'altro, e dimostriamo che la loro unione non è un sottogruppo di G mostrando che non è chiusa rispetto a $*$, proprio come fatto nell'esempio particolare dei multipli di 3 e 5 in $\mathbb{Z}$.

L'ipotesi che H e K non siano contenuti l'uno nell'altro significa che esiste x in G tale che $x \in H \setminus K$, ed esiste y in G tale che $y \in K \setminus H$. Mostriamo che $x * y$ non appartiene all'unione di H e K. Infatti se $x * y$ appartenesse ad H, ovvero se esistesse h in H con $x * y = h$, allora $x^{-1} * h = y$ starebbe in H (infatti H è un sottogruppo e $x \in H$), ma questo è falso per ipotesi ($y \in K \setminus H$). Analogamente si dimostra che $x * y$ non può appartenere a K, e dunque non appartiene a $H \cup K$. $\square$

Abbiamo visto che, in generale, l'unione di sottogruppi non è un sottogruppo, allora come è fatto il più piccolo sottogruppo che contiene $H \cup K$? E più in generale, dato S sottoinsieme di un gruppo G, quali sono gli elementi di $< S >$? La dimostrazione della Proposizione 5.47 non fornisce una risposta chiara a questa questione. Cerchiamo di capirlo procedendo per passi al variare della *numerosità* di S.

Il caso più semplice è quello di un insieme S formato da un unico elemento x. In questo caso, il sottogruppo $< S >$ è indicato anche con $< x >$, e viene chiamato **sottogruppo generato dall'elemento** x. Come è fatto $< x >$? Per essere un sottogruppo (ovvero chiuso per $*$ e per inverso) deve contenere tutte le potenze intere di x. Da questa osservazione e dal seguente esercizio segue che $< x >$ è proprio l'insieme delle potenze intere di x.

Esercizio 5.51. *Dato $(G, *)$ gruppo, e dato x in G, l'insieme H delle potenze intere di x è un sottogruppo di G.*

Svolgimento. H non è vuoto in quanto $x \in H$. Inoltre, se $s, t \in H$, allora sono della forma $s = x^a$, $t = x^b$ (con a, b interi). Perciò:

$$s * t^{-1} = x^a * x^{-b} = x^{\overbrace{a-b}^{\in \mathbb{Z}}} \in H$$

Dal Lemma 5.39 segue che H è un sottogruppo di G.

Osservazione 5.52. In particolare si ha che il sottogruppo $< x >$ generato da un elemento è abeliano.

Studiamo ora il caso di un sottoinsieme S del gruppo G di cardinalità finita $n > 1$: $S = \{x_1, \ldots, x_n\}$. Sappiamo che in $< S >$ devono stare necessariamente almeno tutti i prodotti finiti di elementi di S e tutti gli inversi degli elementi di S. Consideriamo dunque l'insieme S^{-1} degli inversi degli elementi di S: $S^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$ e definiamo $T = S \cup S^{-1}$. Vogliamo provare che $< S >$ è uguale all'insieme H dei prodotti finiti tra gli elementi di T:

$$H = \{t_1 * \ldots * t_k | t_i \in T \text{ e } k \in \mathbb{N}\}$$

Dobbiamo mostrare dunque che H contiene S, che è un sottogruppo di G, e che è il più piccolo insieme con queste due proprietà.

Che H contenga S è ovvio, infatti gli elementi di T appartengono ad H (basta scegliere $k = 1$), e T contiene S per definizione. In particolare H non è vuoto. Inoltre, se r, g sono due elementi di H allora sono della forma $r = t_1 * \ldots * t_k$ $g = a_1 * \ldots * a_l$ con t_i e a_j (al variare di i, j rispettivamente in $\mathbb{N}_k$ e $\mathbb{N}_l$) appartenenti a $S \cup S^{-1}$. Dall'Esercizio 5.23 segue che r^{-1} è uguale a ${t_k}^{-1} * \ldots * {t_1}^{-1}$ (in particolare appartiene ad H), e dunque:

$$g * r^{-1} = (a_1 * \ldots * a_l) * ({t_k}^{-1} * \ldots * {t_1}^{-1}) = a_1 * \ldots * a_l * {t_k}^{-1} * \ldots * {t_1}^{-1}$$

Ovvero $g * r^{-1}$ è un elemento di H, e, dal Lemma 5.39, segue che H è un sottogruppo.

Infine, se K è un sottogruppo di G contenente S, allora anche S^{-1}, e di conseguenza T, è contenuto in K. K deve contenere tutti i prodotti finiti di elementi di suoi sottoinsiemi, e quindi $H \subset K$.

Consideriamo ora il caso di un insieme S infinito, contenuto in un gruppo G. Come in precedenza, se H sottogruppo di G deve contenere S, allora deve contenere anche $S^{-1} = \{x^{-1} | x \in S\}$ e tutti i prodotti finiti tra elementi di $T = S \cup S^{-1}$. Quindi come nel caso precedente di S finito, il sottogruppo H cercato è definito come segue:

$$H =< S >= \{t_1 * ... * t_k | t_i \in T \wedge k \in \mathbb{N}\}.$$

La dimostrazione che H è il più piccolo sottogruppo contenente S è identica a quella vista nel caso S finito.

3. Gruppi ciclici e ordine di un elemento

Dato un gruppo $(G, *)$ e un elemento $x \in G$, abbiamo definito il sottogruppo $< x >$ delle potenze intere di x.

Definizione 5.53. Un gruppo $(G, *)$ si dice **ciclico**, se esiste $x \in G$ tale che $G =< x >$, cioè se per ogni elemento g di G esiste $m \in \mathbb{Z}$ tale che $g = x^m$.

Esempio 5.54. Vediamo alcuni gruppi ciclici tra gli esempi trattati nella prima parte del libro. Come vedremo in seguito, i primi due esempi *in un certo senso* caratterizzano le due tipologie possibili di gruppi ciclici: infiniti e finiti.

(1) $(\mathbb{Z}, +)$ è un gruppo ciclico infinito generato da 1. Infatti ogni $m \in \mathbb{Z}$ può essere visto come $m = \underbrace{1 + ... + 1}_{m \text{ volte}}$.
(2) $(\mathbb{Z}/m\mathbb{Z}, +)$ è un gruppo ciclico finito generato da $[1]_m$. Dunque, tutti i risultati che dimostreremo sui gruppi ciclici finiti varranno in particolare per questo gruppo che abbiamo imparato a conoscere nella prima parte del libro.
(3) $(n\mathbb{Z}, +)$ è un gruppo ciclico infinito generato da n
(4) $(\mathbb{Z}_6^*, \cdot)$ è ciclico generato da $[5]_6$. Infatti $\mathbb{Z}_6^*$ ha due elementi $[1]_6, [5]_6$ entrambi ottenuti dalle potenze di $[5]_6$: $[5]_6^1 = [5]_6$, $[5]_6^2 = [1]_6$.

Osservazione 5.55. Sia $(G, *)$ un gruppo e sia $x \in G$ tale che il sottogruppo ciclico generato da $< x >$ è finito. Allora esistono due interi m e n, con $m > n$ tali che $x^m = x^n$ (altrimenti la funzione f_x da $\mathbb{Z}$ all'insieme finito $< x >$, che ad ogni intero s associa x^s, sarebbe iniettiva). Da questo segue che:

$$x^{m-n} = x^m * x^{-n} = x^n * x^{-n} = e$$

Ovvero, se x genera un sottogruppo finito, allora esiste un $k \in \mathbb{N}^+$ (in questo caso $m - n$) tale che $x^k = e$.

Definizione 5.56. Sia $(G, *)$ un gruppo e sia $x \in G$. Se il sottogruppo ciclico generato da $< x >$ è finito, si chiama **ordine di** x, e lo indicheremo con $o(x)$, il minimo esponente positivo t per cui $x^t = e$. Se $< x >$ non è finito si dice che x ha ordine infinito.

Proposizione 5.57. *Sia $(G, *)$ un gruppo finito e $x \in G$. Se x ha ordine finito, allora $o(x) = | < x > |$ (per questo la cardinalità del gruppo generato si dirà anche* **ordine del gruppo***), ed in particolare:*

$$< x >= \{x, \ldots, \underbrace{x^{o(x)}}_{=e}\}$$

Dimostrazione. Consideriamo il sottogruppo $< x >$ di G. Vogliamo mostrare che tutte le potenze di x con l'esponente che varia tra 1 e $o(x)$ sono distinte. Supponiamo per assurdo esistano $i, j \in \mathbb{N}$ tali che: $1 \leq i < j \leq o(x)$ e $x^i = x^j$. Allora x^{j-i} sarebbe uguale ad e, con $j - i < o(x)$. Assurdo.

Mostriamo infine che ogni potenza intera di x è del tipo x^i con $1 \leq i \leq o(x)$. Per far questo, dato i in $\mathbb{Z}$, siano q e r rispettivamente quoziente e resto della divisione euclidea di i con $o(x)$. Si ha:

$$x^i = x^{q \cdot o(x) + r} = \underbrace{x^{o(x)^q}}_{e} \cdot x^r = x^r$$

Dunque x^i è uguale a x^r con $0 \leq r < o(x)$. Per concludere basta osservare che $x^0 = x^{o(x)} = e$. □

Proposizione 5.58. *Un gruppo $(G, *)$ finito è ciclico se e solo se esiste un elemento x di G di ordine uguale all'ordine del gruppo.*

Esempio 5.59. Abbiamo visto (Esempio 5.54) che $(\mathbb{Z}_6^*, \cdot)$ è ciclico, ma in generale $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ non sempre è ciclico. Ad esempio $\mathbb{Z}_{12}^*$, i cui elementi sono $[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}$, non è ciclico. Infatti, a parte $[1]_{12}$ che sappiamo avere ordine 1, tutti gli altri elementi hanno ordine 2. Non esiste quindi in $\mathbb{Z}_{12}^*$ un elemento di ordine uguale all'ordine del gruppo (che è 4).

Proposizione 5.60. *Siano $(G, *)$ un gruppo e $x \in G$. $x^m = e$ se e solo se $o(x)$ divide m.*

Dimostrazione. Supponiamo che $o(x)$ divida m, allora $m = o(x) \cdot k$ e:

$$x^m = x^{o(x)\cdot k} = (x^{o(x)})^k = e^k = e$$

Viceversa sia m tale che $x^m = e$. Consideriamo la divisione euclidea di m con $o(x)$: $m = o(x) \cdot q + r$ con $0 \leq r < o(x)$. Per ipotesi

$$e = x^m = x^{o(x)\cdot q + r} \underbrace{=}_{prop.potenze} (x^{o(x)})^q \cdot x^r = e \cdot x^r = x^r$$

Cioè r è tale che $x^r = e$. Ma $r < o(x)$ e quindi non può essere positivo (perché $o(x)$ è il minimo esponente positivo a per cui $x^a = e$) e perciò $r = 0$, cioè $o(x)$ divide m. □

Proposizione 5.61. *Tutti i sottogruppi di un gruppo ciclico $(G, *)$ sono ciclici.*

Dimostrazione. I sottogruppi banali (G ed $\{e\}$) di G sono ovviamente ciclici: uno lo è per ipotesi, l'altro perché sottogruppo composto da un unico elemento.

Supponiamo dunque $H < G$ non banale (dunque esiste h in H diverso da e), e sia $G =< g >$ (cioè g un generatore di G). Essendo in particolare h un elemento di G, esiste m intero diverso da zero con $h = g^m$. Essendo H un sottogruppo anche $h^{-1} = g^{-m}$ è in H. Almeno uno tra m e $-m$ è sicuramente positivo dunque l'insieme $A = \{m \in \mathbb{N}^+ | g^m \in H\}$ non è vuoto. Sia s il minimo di A: mostriamo che $H =< g^s >$. Dalla definizione di sottogruppo generato e dal fatto che H è un gruppo contenente $\{g^s\}$, segue che $< g^s > \subset H$.

Viceversa per ogni $h \in H$, come già osservato, $h = g^m$ per un certo m intero. Dalla divisione euclidea di m con s troviamo q e r tali che $m = q \cdot s + r$ e $0 \leq r < s$. Osserviamo che g^r appartiene ad H in quanto:

$$g^r = g^{m - q\cdot s} = \underbrace{g^m}_{h \in H} * \underbrace{(g^s)^{-q}}_{\in < g^s > \subset H}$$

Questo implica $r = 0$, perché m è il minimo intero positivo per cui g^m appartiene ad H. Abbiamo dunque dimostrato che s divide m, ovvero che $h \in < g^s >$. □

Esercizio 5.62. *Sia $(G, *)$ un gruppo. Se H e K sono sottogruppi ciclici di G ed un generatore di H appartiene a K, allora $H \subseteq K$.*

Osservazione 5.63. La dimostrazione della Proposizione 5.61 ricorda molto da vicino l'idea della dimostrazione del Teorema 5.42. Osserviamo d'altra parte come il Teorema 5.42 poteva essere ricavato come corollario della Proposizione 5.61, infatti sappiamo che $(\mathbb{Z}, +)$ è ciclico generato da 1.

A questo punto, possiamo determinare, dati un gruppo $(G, *)$ e un elemento g di ordine finito, l'ordine delle potenze di g in funzione di $o(g)$.

Teorema 5.64. *Sia $(G, *)$ un gruppo e $g \in G$ di ordine n. $\forall\, k \in \mathbb{N}$ vale:*

$$o(g^k) = \frac{n}{(n,k)}$$

DIMOSTRAZIONE. Indichiamo con d il massimo comun divisore (n,k) tra n e k. Possiamo scrivere $k = k_1 \cdot d$ e $n = n_1 \cdot d$ e calcolare $(g^k)^{\frac{n}{d}}$:

$$(g^k)^{\frac{n}{d}} = g^{\frac{k_1 \cdot d \cdot n_1 \cdot d}{d}} = g^{k_1 \cdot d \cdot n_1} = (g^n)^{k_1} = e^{k_1} = e$$

Questo non conclude la dimostrazione perché non è detto che n_1 sia il minimo esponente per cui $(g^k)^{n_1} = e$.

Dalla Proposizione 5.60 si ha che se $(g^k)^a = e$ allora $k \cdot a$ deve essere multiplo di n, cioè esiste h tale che $k \cdot a = n \cdot h$. Da questo segue che $k_1 \cdot a = n_1 \cdot h$, ed essendo $(k_1, n_1) = 1$, si ha che n_1 divide a. Dunque a è della forma $n_1 \cdot t$ con $t \in \mathbb{N}$. Il minimo a maggiore di zero si ottiene per $t = 1$. □

Esercizio 5.65. *Sia $(G, *)$ un gruppo ciclico finito di ordine m, allora ogni sottogruppo H di G ha ordine che divide m.*

Svolgimento. Sia g un generatore di G (ovvero $o(g) = m$). Sappiamo (Proposizione 5.61) che H è ciclico: consideriamo un generatore h di H. Sappiamo che $o(h) = |H|$ e che esiste s intero tale che $h = g^s$ (in quanto g è un generatore di tutto G). Dal teorema 5.64 si ha che:

$$|H| = o(h) = \frac{m}{(m,s)}$$

Perciò $|H| \cdot (m,s) = m$.

Esempio 5.66. Abbiamo osservato (Esempio 5.54) che $(\mathbb{Z}/m\mathbb{Z}, +)$ è un gruppo ciclico finito generato da $[1]_m$ ($o([1]_m) = m$). In particolare, il Teorema 5.64 ci permette di determinare l'ordine di un qualsiasi elemento $[a]_m$ di $\mathbb{Z}/m\mathbb{Z}$, infatti $[a]_m = a \cdot [1]_m$ (in questo caso, essendo esplicito il fatto che stiamo trattando un gruppo additivo, usiamo la notazione $a \cdot n$ in luogo di a^n), dunque:

$$o([a]_m) = \frac{m}{(a,m)}$$

Teorema 5.67 (Teorema dell'elemento primitivo per gruppi finiti abeliani)**.** *Se $(G, *)$ è un gruppo finito abeliano, esiste un elemento $g \in G$ di ordine a uguale al minimo comun multiplo degli ordini di tutti gli elementi di G.*

DIMOSTRAZIONE. Sia $a = \prod_{i=1}^{t} p_i^{k_i}$ la fattorizzazione in primi distinti di a, allora esiste $h_1 \in G$ tale che $p_1^{k_1} | o(h_1)$. Infatti, se nessun elemento di G ha ordine multiplo di $p_1^{k_1}$, allora anche il minimo comun multiplo degli ordini non sarebbe multiplo di $p_1^{k_1}$. Quindi $o(h_1) = a_1 \cdot p_1^{k_1}$. Analogamente, per ogni i compreso tra 1 e t possiamo trovare h_i di ordine $a_i \cdot p_i^{k_i}$, cioè un multiplo di $p_i^{k_i}$.

Definiamo $s_i = h_i^{a_i}$, dal Teorema 5.64 segue che:

$$o(s_i) = \frac{o(h_i)}{(a_i, o(h_i))} = \frac{a_i \cdot p_i^{k_i}}{a_i} = p_i^{k_i}$$

Lasciamo come esercizio la verifica che $g = \prod_{i=1}^{t} s_i$ ha ordine a (osservando che proprio in questa verifica interviene l'ipotesi che G è abeliano). □

Abbiamo definito i gruppi ciclici come quei gruppi G per cui esista un generatore. Adesso vogliamo dimostrare dei risultati generali per i gruppi ciclici che consentano, in base alla cardinalità del gruppo, di contare il numero di generatori, di sottogruppi e di elementi di un certo ordine.

Teorema 5.68. *Sia $(G, *)$ un gruppo ciclico. Se $|G| = \infty$ allora G ha due generatori (uno l'inverso dell'altro), se $|G| = s < \infty$ allora G ha $\phi(s)$ generatori.*

DIMOSTRAZIONE. Supponiamo che a sia un generatore di G, ovvero $G =< a >$. Ogni altro eventuale generatore di G, essendo in particolare un elemento di G, sarà del tipo a^n. a^n è un generatore se e solo se esiste una sua potenza uguale ad a (che è un elemento di G), cioè se e solo esiste m tale che $a^{n \cdot m} = a$. Abbiamo dunque che sono generatori di G tutti e soli gli elementi a^n di G con n tale che:

$$e = a^{n \cdot m} * a^{-1} = a^{n \cdot m - 1}$$

Distinguiamo a questo punto il caso G infinito dal caso G finito.

Se $|G| = \infty$, allora a ha ordine infinito e dunque deve essere $n \cdot m - 1 = 0$. Ovvero n può essere uguale solo ad 1 (e si ottiene a) o -1 (e si ottiene a^{-1}).

Se $|G| = s < \infty$, allora dalla Proposizione 5.60 segue che $a^{n \cdot m - 1} = e$ se e solo se $n \cdot m - 1$ è un multiplo di s, ovvero se e solo $n \cdot m \equiv 1\ (s)$. Questa congruenza ha soluzione se e solo se $(n, s) = 1$. Dunque i generatori distinti di G sono della forma a^n con n minore di s e primo con s. In particolare G ha $\phi(s)$ generatori. □

Teorema 5.69. *Se $(G, *)$ è un gruppo ciclico di cardinalità s finita, allora per ogni divisore d di s esiste uno e un solo sottogruppo H di ordine d.*

DIMOSTRAZIONE. Sia d un divisore di s, cioè esiste $m \in \mathbb{Z}$ tale che $s = m \cdot d$, e consideriamo un generatore a di G.

Esistenza. Consideriamo l'elemento a^m ed il sottogruppo H generato da a^m ($H =< a^m >$). Dal Teorema 5.64 segue che:

$$o(a^m) = \frac{s}{(s, m)} = \frac{s}{m} = d$$

Dunque H è un sottogruppo di G di ordine d.

Unicità. Sia $K < G$ di ordine d, e dimostriamo che K non può essere che $H =< a^m >$. Dalla proposizione 5.61 sappiamo che K, sottogruppo di un gruppo ciclico, è ciclico. Sia k un generatore di K (ovvero $o(k) = d$), essendo a un generatore di G deve esistere l tale che $k = a^l$. Sempre dal Teorema 5.64 sappiamo che:

$$d = o(a^l) = \frac{s}{(s, l)}$$

Questo implica che $(s, l) = m$ (perché abbiamo trovato che d è uguale ad s diviso (s, l), ma anche ad s diviso m), ovvero l è un multiplo di m. Dunque $a^l = (a^m)^t$ per un certo t intero, ed a^l appartiene ad H. Di conseguenza (Esercizio 5.62) $K \subseteq H$. Essendo i due insiemi della stessa cardinalità, questo implica $K = H$. □

Corollario 5.70. *Se G è ciclico di ordine s finito, allora, per ogni divisore d di s, esistono esattamente $\phi(d)$ elementi di ordine d in G.*

DIMOSTRAZIONE. Dal Teorema 5.69 sappiamo che esiste un solo sottogruppo H (ciclico) di ordine d che contiene tutti gli elementi di ordine d. Infatti, se a di ordine d non appartenesse ad H, il sottogruppo $< a >$ avrebbe ordine d e sarebbe diverso da H. Gli elementi di G di ordine d sono quindi i generatori di H, che dal Teorema 5.68 applicato ad H, gruppo ciclico di ordine d, sappiamo essere $\phi(d)$. □

Concludiamo il paragrafo con alcuni risultati sui gruppi $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$. Usando il teorema di Ruffini (che dimostreremo solo nella parte relativa all'anello dei polinomi a coefficienti in un campo (vedi Teorema 6.64), ma che spesso è noto in quanto presente nel programma delle scuole superiori) possiamo dimostrare che:

Teorema 5.71. *Se p è primo allora $(\mathbb{Z}/p\mathbb{Z}^*, \cdot)$ è ciclico.*

Dimostrazione. Dal Teorema 5.67 sappiamo che in $\mathbb{Z}/p\mathbb{Z}^*$ esiste un elemento a di ordine h, con h uguale al minimo comun multiplo degli ordini di tutti gli elementi di $\mathbb{Z}/p\mathbb{Z}^*$. Quel che dobbiamo dimostrare (Proposizione 5.58) è che $h = p-1$. Sicuramente, essendo $|\mathbb{Z}/p\mathbb{Z}^*| = p-1$, $h \leq p-1$.

D'altra parte, essendo h un multiplo dell'ordine di qualsiasi elemento di $\mathbb{Z}/p\mathbb{Z}^*$, per ogni x in $\mathbb{Z}/p\mathbb{Z}^*$ si ha $x^h = 1$. Ovvero tutti gli elementi di $\mathbb{Z}/p\mathbb{Z}^*$ sono radici di $x^h - 1$. Una conseguenza del teorema di Ruffini è che un polinomio di grado h ha al più h radici, da cui $p - 1 \leq h$. □

Osservazione 5.72. Abbiamo visto nell'Esercizio 5.54 che la condizione p primo non è necessaria: $\mathbb{Z}_6^*$ è ciclico nonostante 6 non sia primo. D'altra parte abbiamo visto anche (Esempio 5.59) che non tutti gli $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ sono ciclici.

Il Teorema 5.68 ci dice che se $\mathbb{Z}/m\mathbb{Z}^*$ è ciclico allora ha $\phi(\phi(m))$ generatori distinti. Dalla dimostrazione del Teorema 5.68, emerge anche una caratterizzazione dei generatori di un gruppo ciclico finito, a partire dalla conoscenza di un generatore. Abbiamo visto infatti che, dato a generatore del gruppo $(G, *)$ di cardinalità finita s, tutti i generatori di G sono della forma a^n con n minore di s e primo con s. In particolare, per gli $\mathbb{Z}/m\mathbb{Z}^*$ ciclici, se a è un generatore, allora lo sono tutti e soli gli elementi di $\mathbb{Z}/m\mathbb{Z}^*$ della forma a^n con $(n, \phi(m)) = 1$.

Ad esempio, nel caso di $\mathbb{Z}_7^*$ (che sappiamo essere ciclico dal Teorema 5.71), ci sono $\phi(\phi(7)) = \phi(6) = 2$ generatori, e, trovatone uno che indichiamo con a, l'altro sarà a^5 (in quanto i k primi con $\phi(7) = 6$ sono 1 e 5).

Esercizio 5.73 (Teorema di Wilson)**.** *Dimostrare che se p è un primo, allora:*

$$(p-1)! \equiv -1 \ (p)$$

Svolgimento. Calcolare $(p-1)!$ modulo p, equivale a trovare l'elemento in $\mathbb{Z}/p\mathbb{Z}^*$ uguale al prodotto di tutti gli elementi di $\mathbb{Z}/p\mathbb{Z}^*$ (moltiplichiamo infatti tutte le classi di $\mathbb{Z}/p\mathbb{Z}$ tranne quella nulla):

Osserviamo che, essendo $\mathbb{Z}/p\mathbb{Z}^*$ un gruppo, ogni elemento in $\mathbb{Z}/p\mathbb{Z}^*$ ha un inverso. Dunque moltiplicando tra loro tutti gli elementi di $\mathbb{Z}/p\mathbb{Z}^*$, tutti i prodotti tra coppie di elementi che sono uno l'inverso dell'altro daranno $[1]_p$, e rimarranno fuori solo quelli elementi $[x]_p$ che coincidono con il proprio inverso in $\mathbb{Z}/p\mathbb{Z}^*$. Quali sono questi elementi? Sono gli $[x]_p$ tali che $[x^2]_p = [1]_p$, ovvero quelli di ordine 1 (in realtà di ordine 1 vuol dire l'elemento neutro, che è unico, in questo caso $[1]_p$), e quelli di ordine 2. Anche di ordine 2, essendo $\mathbb{Z}/p\mathbb{Z}^*$ ciclico, dal Corollario 5.70 sappiamo che ne esiste uno solo, ed è facile provare che è $[p-1]_p$, infatti $p - 1^2 = p^2 - 2p + 1$ che modulo p è proprio 1.

Riassumendo, se facciamo il prodotto di tutti gli elementi di $\mathbb{Z}/p\mathbb{Z}^*$, troviamo un prodotto di tanti $[1]_p$ (le coppie di inversi, e l'elemento neutro) per $[p-1]_p$. Dunque:

$$(p-1)! \equiv p-1 \ (p)$$

Si conclude facilmente, osservando che $p-1$ è congruo a -1 modulo p.

4. Gruppi quoziente, classi laterali e sottogruppi normali

Abbiamo visto nel capitolo 1 che dato un insieme A, una relazione di equivalenza $\sim$ su A induce una partizione dell'insieme in classi di equivalenza e abbiamo definito l'insieme quoziente $A/\sim$, i cui elementi sono per l'appunto le classi di equivalenza di A tramite $\sim$.

Vogliamo capire se, nel caso di un gruppo $(G,*)$ e di una relazione di equivalenza $\sim$ su G, è possibile indurre in $G/\sim$ un'operazione in modo che $G/\sim$ sia un gruppo. Se $\sim$ è compatibile con l'operazione $*$ possiamo *ben* definire un'operazione $*_\sim$ sull'insieme $G/\sim$. Nell'indicare la classe di un elemento x di G useremo qui di seguito la notazione $\overline{x}$ (non faremo riferimento alla relazione $\sim$ che in questo momento è una generica relazione di equivalenza compatibile con $*$).

Definizione 5.74. Dato un gruppo $(G,*)$ e una relazione di equivalenza $\sim$ compatibile con $*$, l'operazione $*_\sim$ definita su $G/\sim$ da

$$\overline{x} *_\sim \overline{y} \overbrace{=}^{def.} \overline{x*y}$$

è detta **operazione indotta** da $*$ sul quoziente $G/\sim$.

Osservazione 5.75. Il fatto che $*_\sim$ sia ben definita, ovvero che $*/\sim$ sia un'applicazione da $G/\sim \times G/\sim$ in $G/\sim$ il cui risultato non dipende dai rappresentanti della classe scelti, è appunto una conseguenza della compatibilità di $*$ con $\sim$.

Se $\sim$ non fosse compatibile con $*$, allora esisterebbero $a,b,c,d \in G$ con $a\sim b$ e $c\sim d$ e $a*c$ non equivalente a $b*d$, cioè:

$$\overline{a} *_\sim \overline{c} = \overline{a*c} \neq \overline{b*d} = \overline{b} *_\sim \overline{d}$$

nonostante che la coppia $(\overline{a},\overline{c})$ in $G/\sim$ sia uguale alla coppia $(\overline{b},\overline{d})$.

Mostriamo ora che dato un gruppo $(G,*)$ e una relazione di equivalenza $\sim$ compatibile con $*$, definita l'operazione $*_\sim$ sul quoziente $G/\sim$, $(G/\sim, *_\sim)$ è a sua volta un gruppo.

Proposizione 5.76. *Se $(G,*)$ è un gruppo e $\sim$ una relazione di equivalenza compatibile con $*$, allora $(G/\sim, *_\sim)$, con $*_\sim$ operazione indotta sull'insieme quoziente $G/\sim$ da $*$, è un gruppo.*
Se inoltre G è abeliano allora anche $G/\sim$ lo è.

Dimostrazione. Mostriamo che in $(G/\sim, *)$ valgono le proprietà caratterizzanti un gruppo:

- **proprietà associativa:** siano $\overline{x},\overline{y},\overline{z} \in G/\sim$ allora:

$$(\overline{x} *_\sim \overline{y}) *_\sim \overline{z} \underbrace{=}_{def.\ *_\sim} \overline{x*y} *_\sim \overline{z} \underbrace{=}_{def.\ *_\sim} \overline{(x*y)*z} =$$
$$\underbrace{=}_{prop.ass.*} \overline{x*(y*z)} \underbrace{=}_{def.\ *_\sim} \overline{x} *_\sim \overline{y*z} \underbrace{=}_{def.\ *_\sim} \overline{x} *_\sim (\overline{y} *_\sim \overline{z})$$

- **esistenza elemento neutro:** consideriamo $\overline{e}$ allora per ogni $\overline{x} \in G/\sim$ si ha:

$$\overline{e} *_\sim \overline{x} \underbrace{=}_{def.\ *_\sim} \overline{e*x} = \overline{x} = \overline{x*e} \underbrace{=}_{def.\ *_\sim} \overline{x} *_\sim \overline{e}$$

- **esistenza dell'inverso di ogni elemento:** dato $\overline{x} \in G/\sim$, l'elemento $\overline{x^{-1}}$ è in $G/\sim$ in quanto G è un gruppo. Mostriamo che $\overline{x^{-1}}$ è proprio $\overline{x}^{-1}$:

$$\overline{x} *_\sim \overline{x^{-1}} \underbrace{=}_{def.\ *_\sim} \overline{x * x^{-1}} = \overline{e}$$

Osserviamo che nello stesso modo in cui abbiamo provato che la $*_\sim$ è associativa, ovvero sfruttando la proprietà su $*$, si dimostra che se G è abeliano anche $G/\sim$ lo è. □

Definizione 5.77. Il gruppo $(G, *_\sim)$ è detto **gruppo quoziente** del gruppo $(G, *)$.

Esempio 5.78. $(\mathbb{Z}/m\mathbb{Z}, +)$ è il gruppo quoziente di $(\mathbb{Z}, +)$ attraverso la relazione di equivalenza definita dalla congruenza modulo m tra numeri interi.

Proprio questo esempio conosciuto ci permette di mostrare l'importanza di verificare che un'operazione su un insieme quoziente sia ben definita. Consideriamo l'operazione $*$ su $\mathbb{Z}$ definita da $a * b = 2^{a+b}$. Supponiamo di passare al quoziente tramite la congruenza modulo 8, e consideriamo $(\mathbb{Z}_8, *_{\equiv_8})$. Data la classe di equivalenza $[1]_8$, calcoliamo $[1]_8 * [1]_8$. Se scegliamo come rappresentanti $a = b = 1$ si ha che $a * b = 2^2 = 4$, mentre scegliendo come rappresentanti $a = 1$ e $b = 9$ si ha $a * b = 1024$, che modulo 8 è congruo a 0. Ovvero $*_{\equiv_8}$ non è ben definita in $\mathbb{Z}_8$.

Notazione: d'ora innanzi per semplicità di notazione, quando non ci sia ambiguità, indicheremo $*_\sim$ con $*$ (a volte omettendo del tutto il simbolo di operazione). In generale, dato un gruppo $(G, *)$, un sottoinsieme A di G e un $x \in G$, useremo la notazione xA per indicare il sottoinsieme di G i cui elementi sono del tipo $x * a$ al variare di a in A.

Siano $(G, *)$ un gruppo e H un sottogruppo di G, e definiamo una relazione binaria su G nel modo seguente:

$$\forall x, y \in G \quad x \sim_H y \Leftrightarrow x^{-1}y \in H \tag{4.1}$$

Esercizio 5.79. *Verificare che effettivamente la relazione binaria definita dalla 4.1 è di equivalenza.*

Svolgimento. $x \sim_H x$ in quanto $x^{-1}x = e \in H$.

Se $x \sim_H y$ allora $x^{-1}y \in H$. Perciò, essendo H un sottogruppo di G, anche $(x^{-1}y)^{-1} = y^{-1}x \in H$, cioè $y \sim_H x$.

Se $x \sim_H y$ e $y \sim_H z$ allora $x^{-1}y, y^{-1}z \in H$. Quindi anche il loro prodotto $x^{-1}yy^{-1}z = x^{-1}z$ sta in H, cioè $x \sim_H z$.

Fissato $x \in G$, cerchiamo di capire a cosa corrisponde la classe di equivalenza di x, che indichiamo con xH:

$$xH = \{y \in G | x \sim_H y\} = \{y \in G | x^{-1}y \in H\} = \{y \in G | \exists h \in H\ x^{-1}y = h\}$$

Definizione 5.80. La classe di equivalenza di x rispetto alla relazione $\sim_H$ introdotta è chiamata **classe laterale sinistra** del sottogruppo H, e corrisponde all'insieme:

$$xH = \{xh | h \in H\}$$

A partire da un $H < G$ si può introdurre un'altra relazione su G definita da:

$$x \sim'_H y \Leftrightarrow yx^{-1} \in H$$

Analogamente a quanto fatto in precedenza è facile verificare che $\sim'_H$ è di equivalenza su G.

Definizione 5.81. La classe di equivalenza di $x \in G$ rispetto a $\sim'_H$, detta **classe laterale destra** del sottogruppo H, è data dall'insieme:

$$Hx = \{hx | h \in H\}$$

Esercizio 5.82. *Dimostrare che dato un gruppo $(G, *)$ e $H < G$, per ogni x in G, $x \in yH$ se e solo se $xH = yH$.*

Svolgimento. x appartiene per ipotesi ad yH, e per definizione a xH (e appartiene ad H che è sottogruppo, e $x = e * x$). Concludiamo osservando che, le classi laterali sinistre (destre) di un sottogruppo H di un gruppo $(G, *)$ sono di equivalenza rispetto a $\sim_H$ ($\sim'_H$): ne segue che sono una partizione di G. Dunque due classi o sono disgiunte, o coincidono.

Se $(G, *)$ è abeliano allora $\sim_H$ e $\sim'_H$ coincidono, ovvero coincidono classi laterali destre e sinistre di un sottogruppo H. In generale, se $(G, *)$ non è commutativo, le relazioni $\sim_H$ e $\sim'_H$ e le relative partizioni indotte su G sono differenti.

Esempio 5.83. Consideriamo $(S(A), \circ)$, l'insieme delle bigezioni di un insieme A, che sappiamo (Esercizio 5.13) non essere commutativo per $|A| > 2$.

Sia $A = \{1, 2, 3\}$ e consideriamo il sottoinsieme H di $S(A)$ che contiene l'identità, e la bigezione ϕ che scambia tra loro 1 e 2 e lascia fisso 3. È facile provare che H è un sottogruppo di $S(A)$ (provarlo per esercizio).

Consideriamo $\psi \in S(A)$ che scambia tra loro il 2 e il 3 e lascia fisso l'1 e mostriamo che ψH (la classe laterale sinistra di ψ) è diversa da $H\psi$ (la classe laterale destra di ψ):

$$\psi H = \{\psi \circ id,\ \psi \circ \phi\} \quad H\psi = \{id \circ \psi, \phi \circ \psi\}$$

Vogliamo dunque mostrare che $\psi \circ \phi \neq \phi \circ \psi$, vediamolo confrontando l'azione sugli elementi di A di $\psi \circ \phi$ con quella di $\phi \circ \psi$:

$$\psi \circ \phi : \begin{cases} 1 \overset{\phi}{\longrightarrow} 2 \overset{\psi}{\longrightarrow} 3 \\ 2 \overset{\phi}{\longrightarrow} 1 \overset{\psi}{\longrightarrow} 1 \\ 3 \overset{\phi}{\longrightarrow} 3 \overset{\psi}{\longrightarrow} 2 \end{cases} \qquad \phi \circ \psi : \begin{cases} 1 \overset{\psi}{\longrightarrow} 1 \overset{\phi}{\longrightarrow} 2 \\ 2 \overset{\psi}{\longrightarrow} 3 \overset{\phi}{\longrightarrow} 3 \\ 3 \overset{\psi}{\longrightarrow} 2 \overset{\phi}{\longrightarrow} 1 \end{cases}$$

Dunque, in generale, dato un gruppo $(G, *)$ e un sottogruppo H di G le classi laterali destre e sinistre di H non coincidono.

Esercizio 5.84. *Dimostrare che, dato un gruppo $(G, *)$ e un sottogruppo H di G, se le classi laterali sinistre e destre di H coincidono, allora per ogni x in G si ha $xH = Hx$.*

Svolgimento. Supponiamo $xH = Hy$. Vogliamo provare che $Hy = Hx$. Basta osservare che x appartiene sia ad $Hy = xH$ ($x = xe$) che ad Hx ($x = ex$). Trattandosi di classi di equivalenza, le due classi Hy e Hx o sono disgiunte o sono

coincidenti, avendo x come elemento in comune le due classi Hy e Hx coincidono, ovvero $xH = Hx$.

Proposizione 5.85. *Dato un gruppo $(G, *)$, un sottogruppo H di G, e considerati gli insiemi (in generale distinti) $G/\sim_H$ e $G/\sim'_H$, si ha:*

$$|G/\sim| = |G/\sim'_H|$$

Dimostrazione. Consideriamo l'applicazione σ tra i due insiemi che associa alla classe laterale sinistra xH la classe laterale destra Hx^{-1}. Dimostriamo che σ è ben definita sulle classi laterali sinistre e che è una applicazione bigettiva tra l'insieme delle classi laterali sinistre e quello delle classi laterali destre.

σ è ben definita sull'insieme $G/\sim_H$ delle classi laterali sinistre di H, infatti, se $xH = yH$, allora $x \sim_H y$, ovvero $x^{-1}y \in H$. Essendo H un sottogruppo anche $(x^{-1}y)^{-1} = y^{-1}x \in H$, dunque $y^{-1}x = h$ per un certo $h \in H$ e quindi $y^{-1} = hx^{-1} \in Hx^{-1}$. Osservando che y^{-1} appartiene ad Hy^{-1} (in quanto $y^{-1} = ey^{-1}$ ed e sta in H, essendo H un sottogruppo) e sapendo che due classi di equivalenza o sono coincidenti, o non hanno elementi in comune, si ha che $Hx^{-1} = Hy^{-1}$.

σ è surgettiva: per ogni classe laterale destra Hx si ha che $\sigma(x^{-1}H) = Hx$.

Infine se $Hx^{-1} = Hy^{-1}$ allora, per definizione $x^{-1}y \in H$, ovvero $y = xh$ per un certo $h \in H$, cioè $y \in xH$ e dunque (sempre per il fatto che due classi di equivalenza o sono coincidenti o non hanno elementi in comune) $yH = xH$. □

Quanto provato ci permette di introdurre la seguente definizione, senza specificare classi laterali destre e sinistre:

Definizione 5.86. Dato un gruppo $(G, *)$ e un sottogruppo H di G, il numero delle classe laterali di H si chiama **indice** di H in G e si indica con $[G : H]$.

Esempio 5.87. Consideriamo il gruppo additivo $(\mathbb{Z}, +)$ e i sottogruppi $n\mathbb{Z}$ e $H' = \{0\}$, allora:

- $[\mathbb{Z} : n\mathbb{Z}] = n$. Le classi laterali destre e sinistre di $n\mathbb{Z}$ (coincidenti in quanto $(\mathbb{Z}, +)$ è abeliano) sono le classi di equivalenza modulo n.
- $[\mathbb{Z} : H'] = +\infty$. Questo mostra come in generale non è detto che le classi laterali di un sottogruppo siano finite.
- La generalizzazione del caso precedente è: dato il gruppo G, calcolare l'indice del sottogruppo $H = \{e\}$. Tale indice è uguale a $|G|$ in quanto le classi laterali xH sono composte dal solo elemento x. In questo caso, anche se G non è abeliano, le classi Hx e xH coincidono.

Proposizione 5.88. *Dato un gruppo $(G, *)$, e un sottogruppo H di G, consideriamo l'insieme delle classi laterali sinistre $G/\sim_H$ di H. Per ogni coppia di classi laterali sinistre xH, yH in $G/\sim_H$ si ha $|xH| = |yH|$ (analogamente per le classi laterali destre).*

Dimostrazione. Il sottogruppo H è una classe laterale sinistra (e analogamente anche destra): $eH = \{eh | h \in H\} = H$.

Osservato quanto sopra, per ogni x in G costruiamo una bigezione f_x da H ad xH (lo stesso potremmo fare analogamente per qualsiasi classe laterale destra) in questo modo: per ogni h in H, definiamo $f_x(h)$ come xh. f_x è surgettiva per definizione di xH, ed è iniettiva in quanto, se $f_x(h) = f_x(h')$, ovvero $xh = xh'$, allora, moltiplicando a sinistra per x^{-1}, si ha $h = h'$. Dunque, tutte le classi

laterali sinistre (destre) sono in corrispondenza biunivoca con H e di conseguenza hanno la stessa cardinalità $|H|$. □

Teorema 5.89. *Se $(G, *)$ è un gruppo finito e H è un sottogruppo di G, si ha che la cardinalità di G è uguale all'indice di H in G per la cardinalità di H:*

$$|G| = [G : H] \cdot |H|$$

DIMOSTRAZIONE. Le classi laterali sinistre (destre) di H formano una partizione di G (cioè G è l'unione disgiunta di esse). Il numero di classi laterali sinistre (destre) di H è $[G : H]$ e ogni classe laterale ha cardinalità uguale ad H, da questo segue la tesi. □

Dal Teorema 5.89 seguono due risultati molto importanti sugli ordini dei sottogruppi e degli elementi di un gruppo finito.

Teorema 5.90 (Teorema di Lagrange)**.** *Se $(G, *)$ è un gruppo finito e H è un sottogruppo di G, allora $|H|$ divide $|G|$.*

Teorema 5.91. *Sia g in $(G, *)$, con G gruppo finito, allora l'ordine di g divide $|G|$.*

DIMOSTRAZIONE. Consideriamo il sottogruppo ciclico H generato da g, ossia $H =< g >$. H ha esattamente $o(g)$ elementi, dunque dal teorema di Lagrange si ha che:

$$|H| = o(g) \mid |G|$$

□

Esercizio 5.92. *Risolvere se possibile la seguente congruenza esponenziale:*

$$4^x \equiv 3 \ (13)$$

Svolgimento. Procedendo per tentativi ci si dovrebbe accorgere che $4^2 = 16 \equiv 3 \ (13)$. Quindi possiamo riscrivere la congruenza da risolvere come:

$$4^x \equiv 4^2 \ (13) \underbrace{\leftrightarrow}_{4 \in \mathbb{Z}_{13}^*} 4^{x-2} \equiv 1 \ (13)$$

Ponendo $y = x - 2$ si ha $4^y \equiv 1 \ (13)$. Tale congruenza è sicuramente risolubile infatti, dal teorema di Fermat, sappiamo che $4^{\phi(13)} \equiv 1 \ (13)$.

Essendo 4^3 congruo a 12 (ovvero -1) modulo 13, si ha che $4^6 \equiv 1 \ (13)$ e 6 è proprio l'ordine di 4 in $\mathbb{Z}_{13}^*$. Dato quindi y intero, facciamo la divisione euclidea tra y e 6, e scriviamo $y = 6q + r$ con $0 \leq r < 6$. Per ogni y intero, si può dunque riscrivere 4^y come segue:

$$4^y = 4^{6q+r} = \underbrace{4^{6\ q}}_{1} \cdot 4^r \equiv 4^r \ (13)$$

La congruenza $4^r \equiv 1 \ (13)$ è risolubile se e solo se r, che è minore dell'ordine di 4 (6), è uguale a 0.

Possiamo dunque concludere che:

$$4^x \equiv 3 \ (13) \Leftrightarrow 4^{x-2} \equiv 1 \ (13) \Leftrightarrow x - 2 \equiv 0 \ (6) \Leftrightarrow x \equiv 2 \ (6)$$

L'insieme S delle soluzioni in $\mathbb{Z}$ della congruenza data è dunque:

$$S = \{x \in \mathbb{Z} | x = 2 + 6k \quad k \in \mathbb{Z}\}$$

In generale, dovendo risolvere $a^x \equiv b\ (n)$, con $(a,n)=1$ (condizione necessaria affinché $[a]_n$ appartenga al gruppo moltiplicativo $(\mathbb{Z}_n^*,\cdot)$), cerchiamo t tale che $a^t = b$ e riscriviamo la congruenza iniziale come $a^{x-t} \equiv 1\ (n)$. Cerchiamo inoltre l'ordine di $[a]_n$ in $\mathbb{Z}_n^*$, ed effettuiamo la divisione euclidea tra $x-t$ e $o([a]_n)$:

$$x - t = q \cdot o([a]_n) + r \quad 0 \leq r < o([a]_n)$$

A questo punto $a^{x-t} \equiv a^r\ (n)$, e:

$$a^r \equiv 1\ (n) \Leftrightarrow r = 0 \Leftrightarrow x - t \equiv 0\ (o([a]_n)) \Leftrightarrow x \equiv t\ (o([a]_n))$$

Esercizio 5.93. *Risolvere il seguente sistema di congruenze:*

$$\begin{cases} 2^{x^2} \equiv 8^{x-2}\ (11) \\ 5x \equiv 4\ (22) \end{cases}$$

Svolgimento. Innanzitutto discutiamo la risolubilità delle singole congruenze presenti nel sistema. Dal teorema cinese del resto sappiamo che $5x \equiv 4\ (22)$ è equivalente al sistema:

$$\begin{cases} 5x \equiv 4\ (2) \\ 5x \equiv 4\ (11) \end{cases} \underbrace{\Leftrightarrow}_{riduzione\ coefficienti} \begin{cases} x \equiv 0\ (2) \\ x \equiv 3\ (11) \end{cases}$$

Per quanto riguarda la congruenza $2^{x^2} \equiv 8^{x-2}\ (11)$, scrivendo 8 come 2^3, possiamo scriverla:

$$2^{x^2} \equiv (2^3)^{x-2}\ (11) \Leftrightarrow 2^{x^2-3x+6} \equiv 1\ (11)$$

Dunque $x^2 - 3x + 6$ deve essere congruo a 0 modulo l'ordine di 2 in $\mathbb{Z}_{11}^*$ (che deve essere un divisore dell'ordine del gruppo, ovvero 10). Calcoliamoci dunque le potenze di 2 *candidate* ad essere l'ordine di 2:

$$2^1 \equiv 2\ (11) \quad 2^2 \equiv 4\ (11) \quad 2^5 \equiv -1\ (11)$$

Dunque $o(2) = 10$ e la prima congruenza del sistema originario (quella esponenziale), è equivalente alla seguente congruenza polinomiale:

$$x^2 - 3x + 6 \equiv 0\ (10)$$

A questo punto usiamo di nuovo il teorema cinese del resto per dire che questa congruenza è equivalente al sistema:

$$\begin{cases} x^2 - 3x + 6 \equiv 0\ (2) \\ x^2 - 3x + 6 \equiv 0\ (5) \end{cases} \Leftrightarrow \begin{cases} x^2 + x \equiv 0\ (2) \\ x^2 + 2x + 1 \equiv 0\ (5) \end{cases} \Leftrightarrow \begin{cases} x(x+1) \equiv 0\ (2) \\ (x+1)^2 \equiv 0\ (5) \end{cases}$$

La prima delle due congruenze è sempre verificata (il prodotto di due numeri consecutivi è sempre pari), la seconda è verificata per $x \equiv 4\ (5)$.

Il sistema originario è dunque equivalente a:

$$\begin{cases} x \equiv 0\ (2) \\ x \equiv 3\ (11) \\ x \equiv 4\ (5) \end{cases}$$

Dal teorema cinese del resto sappiamo che questo sistema ha una unica soluzione modulo 110, dunque trovando una soluzione particolare abbiamo terminato. Si può procedere risolvendo il sistema con una delle metodologie descritte precedentemente, o si può provare a cercare tra i numeri pari ($x \equiv 0\ (2)$), che sono maggiori di 3 rispetto ai multipli di 11 ($x \equiv 3\ (11)$), quelli che sono maggiori di 4 rispetto ad un multiplo di 5 ($x \equiv 4\ (5)$). Il primo numero intero che soddisfa le prime due condizioni è 3, che non va bene perché è congruo a 3 modulo 5. Il secondo numero

intero che rispetta le due condizioni è 14, che effettivamente è congruo a 4 modulo 5. Perciò 14 è una soluzione particolare del sistema, e tutte le soluzioni sono descritte da:

$$x \equiv 14 \ (110)$$

Esercizio 5.94. *Determinare i valori positivi dell'intero a per cui il seguente sistema di congruenze è risolubile, e trovarne le soluzioni.*

$$\begin{cases} a^x \equiv 1 \ (9) \\ x^a \equiv 3 \ (12) \end{cases} \tag{4.2}$$

Svolgimento. Applicando il teorema cinese del resto, sappiamo che il sistema da risolvere è equivalente a:

$$\begin{cases} a^x \equiv 1 \ (9) \\ x^a \equiv 3 \ (3) \\ x^a \equiv 3(4) \end{cases} \Leftrightarrow \begin{cases} a^x \equiv 1 \ (9) \\ x^a \equiv 0 \ (3) \\ x^a \equiv 3(4) \end{cases}$$

La seconda congruenza del sistema equivale a dire che x^a, e quindi x (visto che 3 è primo), è un multiplo di 3. Perciò è equivalente a $x \equiv 0 \ (3)$.

La terza congruenza non ha soluzioni se x è congruo ad 1 modulo 4 (perché le potenze di 1 danno sempre 1), e se x è pari (perché potenza di pari è pari, ed un pari ridotto modulo un pari - come 4 - rimane pari). Dunque la terza congruenza ha soluzione se e solo se $x \equiv 3 \ (4)$ ed a è dispari (perché $o(3)$ in $\mathbb{Z}_4^*$ è 2, dunque $[3]_4$ elevato alla a con a pari è uguale a $[1]_4$, mentre $[3]_4$ elevato alla a con a dispari è uguale a $[3]_4$).

Abbiamo dunque trovato finora che $x^a \equiv 3 \ (12)$ è risolubile se e solo se a è dispari, ed in tal caso è equivalente al sistema:

$$\begin{cases} x \equiv 0 \ (3) \\ x \equiv 3 \ (4) \end{cases}$$

Che ha soluzione $x \equiv 3 \ (12)$.

La prima congruenza è risolvibile con a dispari se e solo se a è congruo ad 1, a 5 o a 7 modulo 9.

- Se $a \equiv 1 \ (9)$ la prima congruenza è sempre verificata e perciò, per a siffatti, la soluzione del sistema 4.2 è $x \equiv 3 \ (12)$.
- Se $a \equiv 5 \ (9)$ la prima congruenza è $5^{3+12k} \equiv 1 \ (9)$. Ora, 5 ha ordine 6 in $\mathbb{Z}_9^*$ (provarlo), dunque la congruenza è equivalente a $3 + 12k \equiv 0 \ (6)$ che non è mai risolvibile. Dunque in questo caso, il sistema 4.2 non ha soluzioni.
- Se $a \equiv 7 \ (9)$, analogamente al caso precedente dobbiamo cercare l'ordine di 7 in $\mathbb{Z}_9^*$. Provare che $o(7) = 3$. In questo caso l'equazione $3+12k \equiv 0 \ (3)$ è sempre verificata. Dunque, anche in questo caso, le soluzioni del sistema 4.2 sono $x \equiv 3 \ (12)$.

Riassumendo, il sistema è risolvibile se e solo se a è congruo ad 1 o 7 modulo 9, e, in questi casi, l'insieme delle soluzioni intere è dato dagli x tali che $x \equiv 3 \ (12)$. In particolare le soluzioni positive sono del tipo $3 + 12t$ al variare di t in $\mathbb{N}$.

Osservazione 5.95. Dal Teorema 5.91 si può ottenere come corollario il Teorema di Eulero (4.125) già dimostrato con *metodi aritmetici*. Infatti, considerando il gruppo $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ di ordine $\phi(m)$, si ha che ogni x in $\mathbb{Z}/m\mathbb{Z}^*$ ha ordine che

divide $\phi(m)$. Da questo segue che, per ogni x in $\mathbb{Z}/m\mathbb{Z}^*$, $x^{\phi(m)} = 1$, ovvero, per ogni $x \in \mathbb{Z}$ primo con m, $x^{\phi(m)} \equiv 1\ (m)$.

Corollario 5.96. *Se $(G, *)$ è un gruppo di ordine p primo, allora G è ciclico.*

DIMOSTRAZIONE. Un elemento $g \in G$ diverso dall'identità ha ordine diverso da 1. Per il teorema di Lagrange $o(g)$ deve dividere p, dunque non essendo 1 deve essere p. Notiamo che in questo modo abbiamo anche dimostrato che il numero di generatori di un gruppo di ordine un primo p è $p - 1$. □

Corollario 5.97. *Per ogni $n \in \mathbb{N} \setminus \{0\}$ si ha:*

$$\sum_{d|n} \phi(d) = n$$

DIMOSTRAZIONE. Per ogni $n \in \mathbb{N} \setminus \{0\}$ sappiamo che esiste un gruppo ciclico $(G, *)$ di ordine n (basta considerare ad esempio $\mathbb{Z}/n\mathbb{Z}$). Sia d un divisore di n e consideriamo i sottoinsiemi H_d di G contenenti tutti e soli gli elementi di G di ordine d. Il teorema di Lagrange ci assicura che:

$$G = \cup_{d|n} H_d$$

Da questo, osservando che gli H_d son tutti disgiunti, segue che:

$$|G| = \sum_{d|n} |H_d|$$

La tesi segue dal corollario 5.70 che ci dice che $|H_d| = \phi(d)$. □

Per concludere questo paragrafo, studiamo per quali sottogruppi H di un gruppo $(G, *)$ le relazioni di equivalenza $\sim_H$ e $\sim'_H$ (che definiscono rispettivamente l'insieme delle classi laterali sinistre e destre di H), sono compatibili con $*$ e di conseguenza inducono una struttura di gruppo sui rispettivi insiemi quoziente.

Consideriamo il caso delle classi laterali sinistre, l'eventuale operazione $*_\sim$ indotta da $*$ sull'insieme quoziente sarebbe:

$$xH *_\sim yH \overset{def.}{=} (x * y)H$$

$\sim_H$ è compatibile rispetto a $*$ se e solo se per ogni x, y, w, z tali che $x \sim_H w$ e $y \sim_H z$, si ha:

$$(xy)H = xHyH = wHzH = (wz)H$$

Ovvero se e solo se vale la seguente condizione:

se $w^{-1}x$ e $z^{-1}y$ stanno in H, allora $(wz)^{-1}(xy)$ sta in H

.

Questa condizione in generale non è verificata per qualsiasi $H < G$. La seguente proposizione infatti fornisce la condizione necessaria e sufficiente su H affinché sia verificata la condizione trovata, ovvero affinché $\sim_H$ sia compatibile con l'operazione di G.

Proposizione 5.98. *Dato un gruppo $(G, *)$ e un sottogruppo H di G, la relazione di equivalenza $\sim_H$ è compatibile con $*$ se e solo se per ogni x in G si ha $xH = Hx$.*

DIMOSTRAZIONE. Supponiamo che per ogni $x \in G$ si abbia $xH = Hx$, e mostriamo che vale la condizione voluta. Supponendo che $(w^{-1}x)$ e $z^{-1}y$ stanno in H, mostriamo che $(wz)^{-1}(xy)$ sta in H.

$$(wz)^{-1}(xy) \underbrace{=}_{prop.ass.} z^{-1}\overbrace{(w^{-1}x)}^{\in H}y$$

Dunque $(wz)^{-1}(xy) \in z^{-1}Hy$. Ora osserviamo che, per ipotesi $z^{-1}Hy = Hz^{-1}y$ e che $z^{-1}y$ è un elemento di H, da cui la tesi.

Viceversa sia valida la condizione di compatibilità, e supponiamo che esista $z \in G$ tale che $Hz \neq zH$. Questo significa che esiste $h_1 \in H$ tale che $h_1 z \notin zH$. Siano $x = wh_1$ e $y = zh_2$ con $h_2 \in H$ (ovvero $w^{-1}x \in H$ e $z^{-1}y \in H$): per la condizione di compatibilità esiste $h_3 \in H$ tale che $xy = wzh_3$. Osserviamo che:

$$\underbrace{wh_1}_{x}\underbrace{zh_2}_{y} = wzh_3 \leftrightarrow h_1 z = zh_3h_2^{-1}$$

Questo contraddice l'ipotesi $h_1 z \notin zH$. Dunque se vale la condizione di compatibilità deve essere che $Hx = xH$, per ogni $x \in G$. □

I sottogruppi H per cui $\sim_H$ è compatibile con l'operazione del gruppo hanno dunque un'importanza particolare in quanto permettono di indurre una struttura di gruppo sull'insieme quoziente.

Definizione 5.99. I sottogruppi H di un gruppo $(G, *)$ per cui, per ogni x in G, si ha $xH = Hx$, si dicono **sottogruppi normali** di G. Indicheremo che H è un sottogruppo normale di G con la notazione $H \lhd G$.

Esempio 5.100. Abbiamo già osservato che in un gruppo abeliano $(G, *)$ qualsiasi sottogruppo H di G è normale. Nel caso in cui il gruppo G non sia abeliano sicuramente il sottogruppo $H = \{e\}$ ed il sottogruppo $H = G$ sono normali.

Esercizio 5.101. *Dato un gruppo $(G, *)$, il centro $Z(G)$ di G è un sottogruppo normale di G, ed è abeliano.*

Svolgimento. $e \in Z(G)$, inoltre se $x, y \in Z(G)$, per ogni $g \in G$ si ha:

$$g(xy) = (gx)y \underbrace{=}_{x \in Z(G)} (xg)y = x(gy) \underbrace{=}_{y \in Z(G)} (xy)g$$

ovvero $xy \in Z(G)$. Infine, se $x \in Z(G)$ allora $x^{-1} \in G$, infatti, per ogni $g \in G$ si ha:

$$gx^{-1} = (xg^{-1})^{-1} \underbrace{=}_{x \in Z(G)} (g^{-1}x)^{-1} = x^{-1}g$$

Il fatto che $Z(G)$ sia normale, ovvero che $gZ(G) = Z(G)g$ per ogni $g \in G$, e che sia abeliano sono conseguenze immediate della definizione di $Z(G)$.

Esercizio 5.102. *Un sottogruppo H di indice 2 di un gruppo $(G, *)$, è normale.*

Svolgimento. Se H ha indice 2, allora esistono due classi laterali sinistre di H, una delle quali H stessa e l'altra xH, per un certo x in G. D'altra parte esistono anche due classi destre: una è ancora H, l'altra sarà Hy per un certo y in G. Essendo G l'unione disgiunta delle classi laterali sinistre (destre), si ha che $xH = Hy$. La tesi segue dall'Esercizio 5.84.

Definizione 5.103. Dato $(G, *)$ gruppo e un sottogruppo normale H di G, il gruppo G/H delle classi laterali[2] di H è detto **gruppo quoziente di G modulo H.**

Esercizio 5.104. *Dimostrare che la classe laterale H è l'elemento neutro in G/H.*

Esempio 5.105. Consideriamo il gruppo abeliano $(\mathbb{Z}, +)$ e, fissato $n \in \mathbb{N}^+$, il sottogruppo $H = n\mathbb{Z}$ (che è normale perché sottogruppo in un gruppo commutativo). Il gruppo quoziente $\mathbb{Z}/n\mathbb{Z}$ di $\mathbb{Z}$ modulo $n\mathbb{Z}$ è il gruppo additivo delle classi modulo n. Infatti la classe di equivalenza di $x \in \mathbb{Z}$ è l'insieme $\{x + nz | z \in \mathbb{Z}\}$, ovvero l'insieme di tutti i numeri interi che divisi per n hanno lo stesso resto di x.

Osservazione 5.106. Per verificare che un sottogruppo H di un gruppo G è normale, dobbiamo provare che per ogni $x \in G$ si abbia $xH = Hx$. Osserviamo che l'uguaglianza $xH = Hx$ è insiemistica: è *meno forte* della relazione $xh = hx$ $\forall h \in H$.

La condizione $xH = Hx$ equivale a verificare due contenimenti:

- $xH \subseteq Hx$, ovvero per ogni h in H, esiste h' in H tale che $xh = h'x$.
- $Hx \subseteq xH$, ovvero per ogni h in H, esiste h' in H tale che $hx = xh'$.

Il seguente lemma ci dice che possiamo limitarci a provare uno dei due contenimenti, l'altro ne è conseguenza.

Lemma 5.107. *Se $(G, *)$ è un gruppo e H un sottogruppo tale che per ogni $x \in G$ si ha $xH \subseteq Hx$, allora H è normale. Analogamente se per ogni $x \in G$ si ha $Hx \subseteq xH$, allora H è normale.*

Dimostrazione. Per ogni $x \in G$ consideriamo l'applicazione g_x che ad ogni y di G associa yx in G, e l'applicazione f_x che ad ogni y di G associa xy in G.

Sappiamo per ipotesi che, per ogni x in G, $xH \subseteq Hx$, vogliamo dimostrare che da questo segue l'inclusione inversa $Hx \subseteq Hx$, e dunque che xH ed Hx sono uguali. Dall'ipotesi segue in particolare che $x^{-1}H \subseteq Hx^{-1}$ (x^{-1} appartiene a G), perciò:

$$g_x(x^{-1}H) = x^{-1}Hx \subseteq g_x(Hx^{-1}) = Hx^{-1}x = H$$

Perciò $f_x(x^{-1}Hx) = Hx \subseteq f_x(H) = xH$. □

Vediamo una ulteriore caratterizzazione dei sottogruppi normali (utile anch'essa come criterio per provare che un sottogruppo è normale):

Proposizione 5.108. *Un sottogruppo H di un gruppo G è normale se e solo se per ogni $x \in G$ e per ogni $h \in H$, si ha che $xhx^{-1} \in H$.*

Dimostrazione. Se H è normale, per ogni $x \in G$, $xH = Hx$ che è equivalente alla uguaglianza insiemistica $xHx^{-1} = H$. Questa significa che, per ogni $h \in H$, l'elemento xhx^{-1} è in H.

Viceversa, se per ogni $x \in G$ e per ogni $h \in H$ si ha $xhx^{-1} \in H$, allora $xHx^{-1} \subset H$, ovvero $xH \subset Hx$. Dal Lemma 5.107 segue la tesi (che si può enunciare in termini insiemistici: per ogni x in G, xHx^{-1} è contenuto in H). □

[2]Non c'è più bisogno di specificare classe laterale destra o sinistra visto che in questo caso coincidono.

Esercizio 5.109. *Dimostrare che dato un gruppo $(G, *)$, se $H < G$ allora, per ogni g in G, gHg^{-1} è un sottogruppo di G.*

Esercizio 5.110. *Se $H =< s_1, \ldots, s_n >$ è un sottogruppo finitamente generato di un gruppo $(G, *)$ allora $H \lhd G$ se e solo se per ogni $x \in G$ e per ogni $s_i \in \{s_1, \ldots, s_n\}$, si ha che $xs_ix^{-1} \in H$.*

Esercizio 5.111. *Sia $(G, *)$ un gruppo, N un sottogruppo normale di G, H un sottogruppo di G. Dire quali delle seguenti affermazioni sono vere giustificando la risposta:*

(1) *$N \cap H$ è un sottogruppo normale di H.*
(2) *$N \cap H$ è un sottogruppo normale di G.*
(3) *Se H è normale, $N \cap H$ è un sottogruppo normale di G.*

Svolgimento. Innanzitutto sappiamo che l'intersezione di due sottogruppi N, H di G è un sottogruppo di G, ed anche di N e di H.

(1) Per ogni $x \in N \cap H$ e per ogni h in H, si ha che hxh^{-1} è un elemento di H. Infatti H, essendo un sottogruppo, è chiuso per l'operazione e h, x e h^{-1} sono tutti elementi di H. D'altra parte hxh^{-1} appartiene anche ad N, in quanto $x \in N$ ed N è normale in G. Dunque, con le ipotesi fatte e per la Proposizione 5.108, si ha che $N \cap H \lhd G$.
(2) Non è vero in generale che $N \cap H$ è un sottogruppo normale di G. Infatti basta scegliere un gruppo G con un sottogruppo H non normale, e considerare $N = G$.
(3) Se anche H è normale, per ogni $g \in G$, si ha:

$$gHg^{-1} \subseteq H \quad \text{e} \quad gNg^{-1} \subseteq N$$

Da cui si ha che $g(N \cap H)g^{-1}$ è contenuto sia in N che in H, ovvero in $N \cap H$. Dunque, l'intersezioni di sue sottogruppi normali è normale.

Esercizio 5.112. *Provare che se H è l'unico sottogruppo di ordine n di un gruppo $(G, *)$, allora H è normale.*

Svolgimento. Basta osservare che, per ogni g in G, H e gHg^{-1} hanno la stessa cardinalità n. Dall'Esercizio 5.109 sappiamo che gHg^{-1} è un sottogruppo di G. Per ipotesi esiste un solo sottogruppo di ordine n, per cui $H = gHg^{-1}$, e dalla Proposizione 5.108, segue che H è normale.

Esempio 5.113 (Il gruppo dei quaternioni)**.** Sia $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ e introduciamo su Q l'operazione di moltiplicazione tra gli elementi di Q definita dalla seguente tabella:

·	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

È una facile verifica provare che $(Q, \cdot)$ è un gruppo. Tale gruppo è detto **gruppo dei quaternioni**: studiamone alcune proprietà.

Innanzitutto Q è un gruppo finito (ha 8 elementi) non abeliano: basta osservare ad esempio che $i \cdot j \neq j \cdot i$. Determinando l'ordine degli elementi di Q troviamo che:

$$o(1) = 1 \quad o(-1) = 2 \quad o(i) = o(j) = o(k) = o(-i) = o(-j) = o(-k) = 4$$

Dunque Q non è ciclico perchè non esiste nessun elemento di ordine 8.

A questo punto analizziamo, elencandoli, i sottogruppi di Q:

$$\begin{array}{ccc} < 1 >= \{1\} & Q & < -1 >= \{1, -1\} \\ < i >= \{\pm 1, \pm i\} & < j >= \{\pm 1, \pm j\} & < k >= \{\pm 1, \pm k\} \end{array}$$

I sottogruppi $< i >, < j >, < k >$ hanno indice 2 e perciò (Esercizio 5.102) sono normali. I sottogruppi banali Q ed $\{1\}$ sappiamo che sono normali (Esempio 5.100). Anche il sottogruppo $H =< -1 >$ è normale, essendo l'unico sottogruppo di Q di ordine 2 (Esercizio 5.112).

Q dunque è un esempio di gruppo non abeliano con tutti i sottogruppi normali, e con tutti i sottogruppi non banali ciclici.

Esercizio 5.114. *Dato un gruppo $(G, *)$, per ogni coppia x, y di elementi di G consideriamo il seguente elemento di G detto* **commutatore** *di x, y:*

$$[x, y] = xyx^{-1}y^{-1}$$

Consideriamo inoltre il sottogruppo $[G, G]$, detto **sottogruppo dei commutatori** *o* **derivato** *di G, generato dai commutatori di tutte le coppie di elementi di G:*

$$G' =< [x, y] >_{x,y \in G}$$

Dimostrare che:

(1) *$G' \lhd G$.*
(2) *G/G' è abeliano.*
(3) *Se $H \lhd G$ e G/H è abeliano, allora $G' < H$, ovvero G/G' detto anche* **abelianizzato** *di G è il più grande quoziente di G abeliano.*

Svolgimento. Procediamo a dimostrare un punto alla volta.

(1) G' è un sottogruppo per definizione. Per provare che G', generato dai commutatori, è un sottogruppo normale di G basta provare (Esercizio 5.110) che il coniugato di ogni commutatore è ancora un commutatore.

Per ogni $x, y, g \in G$, $g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1}$, dunque:

$$g[x, y]g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}]$$

(2) Mostriamo che, per ogni $x, y \in G$, si ha:

$$\underbrace{xG'yG'}_{xyG'} = \underbrace{yG'xG'}_{yxG'}$$

Dobbiamo provare che $yx \in xyG'$, in questo modo le due classi laterali xyG' e yxG' non sarebbero disgiunte, e quindi sarebbero la stessa classe (ricordiamo che le classi laterali formano una partizione del gruppo).

$$yx = xyy^{-1}x^{-1}yx = xy[y^{-1}, x^{-1}] \in xyG'$$

(3) G/H abeliano implica che, per ogni x, y in G, si ha:

$$xyH = yxH \Leftrightarrow x^{-1}y^{-1}xyH = x^{-1}y^{-1}yxH$$

ovvero$[x^{-1}, y^{-1}]H = H$ e quindi, per ogni $x, y \in G$, si ha che $[x^{-1}, y^{-1}] \in H$, ovvero $G' < H$.

5. Omomorfismi di gruppo

In questo paragrafo introduciamo l'idea di omomorfismo (nel caso specifico dei gruppi). Tale concetto è fondamentale in algebra: l'omomorfismo infatti è una particolare applicazione che ha la proprietà di conservare la struttura algebrica.

Definizione 5.115. Siano $(G, *)$ e $(G', *')$ gruppi. Una funzione $f : G \longrightarrow G'$ si dice un **omomorfismo di gruppi** se per ogni x, y in G si ha:

$$f(x * y) = f(x) *' f(y)$$

Esempio 5.116. Vediamo alcuni esempi di omomorfismi di gruppo[3]

- Sia $(G, *)$ un gruppo su cui è definita una relazione di equivalenza $\sim$ compatibile con $*$. La proiezione canonica π, introdotta nell'Esempio 1.26, è un omomorfismo (surgettivo) da $(G, *)$ sul gruppo quoziente (questo fatto segue dalla definizione di operazione indotta sul gruppo quoziente che abbiamo dato).

  Un caso particolare di proiezione canonica è quella definita a partire dalla relazione $\sim_H$ (con $H \lhd G$), che va da G a G/H, e che associa ad ogni x in G, la classe laterale xH. Se consideriamo il gruppo $(\mathbb{Z}, +)$, fissato n intero positivo, la proiezione π_n che ad ogni a in $\mathbb{Z}$ associa $[a]_n$ è un omomorfismo surgettivo da $\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$.
- Consideriamo i gruppi $(\mathbb{R}, +)$ ed $(\mathbb{R}^+, \cdot)$, fissato a in $\mathbb{R}^+$, la funzione f_a da $(\mathbb{R}, +)$ a $(\mathbb{R}^+, \cdot)$ definita da: per ogni $x \in \mathbb{R}$, $f_a(x) = a^x$, è un omomorfismo tra il gruppo additivo $\mathbb{R}$ ed il gruppo moltiplicativo $\mathbb{R}^+$. Infatti, per ogni x, y in $\mathbb{R}$:

  $$f(x + y) = a^{x+y} = a^x \cdot a^y = f(x) \cdot f(y)$$

  Analogamente si può dimostrare, con le stesse notazioni precedenti, che l'applicazione $g(x) = log_a(x)$ è un omomorfismo da $(\mathbb{R}^+, \cdot)$ ad $(\mathbb{R}, +)$.
- Mostriamo anche un esempio di applicazione che non è un omomorfismo. Consideriamo la funzione f dal gruppo $(\mathbb{R}, +)$ in se stesso, che ad ogni x di $\mathbb{R}$ associa l'elemento $f(x) = x + 1$. Tale f non è un omomorfismo di gruppo in quanto $f(x + y) = x + y + 1$ è diverso da $f(x) + f(y)$, che è $(x + 1) + (y + 1)$, ovvero $x + y + 2$

Esercizio 5.117. *Siano $(G, *)$, $(H, \diamond)$ e $(T, \cdot)$ gruppi e $f : G \to H$, $g : H \to T$ omomorfismi di gruppo. Allora $g \circ f$ è un omomorfismo.*

Svolgimento. $g \circ f$ è una applicazione da G in T definita da

$$(g \circ f)(x) = g(f(x))$$

Dobbiamo dimostrare che, per ogni $x, y \in G$:

$$(g \circ f)(x * y) = (g \circ f)(x) \cdot (g \circ f)(y)$$

[3]Laddove non ci sia ambiguità, nel seguito ometteremo il riferimento alla struttura di gruppo e scriveremo *omomorfismo*.

Essendo per ipotesi f e g omomorfismi, effettivamente si ha:

$$g(f(x*y)) \underbrace{=}_{f\ omo.} g(f(x)\diamond f(y)) \underbrace{=}_{g\ omo.} g(f(x))\cdot g(f(y)) = (g\circ f)(x)\cdot(g\circ f)(y)$$

Cominciamo ad osservare alcune proprietà interessanti degli omomorfismi di gruppi.

Teorema 5.118 (Proprietà degli omomorfismi)**.** *Se f è un omomorfismo di gruppi da $(G,*)$ a $(G',*')$, allora:*

(1) *$f(e) = e'$.*
(2) *Per ogni x in G si ha $f(x^{-1}) = f(x)^{-1}$.*
(3) *Se $x \in G$ ha ordine finito n, allora $f(x)$ ha ordine che divide n.*

Dimostrazione. Per definizione di elemento neutro $e = e*e$, perciò:

$$f(e) = f(e*e) \underbrace{=}_{def.omo.} f(e) *' f(e)$$

Da cui, essendo $(G',*')$ un gruppo, e moltiplicando entrambi i membri per $f(e)^{-1}$ si ottiene $e' = f(e)$.

Dal punto appena dimostrato abbiamo che:

$$e' = f(e) = f(x*x^{-1}) \underbrace{=}_{def.omo.} f(x) *' f(x^{-1})$$

da cui, moltiplicando agli estremi della catena di uguaglianze per $f(x)^{-1}$, si ottiene:

$$f(x)^{-1} = f(x^{-1})$$

Abbiamo cioè dimostrato che l'inverso in G dell'immagine tramite l'omomorfismo f di x ($f(x)^{-1}$) è uguale all'immagine tramite f dell'inverso in G di x ($f(x^{-1})$).

Infine, se n è tale che $x^n = e$, allora:

$$f(x)^n \underbrace{=}_{def.omo.} f(x^n) \underbrace{=}_{n\ ordine\ di\ x} f(e) = e'$$

□

Un'altra proprietà interessante degli omomorfismi, è la seguente:

Proposizione 5.119. *Un omomorfismo $f : G \longrightarrow G'$ con G ciclico è univocamente determinato dal valore che f assume su un generatore di G.*

Dimostrazione. Sia g un generatore di G e $f(g) = w \in G'$. Allora, per definizione di generatore, per ogni $h \in G$ esiste t intero tale che $h = g^t$. Essendo f un omomorfismo si ha che $f(g^t) = f(g)^t = w^t$. □

Osservazione 5.120. Il teorema 5.119 ci dice ad esempio che per definire un omomorfismo da $(\mathbb{Z}/m\mathbb{Z},+)$ in un gruppo G, basta definire l'immagine di un generatore di $\mathbb{Z}/m\mathbb{Z}$, ovvero $[1]_m$ o una qualsiasi classe $[a]_m$ con a coprimo con m.

Esercizio 5.121. *Dati n, m interi maggiori di 1, quanti sono gli omomorfismi distinti da $\mathbb{Z}/n\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}$? Descriverli.*

Svolgimento. Dalla Proposizione 5.119 sappiamo che, per definire un omorfismo f da $\mathbb{Z}/n\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}$, basta stabilire il valore di $[a]_m$ tale che $f([1]_n) = [a]_m$ (abbiamo scelto $[1]_n$ perché sicuramente genera $\mathbb{Z}/n\mathbb{Z}$, ma avremmo potuto scegliere l'immagine di una qualsiasi classe $[g]_n$ con g tale che $(g,n) = 1$). Tuttavia il Teorema

5.118 ci mette in guardia sul fatto che non ogni valore di $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$ definisce un omomorfismo, $[a]_m$ deve rispettare la seguente condizione:

$$o([a]_m) = o(f([1]_n))|o([1]_n) = n$$

Per contare i possibili omomorfismi, dobbiamo quindi contare quante sono le classi $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$ che hanno ordine che divide n. Sono tutte e sole quelle per cui $n[a]_m = [0]_m$, ovvero bisogna contare quante soluzioni ha in $\mathbb{Z}/m\mathbb{Z}$ la congruenza seguente (dove m, n sono dati e l'incognita è a):

$$a \cdot n \equiv 0 \ (m)$$

Dalla Proposizione 4.87 sappiamo che la precedente congruenza è equivalente a:

$$a \equiv 0 \ \left(\frac{m}{(m,n)}\right)$$

Le soluzioni di questa congruenza in $\mathbb{Z}/m\mathbb{Z}$ sono le classi $[a]_m$ con a multiplo di $\dfrac{m}{(m,n)}$. Dunque abbiamo esattamente (m,n) soluzioni distinte:

$$a \in \left\{0, \frac{m}{(m,n)}, 2\frac{m}{(m,n)} \ldots, ((m,n)-1)\frac{m}{(m,n)}\right\}$$

Ogni soluzioni distinta $[a]_m$ identifica uno e un solo omomorfismo da $\mathbb{Z}/n\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}$ descritto da $f([1]_n) = [a]_m$.

Proposizione 5.122. *Dati n, m interi maggiori di 1 coprimi, esiste un solo omomorfismo da $\mathbb{Z}/n\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}$, quello descritto da $f([1]_n) = [0]_m$: ovvero l'omomorfismo nullo che manda tutto $\mathbb{Z}/n\mathbb{Z}$ in $[0]_m$.*

Mostriamo ora come gli omomorfismi di gruppi *conservano* i sottogruppi.

Proposizione 5.123. *Sia $f : G \to G'$ un omomorfismo di gruppi e H un sottogruppo di $(G, *)$, allora $f(H)$, l'immagine di H tramite f, è un sottogruppo di $(G', *')$.*

Dimostrazione. $f(H)$ non è vuoto, sappiamo ad esempio che e' appartiene a $f(H)$. Mostriamo dunque che, per ogni $x, y \in f(H)$, l'elemento $x *' y^{-1}$ è ancora in $f(H)$ e dunque (Lemma 5.39) che $f(H)$ è un sottogruppo di G'.

Per ipotesi esistono $g, r \in H$ controimmagini in G rispettivamente di x e y, cioè tali che $f(g) = x$, $f(r) = y$. Essendo H un gruppo, anche $r^{-1} \in H$ e di conseguenza anche $g * r^{-1}$ appartiene ad H, perciò $f(g * r^{-1}) \in f(H)$. Inoltre:

$$f(g * r^{-1}) \underbrace{=}_{f \text{ omo}} f(g) *' f(r^{-1}) \underbrace{=}_{teo.\ 5.118} x *' f(r)^{-1} = x *' y^{-1}$$

□

Corollario 5.124. *Sia $f : G \longrightarrow G'$ un omomorfismo e $(G', *')$ generato da un sottoinsieme S'. Allora f è surgettivo se e solo se $S' \subset f(G)$.*

Dimostrazione. Se f è surgettivo $f(G) = G'$ e contiene S'.

Viceversa, se $f(G) \supset S'$, allora $f(G)$ è un sottogruppo di $(G', *')$. G' è, per definizione, il più piccolo sottogruppo contenente S'. Perciò $f(G) = G'$. □

Esercizio 5.125. *Se $f : G \longrightarrow G'$ è un omomorfismo di gruppi e $H < G'$ allora la controimmagine $f^{-1}(H)$ di H in G è un sottogruppo di H.*

Abbiamo visto (Proposizione 5.123 ed Esercizio 5.125) che gli omomorfismi conservano i sottogruppi *in avanti e indietro* (ovvero anche considerando le controimmagini). Mostriamo come per la qualità di essere un sottogruppo *normale* le cose si complichino.

Teorema 5.126. *Se $f : G \longrightarrow G'$ è un omomorfismo di gruppi e $H \lhd G'$, allora $f^{-1}(H)$ è un sottogruppo normale di G. Viceversa se $T \lhd G$ in generale non è vero che $f(T)$ sia un sottogruppo normale di G'.*

Dimostrazione. Indichiamo con S la controimmagine $f^{-1}(H)$ di H. Per ogni x in G si ha che ogni elemento di xSx^{-1} sta in S, infatti:

$$f(xSx^{-1}) \underbrace{=}_{f \text{ omo.}} f(x)f(S)f(x^{-1}) \underbrace{=}_{f(S)=H,\ Teo.5.118} f(x)Hf(x)^{-1} \underbrace{=}_{H \lhd G'} H$$

Dunque, dalla Proposizione 5.108 segue che S è normale.

Viceversa, sia $(G, *)$ un gruppo e $T < G$ non normale. Consideriamo l'identità i da T a G che manda ogni $t \in T$ in $i(t) = t$. È facile mostrare che i è un omomorfismo di gruppi, inoltre $T \lhd T$, ma, per come è stato scelto, $i(T) = T$ non è un sottogruppo normale di G. □

Abbiamo dunque visto che un omomorfismo *preserva* i sottogruppi, ma in generale non il fatto di essere sottogruppi normali. Mostriamo adesso che, aggiungendo l'ipotesi di surgettività dell'omomorfismo, allora anche l'immagine di sottogruppi normali è un sottogruppo normale.

Lemma 5.127. *Se $f : G \longrightarrow G'$ è un omomorfismo surgettivo di gruppi e $H \lhd G$, allora $f(H) \lhd G'$.*

Dimostrazione. La surgettività di f ci dice che, per ogni t in G', esiste x in G con $f(x) = t$. Dunque:

$$tf(H)t^{-1} \underbrace{=}_{f \text{ omo.}} f(xHx^{-1}) \underbrace{=}_{H \lhd G} f(H)$$

□

Abbiamo appena mostrato che, se un omomorfismo da $(G, *)$ a $(G', *')$ è surgettivo, allora c'è corrispondenza biunivoca tra sottogruppi (normali) di G e sottogruppi (normali) di G'. Oltre a proseguire nello studio delle proprietà degli omomorfismi surgettivi e iniettivi, al fine di arrivare a considerare poi quelli bigettivi, siamo interessati ad analizzare ancora più da vicino la corrispondenza tra sottogruppi di G e G', letta tramite un omomorfismo da G a G'.

Definizione 5.128. Dati due gruppi $(G, *)$ e $(G', *')$ e un omomorfismo f da G in G', chiamiamo **nucleo** dell'omomorfismo f il seguente sottoinsieme di G:

$$Ker\ f = \{x \in G | f(x) = e'\}$$

Proposizione 5.129. *Il nucleo $Ker\ f$ di un omomorfismo di gruppi f da $(G, *)$ in $(G', *')$ è un sottogruppo normale di G.*

Dimostrazione. Abbiamo già osservato (Teorema 5.118) che $Ker\ f$ non è vuoto ($e \in Ker\ f$). Per ogni x, y in $Ker\ f$, xy^{-1} sta in $Ker\ f$, infatti:

$$f(xy^{-1}) \underbrace{=}_{f \text{ omo.}} f(x)f(y)^{-1} \underbrace{=}_{x,y \in Ker\ f} e'e' = e'$$

Dunque $Ker\ f$ è un sottogruppo di G.

Adesso mostriamo che, per ogni $x \in G$ e $k \in Ker\ f$, si ha $xkx^{-1} \in Ker\ f$:

$$f(xkx^{-1}) \underbrace{=}_{f\ omo.} f(x)f(k)f(x)^{-1} \underbrace{=}_{k \in Ker\ f} f(x)ef(x)^{-1} = e'$$

Abbiamo dunque provato (Proposizione 5.108) che $Ker\ f \lhd G$. □

Esercizio 5.130. *Sia f un omomorfismo tra $(\mathbb{Z}, +)$ e $(\mathbb{Z}/m\mathbb{Z}, +)$, allora $Ker\ f$ contiene $m\mathbb{Z}$.*

Svolgimento. Basta mostrare che m appartiene a $Ker\ f$, infatti il sottogruppo $Ker\ f$ conterrà necessariamente $m\mathbb{Z}$ (il più piccolo sottogruppo contenente m).

$$f(m) = f(\underbrace{1 + \ldots + 1}_{m\ volte}) \underbrace{=}_{f\ omo.} [m \cdot f(1)]_m = [0]_m$$

Dato un omomorfismo di gruppi f da $(G, *)$ in $(G', *')$, il sottogruppo normale $Ker\ f$ di G ha un *ruolo* particolare nella descrizione della controimmagine di un elemento g' appartenente all'immagine di f.

Teorema 5.131. *Sia f da $(G, *)$ in $(G', *')$ un omomorfismo di gruppi. Sia g' un elemento dell'immagine di f, allora l'insieme*

$$f^{-1}(g') = \{g \in G | f(g) = g'\}$$

controimmagine di g' tramite f è uguale ad una classe laterale di $Ker\ f$.

Dimostrazione. Prima di dimostrare il teorema, osserviamo che non è necessario specificare classe laterale destra o sinistra nell'enunciato in quanto abbiamo appena dimostrato che il $Ker\ f$ è un sottogruppo normale di G. Indichiamo, per semplicità di notazione, il $Ker\ f$ con K.

L'insieme $f^{-1}(g')$ non è vuoto in quanto, per ipotesi, $g' \in f(G)$. Sia $x \in f^{-1}(g')$, e consideriamo la classe laterale xK. Per ogni a in $f^{-1}(g')$ si ha:

$$e' = {g'}^{-1} *' g' = f(x)^{-1} *' f(a) \underbrace{=}_{f\ omo.} f(x^{-1} * a)$$

Dunque $x^{-1} * a \in K$, ovvero $a \in xK$ e quindi $f^{-1}(g') \subseteq xK$.

Viceversa sia $a \in xK$, allora esiste k in K tale che $a = x * k$, e:

$$f(a) = f(x * k) \underbrace{=}_{f\ omo.} f(x) *' f(k) = g' *' e' = g'$$

Cioè $a \in f^{-1}(g')$, che implica $xK \subseteq f^{-1}(g')$, e quindi la tesi. Osserviamo in particolare che, se $x \in f^{-1}(g')$, allora $f^{-1}(g')$ è uguale alla classe laterale xK. □

Dal teorema 5.131 segue un importante risultato che caratterizza i sottogruppi normali di un gruppo $(G, *)$ come i nuclei di omomorfismi da G ad un altro gruppo.

Teorema 5.132. *I sottogruppi normali di un gruppo $(G, *)$ sono tutti e soli i nuclei di omomorfismi di gruppo da G ad un altro gruppo $(G', *')$.*

Dimostrazione. Abbiamo già dimostrato (Proposizione 5.129) che i nuclei di omomorfismi che *partono* da G sono sottogruppi normali di G. Dobbiamo dunque mostrare che, dato un sottogruppo normale H di G, esiste un omomorfismo che parte da G di cui H è il nucleo.

L'idea è piuttosto naturale: consideriamo il gruppo quoziente $G' = G/H$ e la proiezione canonica π_H che ad ogni elemento x di G associa la classe laterale xH. L'elemento neutro di G/H è la classe laterale H (Esercizio 5.104).

$$Ker\ \pi_H = \{x \in G | \pi_H(x) = H\} = \{x \in G | xH = H\}$$

Per concludere basta osservare che $xH = H$ se e solo se $x \in H$. □

Proposizione 5.133. *Sia $f : G \to G'$ un omomorfismo surgettivo di gruppi. L'omomorfismo surgettivo f induce una corrispondenza biunivoca tra:*

- *sottogruppi di G che contengono $Ker\ f$,*
- *sottogruppi di G'.*

Inoltre $H \lhd G \Leftrightarrow f(H) \lhd G'$.

Dimostrazione. In generale (Proposizione 5.123), se $H < G$, allora $f(H)$ è sottogruppo di G': ciò è in particolare vero per i sottogruppi H di G che contengono $Ker\ f$. Inoltre (Teorema 5.126), se $H' < G'$, sappiamo che $f^{-1}(H')$ è un sottogruppo di G. Osserviamo che tale sottogruppo contiene $Ker\ f$, infatti per ogni $k \in Ker\ f$, $f(k) = e'$ è un elemento del sottogruppo H', dunque $k \in f^{-1}(H')$.

Ora indicando con A e B rispettivamente l'insieme dei sottogruppi di G che contengono $Ker\ f$ e l'insieme dei sottogruppi di G', dobbiamo mostrare che la restrizione di f ad un qualsiasi elemento di A è bigettiva su un elemento di B. Ovvero che $f : H \in A \to f(H) \in B$ e $f^{-1} : H' \in B \to f^{-1}(H') \in A$ sono una l'inversa dell'altra, ovvero che per ogni $H \in A$ e per ogni $H' \in B$, si ha:

$$f^{-1}(f(H)) = H$$
$$f(f^{-1}(H')) = H'$$

- $f^{-1}(f(H)) = H$.
  Sia $x \in H$, allora $f(x) \in f(H)$ e per definizione di insieme controimmagine $x \in f^{-1}(f(H))$, dunque $H \subset f^{-1}(f(H))$.
  Viceversa, sia $x \in f^{-1}(f(H))$. Questo significa che esiste $h \in H$ tale che $f(x) = f(h)$. Dall'osservazione alla fine del Teorema 5.131, sappiamo che questo implica $xKer\ f = hKer\ f$, ovvero $x \in hKer\ f$: cioè esiste $k \in Ker\ f$ tale che $x = h * k$. D'altra parte $h * k \in H$ in quanto, per ipotesi, $Ker\ f \subset H$. Perciò $f^{-1}(f(H)) = H$.
- $f(f^{-1}(H')) = H'$.
  Sia $x' \in f(f^{-1}(H'))$, allora esiste $y \in f^{-1}(H')$ tale che $x' = f(y)$. Per definizione di $f^{-1}(H')$, $f(y) \in H'$ e quindi $f(f^{-1}(H')) \subset H'$.
  Viceversa se $x' \in H'$, essendo f surgettivo, esiste $x \in G$ tale che $f(x) = x'$. x è un elemento di $f^{-1}(H')$ e quindi $x' \in f(f^{-1}(H'))$. Perciò $f(f^{-1}(H')) = H'$.

□

Esempio 5.134. $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ è un omomorfismo surgettivo, che associa ad ogni intero x la sua classe $[x]_m$ modulo m. Il nucleo di π è $m\mathbb{Z}$, ovvero i multipli di m. La Proposizione 5.133 ci dice che esiste una corrispondenza biunivoca tra i sottogruppi di $\mathbb{Z}$ che contengono $m\mathbb{Z}$ e i sottogruppi di $\mathbb{Z}/m\mathbb{Z}$.

Sia H un sottogruppo di $\mathbb{Z}$, dal Teorema 5.42 sappiamo che H è della forma $d\mathbb{Z}$, e se contiene $m\mathbb{Z}$ deve essere (Esercizio 5.43) che d divide m. Dunque, dato d che

divide m, la corrispondenza biunivoca descritta dalla Proposizione 5.133 associa al sottogruppo $d\mathbb{Z}$ la sua immagine tramite π: $\pi(d\mathbb{Z}) = d\mathbb{Z}/m\mathbb{Z}$, che ha $\frac{m}{d}$ elementi.

Ad esempio, se consideriamo π_{12}, al sottogruppo $3\mathbb{Z}$ di $\mathbb{Z}$ è associato il sottogruppo $\pi_{12}(3\mathbb{Z}) = 3\mathbb{Z}/12\mathbb{Z}$ di $\mathbb{Z}_{12}$, che è composto dai seguenti quattro elementi: $[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}$.

Abbiamo osservato come il nucleo di un omomorfismo, oltre ad essere *intimamente intrecciato* con il concetto di sottogruppo normale, fornisce importanti informazioni sulle controimmagini. Questo serve anche per discutere l'iniettività dell'omomorfismo.

Teorema 5.135. *Un omomorfismo f da $(G, *)$ in $(G', *')$ è iniettivo se e solo se $Ker\ f = \{e\}$, dove e è l'elemento neutro di G.*

Dimostrazione. Sappiamo che $f(e) = e'$, dunque se f è iniettivo nessun elemento diverso da e può avere come immagine e', ovvero $Ker\ f = \{e\}$.

Viceversa se $Ker\ f = \{e\}$, allora tutte le classi laterali di $Ker\ f$ hanno un elemento (Proposizione 5.88). D'altra parte, abbiamo appena dimostrato (Teorema 5.131) che gli insiemi controimmagine degli elementi di $f(G)$ sono proprio classi laterali di $Ker\ f$, dunque hanno un solo elemento. Questo significa proprio che f è iniettiva. □

Quanto appena dimostrato, nel caso di gruppi finiti, fornisce un ulteriore criterio per determinare la iniettività di un omomorfismo, o per costruire omomorfismi iniettivi.

Teorema 5.136. *Un omomorfismo $f : G \longrightarrow G'$ con $(G, *)$, $(G', *')$ gruppi finiti è iniettivo se e solo se per ogni $x \in G$ si ha che $o(x) = o(f(x))$.*

Dimostrazione. $\Rightarrow$) Supponiamo f iniettiva e che esista x con $o(f(x)) = m$ minore di $n = o(x)$. Avremmo:

$$e' \underbrace{=}_{o(f(x))=m} (f(x))^m \underbrace{=}_{f\ omo.} f(x^m)$$

Ovvero x^m sarebbe un elemento di $Ker\ f$ diverso da e. Assurdo per quanto dimostrato nel Teorema 5.135. Dunque deve essere $o(x) = o(f(x))$ per ogni x in G.

$\Leftarrow$) Sia x un elemento di $Ker\ f$, allora $f(x) = e'$ ha ordine 1, dunque per ipotesi x stesso deve avere ordine 1. Abbiamo dimostrato che x appartiene a $Ker\ f$ se e solo se ha ordine 1, ovvero che $Ker\ f = \{e\}$. □

Esercizio 5.137. *Dati n, m interi maggiori di 1, quanti sono gli omomorfismi iniettivi da $\mathbb{Z}/n\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}$? E quelli surgettivi?*

Svolgimento. Nell'Esercizio 5.121 abbiamo mostrato che il numero di omomorfismi da $\mathbb{Z}/n\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}$ è $d = (m, n)$, e che sono descritti da $f([1]_n) = [a]_m$ al variare di a nell'insieme:

$$\left\{0, \frac{m}{(m,n)}, 2\frac{m}{(m,n)} \ldots, ((m,n)-1)\frac{m}{(m,n)}\right\}$$

Affinchè l'omomorfismo f sia iniettivo, deve essere che $f([1]_n)$ abbia ordine n in $\mathbb{Z}/m\mathbb{Z}$. Allora condizione necessaria per l'esistenza di un omomorfismo iniettivo è che n divida m. Supponiamo che questa condizione sia verificata, cioè che esista

k tale che $m = nk$, e cerchiamo di descrivere (e quindi anche contare) i possibili omomorfismi iniettivi:

$$f([1]_n) = [a]_m = [\lambda k]_m \quad \text{con } 0 \leq \lambda < n$$

Vogliamo che:

$$f([x]_n) = [0]_m \Leftrightarrow [x]_n = [0]_n,$$

ovvero:

$$\lambda k x \equiv 0 \ (m) \Leftrightarrow x \equiv 0 \ (n).$$

Ma $\lambda k x \equiv 0 \ (m)$ è equivalente a $\lambda x \equiv 0 \ (n)$ e quindi la condizione precedente può essere riscritta come segue:

$$\lambda x \equiv 0 \ (n) \Leftrightarrow x \equiv 0 \ (n).$$

Questa condizione è verificata quando λ è invertibile in $\mathbb{Z}/n\mathbb{Z}$, ovvero quando $(\lambda, n) = 1$. Quanti ce ne sono di questi λ (e quindi di omomorfismi iniettivi)? Lo sappiamo, sono $\phi(n)$.
In conclusione:

- Se n divide m, esistono $\phi(n)$ omomorfismi iniettivi da $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$, definiti da:
$$f([1]_n) = [\frac{m}{n}\lambda]_m$$
con λ scelto tra gli invertibili in $\mathbb{Z}/n\mathbb{Z}$.
- Se n non divide m non ci sono omomorfismi iniettivi tra $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z}$.

Dal Corollario 5.124 sappiamo che f è surgettiva se e solo se $f(\mathbb{Z}/n\mathbb{Z})$ contiene un generatore di $\mathbb{Z}/m\mathbb{Z}$. Deve quindi esistere $[x]_n \in \mathbb{Z}/n\mathbb{Z}$ tale che $f([x]_n) = [g]_m$, con (g, m)=1. D'altra parte, se uno $[x]_n$ siffatto esiste, sappiamo (Teorema 5.118) che $o([g]_m)$, ovvero m, deve dividere $o([x]_n$. In particolare, condizione necessaria affinché esistano omomorfismi surgettivi da $\mathbb{Z}/n\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z}$ è che m divida n (che è un multiplo di $o([g]_m)$).

Osserviamo che abbiamo trovato che le due condizioni necessarie per l'iniettività e la surgettività sono rispettivamente $m|n$ e $n|m$, cioè, come sapevamo già per questioni di cardinalità, per la bigettività condizione necessaria è $m = n$.

Mostriamo come con la condizione m divide n rispettata, riusciamo a costruire $\phi(m)$ omomorfismi surgettivi differenti. Infatti, la congruenza $ax \equiv g \ (m)$ ha soluzione se e solo se $(a, m)|g$, ma essendo $(m, g) = 1$ questo equivale a dire che $(a, m) = 1$. Abbiamo dunque un omomorfismo surgettivo (definito da $f([1]_n) = [a]_m$) da $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$, per ogni scelta di $[a]_m$ con $(a, m) = 1$.

6. Teoremi di omomorfismo di gruppi

Dalla Proposizione 5.133 sappiamo che se f è un omomorfismo surgettivo tra $(G, *)$ e $(G', *')$ allora i sottogruppi (normali) di G e di G' sono in corrispondenza biunivoca. Dal Teorema 5.136 sappiamo che se f è iniettiva c'è corrispondenza biunivoca tra elementi dello stesso ordine di G e G'. Dunque l'esistenza di un omomorfismo bigettivo (sia iniettivo che surgettivo) tra G e G' sembra essere particolarmente significativa (in pratica ci dice che G e G' come gruppi sono *indistinguibili*, se non per le *etichette* che usiamo per indicare i loro elementi e la loro operazione), da meritare una terminologia ad hoc.

Definizione 5.138. Un omomorfismo di gruppi iniettivo e surgettivo si dice un **isomorfismo** di gruppi.
Due gruppi $(G, *)$ e $(G', *')$ si dicono **isomorfi** se esiste un isomorfismo tra essi. Useremo la notazione $G \cong G'$ per indicare che G e G' sono isomorfi.

Esercizio 5.139. *Se f è un isomorfismo di gruppi da $(G, *)$ a $(G', *')$ allora anche $f^{-1} : G' \longrightarrow G$ è un isomorfismo.*

Svolgimento. Essendo f bigettiva, f^{-1} è definita ed è bigettiva. Dobbiamo quindi provare che f^{-1} è un omomorfismo di gruppi, ovvero che per ogni $a, b \in G'$ si ha:

$$f^{-1}(a *' b) = f^{-1}(a) * f^{-1}(b)$$

D'altra parte, per ogni a, b in G', per l'ipotesi di bigettività di f esistono $x, y \in G$ tali che $f(x) = a$ e $f(y) = b$, perciò:

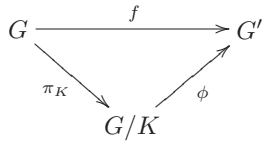
$$f^{-1}(a *' b) = f^{-1}(f(x) *' f(y)) \underbrace{=}_{f \text{ omo.}} f^{-1}(f(x * y)) = x * y = f^{-1}(a) * f^{-1}(b)$$

Esercizio 5.140. *Dimostrare che la relazione $\Re$ $G \Re G' \Leftrightarrow G \cong G'$ è di equivalenza.*

Mostriamo come, a partire da un omomorfismo f tra due gruppi G e G', si possa costruire un unico omomorfismo iniettivo tra il gruppo quoziente $G/Ker\ f$ e G'.

Teorema 5.141 (Primo teorema di omomorfismo per gruppi)**.** *Siano $(G, *)$ e $(G', *')$ gruppi e $f : G \longrightarrow G'$ un omomorfismo di gruppi e sia K il nucleo di f. Allora esiste un unico omomorfismo $\phi : G/K \longrightarrow G'$ tale che $f = \phi \circ \pi_K$, inoltre ϕ è iniettivo. ϕ è surgettivo se e solo se f è surgettivo.*

Dimostrazione. La situazione del teorema è descritta dal seguente diagramma (per dire che ϕ è tale che $f = \phi \circ \pi_K$ si dice anche che **commuta** con il diagramma):



Esistenza di ϕ. L'enunciato del teorema ci dice che, per ogni xK in G/K, poniamo $\phi(xK)$ uguale a $f(x)$. Dobbiamo mostrare innanzitutto che $\phi(xK) = f(x)$ è una buona definizione, cioè non dipende dalla scelta del rappresentante in xK: ovvero se y appartiene anch'esso a xK, vogliamo che $\phi(yK)$ sia uguale a $\phi(xK)$, ovvero $f(y)$ deve essere uguale a $f(y)$. Questo ci è assicurato dal Teorema 5.131.

A questo punto dobbiamo mostrare che ϕ è un omomorfismo. Per ogni coppia di classe laterali xK, yK in G/K si ha:

$$\phi(xK * yK) \underbrace{=}_{K \lhd G} \phi((x * y)K) \underbrace{=}_{def.\ \phi} f(x * y) \underbrace{=}_{f \text{ omo.}} f(x) *' f(y) \underbrace{=}_{def.\ \phi} \phi(xK) *' \phi(yK)$$

Unicità di ϕ. Abbiamo dimostrato che esiste un omomorfismo ϕ che rende il diagramma commutativo, ovvero tale che $f = \phi \circ \pi_K$, da questo segue che ϕ è unico in quanto per ogni classe xK il valore di $\phi(xK)$ è univocamente determinato da $\phi(xK) = f(x)$.
Iniettività di ϕ. Il nucleo di ϕ è l'insieme $Ker\ \phi = \{xK \in G/K | \phi(xK) = e'\}$. Osserviamo che $\phi(xK) = f(x) = e'$ se e solo se x è un elemento di K (il nucleo di f),

dunque se e solo se $xK = K$. Abbiamo dunque dimostrato che $Ker\ \phi$ è composto dal solo elemento neutro (K) del gruppo quoziente G/K, e dunque l'iniettività segue dal Teorema 5.135.
ϕ **surgettivo se e solo se** f **surgettivo**. Basta osservare che f e ϕ hanno la stessa immagine, dunque ϕ è surgettiva se e solo se f lo è. □

Dal Teorema 5.141 segue in particolare che:

Teorema 5.142. *Se $f : G \longrightarrow H$ è un omomorfismo di gruppi allora:*

$$G/Ker\ f \cong f(G)$$

Da quanto appena provato, e dal risultato del Teorema 5.132, segue che le possibili immagini tramite omomorfismo di un gruppo $(G, *)$ sono tutti e soli i gruppi quoziente G/N, con N sottogruppo normale di G. Si possono perciò studiare tutte le immagini omomorfe (ovvero ottenute tramite omomorfismo) di un gruppo $(G, *)$ *senza uscire* dal gruppo G stesso, studiando l'insieme G/N al variare di N nell'insieme dei sottogruppi normali di G.

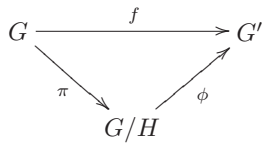
Corollario 5.143. *Se f è un omomorfismo surgettivo da $(G, *)$ a $(G', *')$ e $H < G$ tale che $f(H) = G'$ e $Ker\ f \subset H$ allora $H = G$.*

Dimostrazione. Dal primo teorema di omomorfismo per gruppi sappiamo che:

$$H/Ker\ f \cong \underbrace{G'}_{f(H)} \cong G/Ker\ f$$

Questo implica che $H \cong G$, ma sapendo che $H < G$ si ha $H = G$. □

Il Teorema 5.141 ci dice che un omomorfismo di gruppi $f : G \longrightarrow G'$ con nucleo K induce, in maniera unica, un omomorfismo iniettivo ϕ da G/K in G' tale che $f = \phi \circ \pi_K$. Ci chiediamo se lo stesso vale per un qualsiasi sottogruppo normale H di G (non necessariamente K), ovvero se si può trovare un omomorfismo ϕ da G/H in G' che commuti con il seguente diagramma:



Per poter ben definire ϕ in modo tale che $f = \phi \circ \pi_H$ deve essere che, se $xH = yH$, allora $\phi(xH) = \phi(yH)$, ovvero $f(x) = f(y)$. Affinché $f(x) = f(y) = g$, deve essere (Teorema 5.131) che x e y stanno nella stessa classe laterale di K ($xK = yK$), dunque ϕ è ben definita se e solo se, per ogni $x, y \in G$, $xH = yH$ implica $xK = yK$.

Per definizione della relazione di equivalenza che definisce le classi laterali, questa condizione è equivalente al fatto che, per ogni x, y in G si abbia che $xy^{-1} \in H$ implica $xy^{-1} \in K$. Questo accade se e solo se $H \subseteq K$. Abbiamo dunque provato che:

Proposizione 5.144. *Dato un omomorfismo di gruppi $f : G \longrightarrow G'$ e un sottogruppo normale H di G, è possibile definire (univocamente) un omomorfismo ϕ da G/H in G' tale che $f = \phi \circ \pi_H$ se e solo se $H \subset Ker\ f$.*

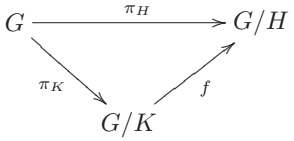
Osservazione 5.145. Osserviamo che, in generale, l'omomorfismo ϕ da G/H a G' della Proposizione 5.144 non è iniettivo.

Teorema 5.146 (Secondo teorema di isomorfismo per gruppi)**.** *Siano* $(G, *)$ *un gruppo,* $H \lhd G$*,* $K \lhd G$ *e* $K \subset H$*. Allora:*

$$G/H \cong (G/K)/(H/K)$$

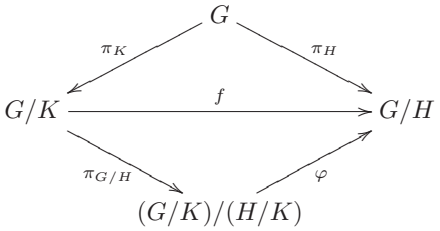
Dimostrazione. Osserviamo innanzitutto che tutti i quozienti sono ben definiti: le proiezioni canoniche sono surgettive e tutti i *denominatori* sono sottogruppi normali. Infatti, dal Lemma 5.127 segue che, se $H \lhd G$, allora $\pi_K(H) = H/K$ è un sottogruppo normale di G/K.

Consideriamo la proiezione π_H di G in G/H. Per ipotesi $K \subset H$ che è il nucleo di π_H perciò, per il primo teorema di omomorfismo, è definito un omomorfismo surgettivo (in quanto ha la stessa immagine di π_H che lo è) f da G/K a G/H che commuta con il seguente diagramma:



Il nucleo di f sono le classi laterali xK di K tali che $f(xK) = H$. Sapendo che il diagramma commuta, abbiamo che $f(xK) = f(\pi_K(x)) = \pi_H(x) = xH$: ovvero il nucleo di f sono le classi xK con $x \in G$ tale che $xH = H$, ovvero $x \in H$. Il nucleo di f è dunque H/K.

Sempre dal primo teorema di omomorfismo segue che possiamo definire un omomorfismo iniettivo φ, in modo tale che il seguente diagramma commuti:



Essendo f surgettivo, φ è un isomorfismo tra $G/H \cong (G/K)/(H/K)$. □

Il fatto che i gruppi isomorfi abbiano caratteristiche algebriche in comune ci spinge a cercare di classificare i gruppi e a descrivere le classi di equivalenza rispetto a $\cong$. Iniziamo con il teorema di Cayley, il quale evidenzia il ruolo del gruppo $S(G)$ delle bigezioni di un gruppo G in se stesso[4], mostrando come ogni gruppo G sia isomorfo ad un sottogruppo di $S(G)$.

Teorema 5.147 (Teorema di Cayley)**.** *Sia* $(G, *)$ *un gruppo. Esiste un omomorfismo iniettivo* ψ *da* G *a* $S(G)$*.*

Dimostrazione. Per prima cosa osserviamo che dalla tesi del teorema di Cayley segue che ψ è un isomorfismo tra G ed il sottogruppo $\psi(G)$ di $S(G)$.

Dato g in G, denotiamo con σ_g l'applicazione da G in G che ad ogni h associa l'elemento $g * h$. Consideriamo l'applicazione ψ che ad ogni elemento g di G associa l'applicazione σ_g. Per avere la tesi del teorema dobbiamo dimostrare due fatti

[4]Gruppo che abbiamo introdotto nell'Esercizio 5.13, e su cui torneremo, nel caso di G finito, in una apposita sezione alla fine del capitolo.

distinti: che σ_g appartiene a $S(G)$, e che ψ, a questo punto potremo dire da G a $S(G)$, è un omomorfismo iniettivo.

- Mostriamo che σ_g è un elemento di $S(G)$, ovvero è una applicazione bigettiva.

  Per ogni h, t in G, $\sigma_g(h) = \sigma_g(t)$ se e solo se $g * h = g * t$. Per la legge di cancellazione (Proposizione 5.26) si ha che $h = t$, ovvero σ_g è iniettiva.

  Per ogni h in G, si ha che $g^{-1} * h$ è un elemento di G, e $\sigma_g(g^{-1} * h) = h$. Dunque σ_g è surgettiva.
- Mostriamo che ψ è un omomorfismo iniettivo.

  Vogliamo innanzitutto mostrare che per ogni g, h in G, si ha:

  $$\underbrace{\psi(g * h)}_{\sigma_{g*h}} = \underbrace{\psi(g) \circ \psi(h)}_{\sigma_g \circ \sigma_h}$$

  Per far questo mostriamo che i due elementi di $S(G)$ coincidono per ogni elemento t di G e dunque sono la stessa funzione. Si ha infatti:

  $$\sigma_{g*h}(t) = (g * h) * t = g * (h * t) = g * \sigma_h(t) = \sigma_g(\sigma_h(t))$$

  Ci rimane da dimostrare che ψ è iniettivo. Per ogni g, h in G, se $\psi(g) = \psi(h)$, ovvero $\sigma_g = \sigma_h$, allora in particolare il loro valore in e (l'elemento neutro) coincide e dunque:

  $$g = g * e = \sigma_g(e) = \sigma_h(e) = h * e = h$$

□

Il teorema di Cayley evidenzia che qualsiasi gruppo può essere considerato come un particolare gruppo di permutazioni.

Cominciamo ora ad analizzare altri teoremi di isomorfismo rispetto a gruppi con specifiche caratteristiche, partendo dal caso dei gruppi ciclici.

Teorema 5.148 (Classificazione dei gruppi ciclici)**.** *Sia $(G, *)$ un gruppo ciclico.*

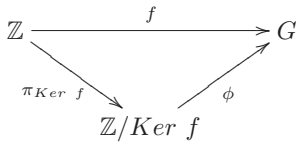
- *Se G è infinito allora $(G, *) \cong (\mathbb{Z}, +)$,*
- *Se G è finito di cardinalità m allora $(G, *) \cong (\mathbb{Z}/m\mathbb{Z}, +)$.*

Dimostrazione. Sia x un generatore di G. Consideriamo la funzione f da $\mathbb{Z}$ in G definita da $f(z) = x^z$. f è un omomorfismo di gruppi, infatti per ogni a, b in $\mathbb{Z}$:

$$f(a + b) = x^{a+b} = x^a * x^b = f(a) * f(b)$$

Inoltre f è surgettivo perché per ipotesi G è composto dalle potenze intere di x, che costituiscono esattamente l'immagine di f.

Per il primo teorema di omomorfismo per gruppi, esiste un isomorfismo ϕ che commuta con il seguente diagramma:



Dunque G è isomorfo a $\mathbb{Z}/Ker\ f$, con $Ker\ f$ sottogruppo di $\mathbb{Z}$. Dal Teorema 5.42 sappiamo che i sottogruppi di $\mathbb{Z}$ sono tutti e soli del tipo $n\mathbb{Z}$ (con n in $\mathbb{N}$), quindi possiamo distinguere due casi per $Ker\ f$:

- Se $Ker\ f = \{0\}$, allora $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ (più in generale $G/\{e\} \cong G$) e quindi $\mathbb{Z} \cong G$.
- Se $Ker\ f = m\mathbb{Z}$ con $m \neq 0$, allora l'insieme delle classi laterali di $Ker\ f$ è $\mathbb{Z}/m\mathbb{Z}$, quindi $\mathbb{Z}/m\mathbb{Z} \cong G$.

□

Abbiamo mostrato (Teorema 5.69) che, se G è un gruppo ciclico finito, per ogni divisore d dell'ordine di G esiste un sottogruppo di ordine d. Vogliamo adesso studiare il caso più generale di un gruppo abeliano finito ma non necessariamente ciclico.

Teorema 5.149 (Teorema di Cauchy per gruppi abeliani)**.** *Sia $(G, *)$ un gruppo abeliano finito di ordine $n > 1$. Sia p un primo che divide n, allora esiste $x \in G$ tale che $o(x) = p$.*

Dimostrazione. Sia $n = p \cdot m$, procediamo per induzione su m.
Passo base. Se $m = 1$, allora G ha ordine p, quindi (Corollario 5.96) G è ciclico e qualsiasi elemento di G diverso dall'identità ha ordine p.
Passo induttivo. Supponiamo la tesi vera per ogni gruppo G di ordine $p \cdot m'$ con $m' < m$ e dimostriamo che questo implica la tesi per i gruppi G di ordine $p \cdot m$.

Sia $y \in G$, $y \neq e$ e consideriamo il sottogruppo ciclico generato da y: $H =< y >$. $H \lhd G$ in quanto G è abeliano (e quindi ogni suo sottogruppo è normale), e (Teorema 5.89) $|G| = |H| \cdot |G/H|$. Per ipotesi p primo divide $|G|$, quindi p deve dividere almeno uno tra $|H|$ e $|G/H|$. Analizziamo i due casi separatamente.

(1) Se p divide $|H|$ allora abbiamo due possibilità: $|H| = p \cdot m$ e allora $G = H =< y >$ è ciclico e quindi dal Teorema 5.69 segue la tesi. Oppure $|H| = p \cdot m'$ con $m' < m$ e dunque, per ipotesi induttiva, esiste x in H con $o(x) = p$. Essendo $H < G$, x è in particolare un elemento di G.
(2) Se p divide $|G/H|$ allora $|G/H| = p \cdot m' < p \cdot m$, in quanto H contiene almeno due elementi y ed e. Per ipotesi induttiva esiste $zH \in G/H$ tale che $o(zH) = p$. Consideriamo allora la proiezione π_H da G in G/H che manda ogni x di G nella classe laterale xH. Essendo la proiezione canonica π_H un omomorfismo (vedi Esempio 5.116) per la terza proprietà del Teorema 5.118 si ha che l'ordine di zH (ovvero p) divide l'ordine di z. Cioè esiste k tale che $o(z) = p \cdot k$. Come nel caso precedente questo implica o che G è ciclico o, per ipotesi induttiva, che in $< z >$ esiste un elemento di ordine p.

□

Corollario 5.150. *Sia $(G, *)$ un gruppo abeliano finito di ordine $n > 1$. Sia p un primo che divide n, allora esiste $H < G$ tale che $|H| = p$.*

Dimostrazione. Il teorema di Cauchy ci assicura l'esistenza in G di x di ordine p. Allora basta considerare $H =< x >$. □

Teorema 5.151 (Teorema di Sylow per gruppi abeliani)**.** *Sia $(G, *)$ un gruppo abeliano finito di ordine $n > 1$. Sia p un primo tale che: p^m divide n, ma p^{m+1} non divide n, allora esiste $H < G$ con $|H| = p^m$.*

Dimostrazione. Il teorema è banalmente vero se $m = 0$ in quanto il sottogruppo $H = \{e\}$ ha un elemento come richiesto.

Se $m \neq 0$ per ipotesi p^m, e dunque anche p, divide n. Dal teorema di Cauchy segue che esiste un elemento $x \in G$ di ordine p. Consideriamo il seguente insieme:

$$H = \{g \in G | \exists t \in \mathbb{Z}\ g^{p^t} = e\}$$

È facile mostrare che $H < G$, inoltre $|H| > 1$ in quanto e e x sono elementi di H. Dimostriamo che $|H| = p^m$. Supponiamo per assurdo che un primo q diverso da p divida $|H|$, il teorema di Cauchy ci dice che esiste un elemento $h \in H$ di ordine q. Tale elemento dunque verifica $h^q = e$, inoltre, per definizione di H, esiste $r \in \mathbb{Z}$ con $h^{p^r} = e$. Essendo q e p^r coprimi, esistono a e b interi tali che $a \cdot q + b \cdot p^r = 1$. Dunque:

$$h = h^{a \cdot q + b \cdot p^r} = h^{a \cdot q} * h^{b \cdot p^r} = e * e = e$$

Questo è assurdo in quanto h ha ordine $q > 1$. Dunque $|H| = p^t$, ci rimane da dimostrare che $t = m$. Supponiamo per assurdo che t sia minore di m e consideriamo il gruppo abeliano G/H, il Teorema 5.89 ci dice che:

$$|G| = [G : H] \cdot |H|$$

Ovvero:

$$|G/H| = \frac{|G|}{|H|}$$

Dunque p divide $|G/H|$ e, sempre per il teorema di Cauchy, questo implica che esiste un elemento xH di G/H che ha ordine p, ovvero $(xH)^p = H$. Questo significa (siamo in un gruppo abeliano) che $x^p H = H$, cioè che $x^p \in H$. Da questo segue, per definizione di H, che $x \in H$ ovvero che $xH = H$. Assurdo perché xH doveva avere ordine $p > 1$ in G/H. Dunque deve essere $t = m$ ovvero $|H| = p^m$. □

Definizione 5.152. Sia G un gruppo finito di ordine $p^n \cdot k$ con k non divisibile per p (dunque p^n è la massima potenza di p che divide G). Un sottogruppo H di G di ordine p^n si dice **p-sottogruppo di Sylow** di G.

A seguito della definizione appena introdotta possiamo ri-enunciare il teorema di Sylow come segue:

Teorema 5.153 (Teorema di Sylow per gruppi abeliani)**.** *Per ogni p che divide l'ordine di un gruppo abeliano finito $(G, *)$, esiste un p-sottogruppo di Sylow di G.*

7. Teorema di struttura per gruppi abeliani finiti

In questo paragrafo andiamo alla ricerca delle proprietà strutturali dei gruppi abeliani finiti. Dopo aver introdotto la nozione di prodotto diretto di gruppi, dimostreremo il teorema di struttura dei gruppi abeliani finiti: ogni gruppo abeliano finito è isomorfo ad un prodotto diretto di gruppi ciclici.

Siano $(G_1, *_1)$, $(G_2, *_2)$ gruppi, ci chiediamo se sia possibile *indurre* una struttura di gruppo sul prodotto cartesiano $G = G_1 \times G_2$. La risposta è affermativa e un modo è quello di definire su G l'operazione $*$ indotta da $*_1, *_2$, componente per componente, come segue:

$$\forall (x_1, x_2), (y_1, y_2) \in G \quad (x_1, x_2) * (y_1, y_2) \overbrace{=}^{def.} (x_1 *_1 y_1, x_2 *_2 y_2)$$

È facile mostrare che $(G, *)$ così definiti formano un gruppo il cui elemento neutro è $e = (e_1, e_2)$, e per ogni $(x_1, x_2) \in G$ l'inverso è dato da (x_1^{-1}, x_2^{-1}).

Definizione 5.154. Dati $(G_1, *_1)$, $(G_2, *_2)$, il gruppo $(G_1 \times G_2, *)$ con $*$ indotta da $*_1$, $*_2$ è detto gruppo **prodotto diretto** dei gruppi G_1 e G_2.

Esercizio 5.155. *Dimostrare che $G = G_1 \times G_2$ è abeliano se e solo se G_1 e G_2 sono abeliani.*

Osservazione 5.156. La costruzione del prodotto diretto di due gruppi è replicabile nel caso di n gruppi, e si può quindi generalizzare la Definizione 5.154 al prodotto diretto di n gruppi.

Se gli n G_i di cui si fa il prodotto diretto sono finiti di cardinalità c_i, allora il gruppo prodotto diretto dei G_i (essendo l'insieme di tutte le n-uple ordinate di elementi appartenenti ai G_i) avrà ordine $\prod_{i=1}^{n} c_i$.

Essendo il prodotto diretto definito componente per componente, le proprietà di questo gruppo *derivano* dalle proprietà di gruppo dei singoli *fattori*. Ad esempio, per quanto riguarda l'ordine di un elemento del prodotto diretto di gruppi finiti, si ha il seguente risultato:

Teorema 5.157. *Sia $G = G_1 \times \ldots \times G_n$ il prodotto diretto di gruppi finiti. L'ordine di un elemento $\overline{x} = (x_1, \ldots, x_n) \in G$ è il minimo comun multiplo k dell'ordine dei singoli x_i nei rispettivi gruppi:*

$$o(\overline{x}) = k = [o(x_1), \ldots, o(x_n)]$$

Dimostrazione. Per ipotesi, per ogni i esiste t_i intero con $o(x_i) \cdot t_i = k$. Mostriamo innanzitutto che $\overline{x}^k = e$, e di conseguenza che $o(\overline{x})$ divide k:

$$(x_1, \ldots, x_n)^k = (x_1^k, \ldots, x_n^k) = ((x_1^{o(x_1)})^{t_1}, \ldots, (x_n^{o(x_n)})^{t_n}) = e$$

Viceversa, per definizione di ordine, si ha:

$$e = \overline{x}^{o(\overline{x})} = (x_1^{o(\overline{x})}, \ldots, x_n^{o(\overline{x})})$$

Da cui segue che, per ogni i, $o(x_i) | o(\overline{x})$, quindi $o(\overline{x})$ è un multiplo comune degli $o(x_i)$, e perciò è un multiplo del loro minimo comun multiplo k. □

Esercizio 5.158. *Contare il numero di sottogruppi non banali del prodotto diretto $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, con p primo.*

Svolgimento. G è un gruppo per la addizione definita componente per componente, di ordine p^2: dunque i sottogruppi non banali di G hanno ordine p.

Dal Teorema 5.157 sappiamo che, per ogni $([a]_p, [b]_p)$ in G, vale:

$$o(([a]_p, [b]_p)) = [ord([a]_p), ord([b]_p)] = \begin{cases} p \text{ se } ([a]_p, [b]_p) \neq ([0]_p, [0]_p) \\ 1 \text{ se } ([a]_p, [b]_p) = ([0]_p, [0]_p) \end{cases}$$

Ci sono quindi $p^2 - 1$ elementi di ordine p ed un elemento di ordine 1. Siano ora H_1, H_2 sottogruppi non banali di G, dunque di ordine p. Consideriamo il sottogruppo $H = H_1 \cap H_2$. H ha p elementi se e solo se $H_1 = H_2$, altrimenti $|H| = 1$. Quindi ogni sottogruppo non banale di G ha $p - 1$ elementi **caratteristici**, ovvero che non stanno in nessun altro sottogruppo non banale di G. Abbiamo quindi che il numero di sottogruppi non banali distinti di G è uguale a:

$$\frac{\text{n.elementi di ordine } p}{\text{n.elementi caratteristici per ogni sottogruppo}} = \frac{p^2 - 1}{p - 1} = p + 1.$$

Ed il numero totale di sottogruppi (inclusi G stesso ed $\{e\}$) è dunque $p + 3$.

Teorema 5.159 (Teorema cinese - terza forma)**.** *Siano m, n interi maggiori di* 1*,* $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *se e solo se* $(m, n) = 1$*.*

Dimostrazione. $\Leftarrow$) Se $(m, n) = 1$ allora il Teorema 4.109 (teorema cinese - seconda forma) definisce l'applicazione bigettiva $\phi([a]_{mn}) = ([a]_m, [a]_n)$ da $\mathbb{Z}/mn\mathbb{Z}$ a $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Resta da dimostrare che ϕ è un omomorfismo, ovvero che per ogni $[a]_{mn}, [b]_{mn}$ in $\mathbb{Z}/mn\mathbb{Z}$, si ha:

$$\phi([a]_{mn} + [b]_{mn}) = \phi([a]_{mn}) + \phi([b]_{mn})$$

La verifica è un facile esercizio.
$\Rightarrow$) Viceversa se m e n non sono primi tra loro allora $(\mathbb{Z}/mn\mathbb{Z}, +)$ e $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, +)$ non possono essere isomorfi. $\mathbb{Z}/mn\mathbb{Z}$ è ciclico (generato da una qualsiasi classe $[a]_{mn}$ con $[a]_{mn}$ primo con $m \cdot n$) mentre, dal Teorema 5.157 segue che $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ non lo è. Infatti sia $([a]_m, [b]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ allora l'ordine di $([a]_m, [b]_n)$ è il minimo comun multiplo tra l'ordine di $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$ e l'ordine di $[b]_n$ in $\mathbb{Z}/n\mathbb{Z}$ e quindi è al più $o([a]_m) \cdot o([b]_n)$ (se $o([a]_m)$ e $o([b]_n)$ sono coprimi). Non essendo m e n coprimi l'ordine di un qualsiasi $([a]_m, [b]_n)$ è dunque sempre strettamente minore di $m \cdot n$, ovvero $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ non è ciclico. □

Esercizio 5.160. *Dimostrare che, per ogni m e n interi maggiori di* 1*:*

$$(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$$

Svolgimento. In questo caso non vogliamo dimostrare un isomorfismo, ma l'uguaglianza tra i due insiemi. Stiamo cioè dicendo che il sottoinsieme $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*$ degli invertibili del gruppo prodotto diretto $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è uguale al prodotto diretto tra il gruppo $\mathbb{Z}/m\mathbb{Z}^*$ degli invertibili di $\mathbb{Z}/m\mathbb{Z}$ e il gruppo $\mathbb{Z}/n\mathbb{Z}^*$ degli invertibili di $\mathbb{Z}/n\mathbb{Z}$.

Sia $([a]_m, [b]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Per definizione $([a]_m, [b]_n)$ è invertibile (cioè appartiene a $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})*$) se e solo se esistono $([c]_m, [d]_n)$ in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tali che $([a]_m, [b]_n) \cdot ([c]_m, [d]_n) = ([1]_m, [1]_n)$. Questo è possibile se e solo se $[a]_m$ è invertibile in $\mathbb{Z}/m\mathbb{Z}$ e $[b]_n$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$, ovvero $([a]_m, [b]_n) \in \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$

Osservazione 5.161. Dal Teorema 5.159 sappiamo che, se $(m, n) = 1$, $\mathbb{Z}/mn\mathbb{Z}$ è isomorfo a $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Per le proprietà degli isomorfismi questo implica (provarlo per esercizio) che gli invertibili moltiplicativi dei due gruppi sono isomorfi, cioè:

$$\mathbb{Z}/mn\mathbb{Z}^* \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*$$

Dall'uguaglianza provata nell'Esercizio 5.160, segue dunque che:

$$\mathbb{Z}/mn\mathbb{Z}^* \cong \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$$

Osserviamo che, essendo i due gruppi finiti $\mathbb{Z}/mn\mathbb{Z}^*$ e $\mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$ isomorfi (e dunque in particolare con la stessa cardinalità, perché esiste una bigezione tra i due), abbiamo come corollario immediato un risultato che abbiamo già dimostrato in maniera molto più laboriosa, ovvero che:

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n)$$

Esercizio 5.162. *Dimostrare che se q, p sono primi distinti diversi da* 2*, allora $\mathbb{Z}_{pq}^*$ non è ciclico.*

Svolgimento. Essendo p e q primi distinti, $\mathbb{Z}_{pq}^*$ ha $\phi(p)\phi(q) = (p-1)(q-1)$ elementi. D'altra parte $\mathbb{Z}_{pq}^*$ è isomorfo a $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$, dunque $\mathbb{Z}_{pq}^*$ è ciclico se e solo se lo è $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Concludiamo mostrando che nessun elemento $([a]_p, [b]_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ ha ordine $(p-1)(q-1)$.

Sappiamo che $([a]_p, [b]_q)$ ha ordine in $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ uguale al minimo comun multiplo tra l'ordine di $[a]_p$ in $\mathbb{Z}_p^*$ ($\leq p-1$ in quanto $p-1$ è l'ordine di $\mathbb{Z}_p^*$) e l'ordine di $[b]_q$ in $\mathbb{Z}_q^*$ ($\leq q-1$ in quanto $q-1$ è l'ordine di $\mathbb{Z}_q^*$). Tale minimo comun multiplo, con le condizioni scritte tra parentesi, non sarà mai uguale a $(p-1)(q-1)$, in quanto $p-1$ e $q-1$ sono entrambi pari, e dunque non primi tra loro.

Abbiamo visto, dalla terza forma del teorema cinese, a quali prodotti diretti gli $\mathbb{Z}_m$ siano isomorfi. A questo punto siamo interessati a studiare il caso generale, per capire se, e quando, un gruppo G è isomorfo ad un prodotto diretto di suoi sottogruppi normali.

Lemma 5.163. *Dati H, K sottogruppi normali di un gruppo $(G, *)$ con $H \cap K = \{e\}$, per ogni $h \in H$ e per ogni $k \in K$, si ha $hk = kh$.*

Dimostrazione. La tesi è equivalente a dimostrare che $hkh^{-1}k^{-1} = e$.

$$hkh^{-1}k^{-1} \underbrace{=}_{prop.ass.} \begin{cases} \underbrace{(hkh^{-1})}_{\in K} k^{-1} \in K \\ h \underbrace{(kh^{-1}k^{-1})}_{\in H} \in H \end{cases} \rightarrow hkh^{-1}k^{-1} \in H \cap K$$

□

Esercizio 5.164. *Siano H, K due sottogruppi finiti di un gruppo $(G, *)$ e consideriamo l'insieme:*

$$HK = \{hk | h \in H,\ k \in K\}$$

Dimostrare che se H e K sono sottogruppi normali di G, allora HK è un sottogruppo di G e calcolare l'ordine di HK in funzione di quello di H e K.

Svolgimento. Per mostrare che HK è un sottogruppo di G basta mostrare che è chiuso rispetto a $*$ (Esercizio 5.38). Siano dunque $x = h_1k_1$ e $y = h_2k_2$ con $h_i \in H$ e $k_i \in K$:

$$\begin{aligned} (h_1k_1)(h_2k_2) &\underbrace{=}_{prop.ass.} h_1(k_1h_2)k_2 \underbrace{=}_{lem.5.163} \\ = h_1(h_2k_1)k_2) &\underbrace{=}_{prop.ass.} (h_1h_2)(k_1k_2) \in HK \end{aligned}$$

Osserviamo che il passaggio nel quale si fa riferimento al Lemma 5.163, poteva essere fatto in maniera diversa senza quel risultato. Infatti sapendo che H è normale, sappiamo che $k_1H = Hk_1$ e dunque avremmo potuto scrivere $k_1h_2 = h_3k_1$, con h_3 in H, e la conclusione sarebbe sempre stata che $(h_1k_1)(h_2k_2)$ è un elemento di HK. Il lemma 5.163 sarà essenziale per il prossimo teorema, non per questo esercizio.

Il numero di elementi di HK sarà sicuramente minore o uguale di $|H| \cdot |K|$ in quanto la restrizione $*_{H \times K}$ di $*$:

$$*_{H \times K} : H \times K \rightarrow HK$$

è sicuramente surgettiva (per definizione di HK) ma non è detto sia iniettiva. Quello che vogliamo mostrare è che ogni elemento nell'immagine di $*_{H\times K}$ è contato esattamente $|H \cap K|$ volte, e dunque che:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Per far questo usiamo il Teorema 5.141 (teorema di omomorfismo di gruppi) osservando che, essendo $*_{H\times K}$ surgettiva, si ha:

$$(H \times K)/Ker\ *_{H\times K} \cong HK$$

Dimostriamo che $|Ker\ *_{H\times K}| = |H \cap K|$. Ci domandiamo quali siano gli elementi di $Ker\ *_{H\times K}$. La risposta è: le coppie (h, k) in $H \times K$ tali che $hk = e$, ovvero $k = h^{-1}$. Essendo H e K sottogruppi, questa condizione è soddisfatta se e solo se $h \in K$ e $k \in H$. Perciò gli elementi del nucleo sono le coppie (h, h^{-1}) con $h \in H \cap K$, ed essendo l'inverso di un elemento h unico, si ha:

$$|Ker\ *_{H\times K}| = |H \cap K|$$

Esercizio 5.165 (Terzo teorema di omomorfismo per gruppi)**.** *Se H e N sono sottogruppi di $(G, *)$ ed N è normale, allora $H/H \cap N$ è isomorfo a HN/N.*

Svolgimento. I quozienti considerati nella tesi dell'esercizio sono ben definiti, infatti abbiamo verificato nell'Esercizio 5.111 che $H \cap N$ è un sottogruppo normale di H, ed è ovvio che N sia un sottogruppo normale di HN (è un sottogruppo normale di G che contiene HN).

Per dimostrare l'isomorfismo, consideriamo l'omomorfismo f da H in HN/N tale che, per ogni h in H, si ha $f(h) = hN$. Osserviamo che ogni elemento di HN/N, ovvero ogni classe laterale di N in HN, è un insieme del tipo hnN, con h in H e n in N. Essendo N un gruppo (dunque chiuso per l'operazione $*$), l'insieme hnN e hN coincidono, ovvero f è surgettiva. Il nucleo di f sono gli $h \in H$ tali che $hN = N$, cioè gli $h \in H$ che appartengono anche a N. La tesi segue dal primo teorema di omomorfismo per gruppi.

Teorema 5.166. *Sia $(G, *)$ un gruppo e siano H, K due sottogruppi normali di G tali che:*

(1) $H \cap K = \{e\}$.
(2) $HK = G$.

Allora $G \cong H \times K$, cioè G è il prodotto diretto di H e K.

Dimostrazione. Dobbiamo costruire un isomorfismo da $H \times K$ a G. Consideriamo la funzione $f : H \times K \longrightarrow G$ definita da: $f(x, y) = xy$.

- f è un omomorfismo. Infatti $f[(x, y)(x', y')] = f(xx', yy') = xx'yy'$ mentre $f(x, y) \cdot f(x', y') = xyx'y'$, ma nelle ipotesi fatte $(H, K \lhd G)$ sappiamo (Lemma 5.163) che $xx'yy' = xyx'y'$.
- f è iniettivo. Infatti $Ker\ f = \{(x, y) \in H \times K | xy = e\}$ è formato da coppie per cui $x = y^{-1}$. Questo significa che x e y appartengono sia ad H che a K, infatti x sappiamo che è in H, ed essendo l'inverso di un elemento di K, x necessariamente sta anche in K (analogamente per y). Dunque $x = y = e$ che, per ipotesi, è l'unico elemento di $H \cap K$, e $Ker\ f$ è composto unicamente dalla coppia (e, e) elemento neutro del prodotto diretto $H \times K$.

- f è surgettivo. Segue dall'ipotesi che $HK = G$.

□

Esercizio 5.167. *Affinchè G sia isomorfo al prodotto diretto di n gruppi G_i è sufficiente che:*

(1) $G = G_1 G_2 \dots G_n$.
(2) *Indicato con B_i il gruppo $G_1 G_2 \dots G_i$ si abbia che:*

$$\forall i < n \quad B_i \cap G_{i+1} = \{e\} \tag{7.1}$$

Suggerimento: per dimostrarlo si proceda per induzione su n, il passo base segue dal Teorema 5.166.
A questo punto ci muoviamo verso la dimostrazione del teorema di struttura per gruppi abeliani finiti: ogni gruppo abeliano finito è isomorfo al prodotto diretto di gruppi ciclici. La strategia dimostrativa sarà suddivisa in due passi distinti:

(1) Dimostreremo che ogni gruppo abeliano finito G è prodotto diretto di sottogruppi di ordini primi tra loro e uguali ad una potenza p^k di un primo p divisore dell'ordine del gruppo.
(2) Dimostreremo che ogni gruppo abeliano finito di ordine p^k è isomorfo al prodotto diretto di gruppi ciclici.

Dal teorema di Cauchy sappiamo che se G è un gruppo abeliano di ordine $p \cdot q$ con p e q primi, esistono due sottogruppi normali H e K di G di ordine rispettivamente p e q. Un elemento di $H \cap K$ ha ordine che divide p e q e dunque deve avere ordine 1, cioè $H \cap K = \{e\}$. Dall'Esercizio 5.164 segue che HK è un sottogruppo di G di ordine $p \cdot q$, dunque uguale a G. Dal Teorema 5.166 si ha quindi:

$$G \cong H \times K$$

Ci chiediamo: è possibile generalizzare questo fatto ad un gruppo abeliano G di ordine $m \cdot n$ con m e n primi tra loro ma non necessariamente primi? La risposta è affermativa ed è l'enunciato del teorema cinese *generalizzato*.

Teorema 5.168 (Teorema cinese *generalizzato*)**.** *Sia $(G, *)$ un gruppo abeliano di ordine $m \cdot n$ con m e n primi tra loro. Allora esistono due sottogruppi G_m e G_n di G di ordine rispettivamente m e n tali che:*

$$G \cong G_m \times G_n$$

Dimostrazione. Consideriamo i due sottoinsiemi di G:

$$G_n = \{x \in G | x^n = e\} \quad G_m = \{x \in G | x^m = e\}$$

Tali insiemi sono entrambi sottogruppi normali di G, in quanto nuclei degli omomorfismi[5] ϕ_n, ϕ_m da G in G definiti come segue:

$$\phi_n(g) = g^n \quad \phi_m(g) = g^m$$

Per concludere mostriamo che G_m e G_n verificano le ipotesi del Teorema 5.166 e che hanno le cardinalità volute.

Essendo $(m, n) = 1$ sappiamo che esistono $a, b \in \mathbb{Z}$ tali che $a \cdot m + b \cdot n = 1$. In particolare per ogni $x \in G$ si ha:

$$x^1 = x^{a \cdot m + b \cdot n} = \underbrace{x^{a \cdot m}}_{y} * \underbrace{x^{b \cdot n}}_{z}$$

[5]Il fatto che queste applicazioni siano omomorfismi segue dalla commutatività di G.

Ora è facile mostrare che y e z appartengono rispettivamente a G_n e G_m e dunque che $G = G_m G_n$ (ed in particolare $|G| = |G_m G_n|$). Si ha infatti per y (analoga prova per z):

$$y^n = (x^{a \cdot m})^n = (x^a)^{m \cdot n} = e$$

L'ultima uguaglianza segue dal fatto che $m \cdot n$ è l'ordine del gruppo G. Sia ora $x \in G_m \cap G_n$, cioè $x^m = x^n = e$, allora:

$$x = x^{a \cdot m + b \cdot n} = e$$

Dal Teorema 5.166 segue appunto che:

$$G \cong G_m \times G_n$$

Ci rimane da dimostrare che $|G_m| = m$ e $|G_n| = n$. Fattorizziamo m e n in prodotto di primi che sappiamo essere distinti in quanto $(m, n) = 1$:

$$m = \prod p_i^{\alpha_i} \quad n = \prod q_j^{\beta_j}$$

Si ha dunque che G_m è il sottogruppo degli x di G tali che:

$$x^{\prod p_i^{\alpha_i}} = e$$

Se x è un elemento di G_m il suo ordine ha dunque una fattorizzazione del tipo:

$$o(x) = \prod p_i^{\alpha_i'} \quad \forall i \ \alpha_i' \leq \alpha_i$$

Dal teorema di Cauchy segue che nella fattorizzazione in primi di $|G_m|$ compaiono solo i primi p_i: infatti se il gruppo abeliano G_m avesse ordine multiplo di un primo q_j allora in G_m ci sarebbe un elemento di ordine q_j. Dunque:

$$|G_m| = \prod p_i^{\overline{\alpha_i}}$$

Ed essendo G_m sottogruppo di G:

$$\forall i \ \overline{\alpha_i} \leq \alpha_i$$

Analogamente si conclude che

$$|G_n| = \prod q_j^{\overline{\beta_i}} \quad \forall j \ \overline{\beta_j} \leq \beta_j$$

Ma avendo provato che:

$$|G_m G_n| \underbrace{=}_{G_m \cap G_n = \{e\}} |G_m| \cdot |G_n| = m \cdot n$$

si ha che:

$$\forall i, j \ \overline{\alpha_i} = \alpha_i \quad \overline{\beta_j} = \beta_j$$

E dunque:

$$|G_m| = m \quad |G_n| = n$$

□

Definizione 5.169. Sia G un gruppo, p un numero primo. Un elemento $g \in G$ si dice di p**-torsione** se esiste $n \in N$ tale che $o(g) = p^n$. Un gruppo i cui elementi siano tutti di p-torsione per un dato p si dice un p**-gruppo**.

La seguente proposizione fornisce una definizione equivalente di p-gruppo nel caso abeliano.

Proposizione 5.170. *Un gruppo finito $(G, *)$ è un p-gruppo se e solo se esiste $n \in \mathbb{N}$ tale che $|G| = p^n$.*

DIMOSTRAZIONE. $\Rightarrow$) Supponiamo $|G| = m$ e che m abbia un fattore primo q diverso da p, allora per il Teorema 5.149 esiste un elemento in G di ordine q. Questo è assurdo in quanto G è un p-gruppo (ovvero ogni elemento di G ha ordine una potenza di p). Quindi m ha come unico fattore primo p, cioè è della forma p^n.

$\Leftarrow$) Gli unici divisori dell'ordine di G (che sappiamo dal Teorema 5.91 essere gli unici ordini possibili degli elementi di G) sono potenze di p, cioè tutti gli elementi di G hanno ordine una potenza di p, che corrisponde alla definizione di p-gruppo. □

Osservazione 5.171. Anche nel caso non abeliano avremo la stessa caratterizzazione dei p-gruppi: dimostreremo infatti l'equivalente del teorema di Cauchy (il cui enunciato abbiamo usato nella precedente dimostrazione) per i gruppi non abeliani.

Esercizio 5.172. *Dimostrare che se G è un gruppo abeliano l'insieme degli elementi di p-torsione è un sottogruppo (detto* **sottogruppo di p-torsione***).*

Osservazione 5.173. Sia p un primo che divide l'ordine di un gruppo abeliano finito G. Consideriamo il sottogruppo H di p-torsione di G e il p-sottogruppo di Sylow K di G. L'ordine di K è per definizione p^m massima potenza di p che divide $|G|$, ovvero $|G| = p^m \cdot r$ con r primo con p. Dunque tutti gli elementi di K hanno ordine una potenza di p e quindi $K \subset H$. Essendo H un sottogruppo di G, il suo ordine deve dividere $|G|$ e non può contenere fattori q diversi da p, altrimenti per il teorema di Cauchy esisterebbe in H un elemento di ordine q. Perciò $|H| \leq p^m$ da cui si ha $H = K$.

Abbiamo quindi dimostrato che per G gruppo abeliano finito i concetti di sottogruppo di p-torsione e p-sottogruppo di Sylow sono equivalenti.

Sia G un gruppo abeliano finito di ordine $a = \prod_{i=1}^{s} p_i^{a_i}$. Iterando ricorsivamente il risultato del Teorema 5.168, si ha che esistono s sottogruppi $H_1, ..., H_s$ di G tali che $|H_i| = p_i^{a_i}$ e tali che:

$$G \cong H_1 \times ... \times H_s$$

Abbiamo cioè dimostrato che:

Teorema 5.174. *Ogni gruppo abeliano finito è isomorfo al prodotto diretto dei suoi p-sottogruppi di Sylow (o sottogruppi di p-torsione).*

A questo punto, per arrivare al teorema di struttura, rimane da dimostrare che ogni p-gruppo abeliano finito (come lo sono per definizione i sottogruppi di p-torsione) è isomorfo ad un prodotto diretto di gruppi ciclici. Abbiamo però bisogno di un risultato preliminare.

Lemma 5.175. *Sia $(G, *)$ un p-gruppo abeliano finito, sia p^α il massimo ordine degli elementi di G, $x \in G$ un elemento di ordine massimo e consideriamo $H =< x >$. Per ogni $y \in G$, indicando con p^β l'ordine[6] in G/H della classe laterale yH, esiste $z \in yH$ tale che l'ordine di z in G è uguale a p^β.*

DIMOSTRAZIONE. Indichiamo con p^α l'ordine di x in G, e consideriamo la proiezione π_H di G in G/H:

$$\forall y \in G \ \pi_H(y) = yH$$

[6]Attenzione ad una possibile confusione: l'ordine di yH in G/H non è la sua cardinalità come insieme, ma il minimo intero positivo a per cui $(yH)^a = H$, la classe elemento neutro in G/H.

Sappiamo che è un omomorfismo, in particolare quindi:

$$\underbrace{o(yH)}_{=p^\beta} | o(y) \leq \underbrace{o(x)}_{=p^\alpha}$$

da cui segue che $\beta \leq \alpha$. Per ipotesi $(yH)^{p^\beta} = y^{p^\beta}H = H$, cioè $y^{p^\beta} \in H$, ovvero esiste m intero tale che: $y^{p^\beta} = x^m$. Inoltre, essendo p^α l'ordine massimo del p-gruppo G, p^α è multiplo dell'ordine di ogni elemento e perció $y^{p^\alpha} = e$. Abbiamo dunque:

$$e = y^{p^\beta \cdot p^{\alpha-\beta}} = (y^{p^\beta})^{p^{\alpha-\beta}} = (x^m)^{p^{\alpha-\beta}} = x^{m \cdot p^{\alpha-\beta}}$$

Quindi $o(x) = p^\alpha | m \cdot p^{\alpha-\beta}$, da cui segue che $p^\beta | m$, ovvero che esiste un intero k tale che $m = p^\beta \cdot k$.

Consideriamo l'elemento $z = y(x^{-1})^k$: per definizione sta in yH, dunque:

$$z^{p^\beta} = \underbrace{y^{p^\beta}}_{=x^m} \underbrace{(x^{-1})^{p^\beta \cdot k}}_{=x^{-m}} = e$$

Abbiamo trovato che p^β è un multiplo dell'ordine di z e allo stesso tempo sappiamo che:

$$p^\beta = o(yH) = o(zH) | o(z)$$

Quindi p^β è proprio l'ordine di z. □

A questo punto abbiamo gli strumenti per dimostrare il teorema di struttura per gruppi abeliani finiti.

Teorema 5.176. *Ogni p-gruppo abeliano finito $(G, *)$ è isomorfo ad un prodotto diretto di gruppi ciclici. Tale prodotto è unico a meno dell'ordine (non dimostreremo l'unicità della decomposizione ma solo l'esistenza).*

Dimostrazione. Dal teorema di Cauchy sappiamo che la cardinalità di G deve essere una potenza di p (altrimenti, se fosse $p^k \cdot q$ con $(p, q) = 1$, esisterebbe un elemento x di G di ordine q e G non sarebbe un p-gruppo). Sia quindi $|G| = p^n$ e procediamo per induzione su n: se $n = 1$ sappiamo che un gruppo abeliano finito di ordine un primo p è ciclico. Supponiamo dunque la tesi vera per ogni p-gruppo abeliano finito di cardinalità uguale a $p^{n'}$ con $n' < n$ e dimostriamo che allora l'enunciato è valido per ogni gruppo abeliano di ordine p^n.
G ha ordine finito, dunque esistono x e H come nel Lemma 5.175, ed essendo $n > 1$ si ha $o(G/H) < o(G)$. G/H è sempre un p-gruppo, perciò su esso possiamo usare l'ipotesi induttiva ed avere che:

$$G/H \cong K_1 \times ... \times K_m$$

con i K_i ciclici e dunque $K_i =< y_i H >$. Associamo ad ogni K_i, l'elemento z_i di ordine in G uguale all'ordine in G/H di $y_i H$, come nel Lemma 5.175. Siano L_i i sottogruppi ciclici di G generati dagli z_i. Per concludere dobbiamo dimostrare che:

$$G \cong H \times L_1 \times ... \times L_m$$

Dall'Esercizio 5.167 sappiamo che basta verificare che G sia uguale a $HL_1 \dots L_m$ e che per ogni $i < n$ si abbia:

$$(HL_1 \dots L_i) \cap L_{i+1} = \{e\}$$

Dimostriamo separatamente questi due punti:

(1) Sia $g \in G$ e consideriamo la proiezione

$$\pi_H : G \longrightarrow G/H \cong K_1 \times ... \times K_m.$$

Sia $\pi_H(g) = \prod_{i=1}^m (y_i H)^{n_i}$ e consideriamo l'elemento $h = \prod_{i=1}^m z_i^{n_i}$ di G. Ricordiamo che, per ogni i, $z_i \in y_i H$ e perciò $\pi_H(h) = \pi_H(g)$. Quindi:

$$e = \pi_H(h)(\pi_H(g))^{-1} \underbrace{=}_{thm\ 5.118} \pi_H(h)(\pi_H(g^{-1})) \underbrace{=}_{\pi_H\ omo.} \pi_H(hg^{-1})$$

Ovvero $gh^{-1} \in Ker\ \pi_H = H$. In particolare $gh^{-1} = x^n$, ovvero $g = x^n h$, e quindi:

$$g = \underbrace{x^n}_{\in H} \prod_{i=1}^m \underbrace{z_i^{n_i}}_{\in L_i}.$$

(2) Consideriamo $g \in (HL_1 \dots L_i) \cap L_{i+1}$, allora:

$$g = x^n \cdot \prod_{j=1}^i z_j^{n_j} \quad \text{e} \quad g = z_{i+1}^{n_{i+1}}$$

Quindi:

$$\pi_H(g) = e \prod_{j=1}^i \underbrace{(y_j H)^{n_i}}_{\in K_i} = \underbrace{(y_{i+1} H)^{n_{i+1}}}_{\in K_{i+1}}$$

Osserviamo che l'intersezione tra $K_1 \dots K_i$ e K_{i+1} è $\{e\}$ in quanto G/H è il prodotto diretto dei gruppi K_j. Quindi $n_i = 0$ per ogni $i \leq n$, e questo implica che $g = e$.

□

Dal Teorema 5.176 e dal Teorema 5.148 segue:

Corollario 5.177. *Sia $(G, *)$ un p-gruppo abeliano di ordine p^n. Sono univocamente determinati degli interi $a_1, \dots, a_k$ tali che:*

(1) $\sum_{i=1}^k a_i = n$.
(2) $G \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$.

Corollario 5.178. *Il numero dei p-gruppi abeliani di ordine p^n distinti (non isomorfi), è uguale al numero di partizioni di n.*

Abbiamo dunque finalmente provato che:

Teorema 5.179. *[Teorema di struttura dei gruppi abeliani finiti] Ogni gruppo abeliano finito G è isomorfo ad un prodotto diretto di gruppi ciclici. Tale decomposizione è unica a meno dell'ordine.*

Corollario 5.180. *Il numero dei gruppi abeliani G non isomorfi di ordine $n = \prod_{i=1}^k p_i^{\alpha_i}$ (con $p_i \neq p_j$ se $i \neq j$) è uguale a $\prod_{i=1}^k p(\alpha_i)$ dove $p(\alpha_i)$ è il numero di partizioni dell'esponente α_i.*

Dimostrazione. Dato un gruppo abeliano finito G di ordine n la cui fattorizzazione in primi distinti è $n = \prod_{i=1}^k p_i^{k_i}$, G è isomorfo al prodotto diretto dei suoi p-sottogruppi di torsione H_i (con $|H_i| = p_i^{k_i}$):

$$G \cong H_1 \times \dots \times H_k$$

Dal Corollario 5.177 sappiamo che per ogni i sono univocamente determinati degli interi positivi $a_1, \ldots, a_{j_i}$ tali che:

(1) $\sum_{h=1}^{j_i} a_h = i$.
(2) $H_i \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{a_{j_i}}\mathbb{Z}$.

Da questo segue la tesi del corollario. □

Esempio 5.181. Descriviamo (a meno di isomorfismi) tutti i possibili gruppi abeliani G di ordine 16. G (che è un 2-gruppo) è isomorfo ad un prodotto diretto di gruppi ciclici, prodotto diretto il cui ordine deve essere $16 = 2^4$, ovvero G è isomorfo ad uno di questi gruppi:

(1) $\mathbb{Z}/16\mathbb{Z}$;
(2) $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
(3) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$;
(4) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
(5) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Queste 5 possibilità corrispondono alle possibili partizioni diverse di 4 (l'esponente del primo 2 per ottenere 16):

$$\begin{cases} 4 = 4 \\ 4 = 3 + 1 \\ 4 = 2 + 2 \\ 4 = 2 + 1 + 1 \\ 4 = 1 + 1 + 1 + 1 \end{cases}$$

Osserviamo che il numero di gruppi abeliani di ordine 16 distinti (a meno di isomorfismi) è uguale al numero di gruppi abeliani distinti di ordine p^4 con p primo qualsiasi, in quanto come osservato tale numero dipende solo dall'esponente 4.

Osserviamo anche che, fissando come ordine della partizione quello ottenuto con numeri decrescenti (per esempio la partizione di 12 con $2, 4, 3, 2$ e 1 scritta $12 = 4 + 3 + 2 + 2 + 1$), si ha l'unicità di scrittura.

Esempio 5.182. Vogliamo elencare (a meno di isomorfismi) tutti i gruppi abeliani G con $|G| = 2^4 \cdot 3^3 \cdot 5^2$.

Sappiamo che $G \cong H_1 \times H_2 \times H_3$, dove gli H_i sono p-gruppi (con p che varia tra $2, 3, 5$).

Studiamo dunque quanti sono e come son fatti i possibili p-gruppi H_1, H_2 e H_3 di ordine rispettivamente 2^4, 3^3, 5^2.

- Per H_1 con $|H_1| = 2^4 = 16$ abbiamo già visto (Esempio 5.181) che ci sono 5 diverse possibilità e le abbiamo elencate.
- Per H_2 con $|H_2| = 3^3$ abbiamo 3 possibilità: tante quante sono le partizioni dell'esponente 3.

  La partizione $3 = 3$ corrisponde all'isomorfismo

  $$H_2 \cong \mathbb{Z}/27\mathbb{Z}$$

  La partizione $3 = 2 + 1$ corrisponde all'isomorfismo

  $$H_2 \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

  La partizione $3 = 1 + 1 + 1$ corrisponde all'isomorfismo

  $$H_2 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

- Per H_3 con $|H_3| = 5^2$ abbiamo 2 possibilità: tante quante sono le partizioni dell'esponente 2.

  La partizione $2 = 2$ corrisponde all'isomorfismo:

$$H_3 \cong \mathbb{Z}/25\mathbb{Z}$$

  La partizione $2 = 1 + 1$ corrisponde all'isomorfismo:

$$H_3 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

I gruppi abeliani G di ordine $2^4 \cdot 3^3 \cdot 5^2$ sono dunque $5 \cdot 3 \cdot 2 = 30$ (lo sapevamo dal corollario 5.180) e si ottengono come prodotto diretto dei diversi possibili H_i descritti sopra.

Osservazione 5.183. Dato un gruppo abeliano finito G di ordine n scritto come prodotto diretto di gruppi ciclici, il corollario 5.70 e il Teorema 5.157 permettono di contare il numero di elementi di ordine d in G, per ogni divisore d di n (nel prossimo esempio faremo questo conteggio in un caso concreto).

Questo è molto interessante in quanto, se di un gruppo abeliano finito G conosciamo l'ordine n e abbiamo alcune informazioni sul numero di elementi di ordine $d_1, \ldots, d_k$ (con d_i divisori di n), possiamo identificare l'unico prodotto diretto di ciclici che ha gli stessi numeri di elementi di ordine $d_1, \ldots, d_k$.

Esempio 5.184. Consideriamo il gruppo abeliano G con 4840 elementi, dove con H_p abbiamo indicato i p-gruppi di Sylow di G:

$$G \cong \underbrace{\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}_{H_2} \times \underbrace{\mathbb{Z}/5\mathbb{Z}}_{H_5} \times \underbrace{\mathbb{Z}/121\mathbb{Z}}_{H_{11}}$$

Vogliamo contare, per ogni divisore d di 4840, il numero di elementi di ordine d. Possiamo vedere ogni elemento di G come una terna $([a]_2, [b]_5, [c]_{11})$ dove con $[x]_p$ indichiamo un elemento del p-gruppo di Sylow H_p. Il vantaggio di questa scrittura è facilmente spiegabile: l'ordine del generico $([a]_2, [b]_5, [c]_{11})$ è il minimo comun multiplo degli ordini dei singoli elementi (per il Teorema 5.157), ma essendo ogni elemento appartenente al p-gruppo H_p con p distinti tra loro, il minimo comun multiplo degli ordini è semplicemente il prodotto degli ordini.

Supponiamo di voler calcolare il numero di elementi di ordine 20 in G. Per avere un elemento di ordine $20 = 2^2 \cdot 5$ di G, $[a]_2$ deve avere ordine $4 = 2^2$, $[b]_5$ deve avere ordine 5 e $[c]_{11}$ deve avere ordine 1. A questo punto rimane da contare quanti elementi distinti dell'ordine voluto ci sono negli H_p considerati:

- Un elemento $[a]_2$ di $H_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ è una coppia (a_1, a_2) con $a_1 \in \mathbb{Z}/4\mathbb{Z}$ e $a_2 \in \mathbb{Z}/2\mathbb{Z}$. Sempre dal Teorema 5.157 segue che, per avere un elemento di ordine 4, a_1 deve avere ordine 4 e a_2 può avere un qualunque ordine. Di elementi di ordine 4 in $\mathbb{Z}_4$ ce ne sono (corollario 5.70) $\phi(4) = 2$ e a_2 lo possiamo scegliere in 2 modi (uno qualsiasi degli elementi di $\mathbb{Z}/2\mathbb{Z}$). Ci sono perciò 4 coppie (a_1, a_2) di ordine 4 in H_2.
- Di elementi di ordine 5 in H_5, che è ciclico, ce ne sono (sempre per il corollario 5.70) $\phi(5) = 4$.
- Di elementi di ordine 1 in H_{11} ce ne è 1 soltanto (l'identità).

Dunque di elementi $([a]_2, [b]_5, [c]_{11}) \in G$ di ordine 20 ce ne sono $4 \cdot 4 \cdot 1 = 16$.

Consideriamo ora un generico divisore d di 4840. I divisori di 4840 sono 24 e della forma:

$$\begin{cases} d = 2^{\alpha_1} \cdot 5^{\alpha_2} \cdot 11^{\alpha_3} \\ 0 \leq \alpha_1 \leq 3, \;\; 0 \leq \alpha_2 \leq 1, \;\; 0 \leq \alpha_3 \leq 2 \end{cases}$$

Quanti sono gli elementi di ordine d in G? Ripetendo il ragionamento fatto nel caso particolare di $d = 20$, dobbiamo contare quanti sono gli elementi $[a]_2$ di ordine 2^{α_1} in H_2, quanti sono gli elementi $[b]_5$ di ordine 5^{α_2} in H_5, quanti sono gli elementi $[c]_{11}$ di ordine 11^{α_3} in H_{11} e il numero cercato sarà il prodotto di questi tre numeri. Osserviamo che l'unico caso delicato è H_2 infatti, essendo H_5 e H_{11} ciclici, il corollario 5.70 ci dice che ci sono $\phi(5^{\alpha_2})$ elementi $[b]_5$ di H_5 di ordine 5^{α_2} e $\phi(11^{\alpha_3})$ elementi $[c]_{11}$ di H_{11} di ordine 11^{α_3}.

Studiamo dunque a parte quanti sono gli elementi $[a]_2$ di ordine 2^{α_1} in H_2. Con la notazione usata nel caso $d = 20$, ci chiediamo quali ordini t e q (potenze di 2 minori rispettivamente di 4 e 2) devono avere a_1 e a_2 in modo che $(a_1, a_2) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ abbia ordine 2^{α_1}. La risposta è tutte le coppie (t, q) tali che il minimo comun multiplo tra t e q è uguale a 2^{α_1}. A questo punto possiamo osservare che di elementi a_1 di ordine t in $\mathbb{Z}/4\mathbb{Z}$ ce ne sono $\phi(t)$ (sempre per il corollario 5.70) e di elementi a_2 di ordine q in $\mathbb{Z}/2\mathbb{Z}$ ce ne sono $\phi(q)$. Dunque di coppie (a_1, a_2) di ordini fissati rispettivamente t e q ce ne sono $\phi(t) \cdot \phi(q)$. Sommando questi numeri al variare delle possibili coppie t e q che hanno come minimo comun multiplo 2^{α_1}, troviamo il numero di elementi di H_2 di ordine 2^{α_1}.

- $\alpha_1 = 0$. Quanti sono gli elementi di H_2 di ordine $2^0 = 1$? La risposta è 1: solo l'identità di H_2 ha ordine 1 (t e q devono essere uguali a 1).
- $\alpha_1 = 1$. Cerchiamo elementi di H_2 di ordine 2. Allora per t e q abbiamo 3 possibilità:
  (1) $t = q = 2$. Il numero di elementi del tipo (a_1, a_2) con $o(a_1) = t = 2$ e $o(a_2) = q = 2$ è $\phi(2) \cdot \phi(2) = 1$.
  (2) $t = 2, q = 1$. Il numero di elementi del tipo (a_1, a_2) con $o(a_1) = t = 2$ e $o(a_2) = q = 1$ è $\phi(2) \cdot \phi(1) = 1$.
  (3) $t = 1, q = 2$. Il numero di elementi del tipo (a_1, a_2) con $o(a_1) = t = 1$ e $o(a_2) = q = 2$ è $\phi(1) \cdot \phi(2) = 1$.
  Perciò ci sono $1 + 1 + 1 = 3$ elementi di ordine 2 in H_2.
- $\alpha_1 = 2$. Cerchiamo elementi di H_2 di ordine 4. In questo caso per avere $[t, q] = 4$ deve essere $t = 4$ e q qualsiasi. Dunque abbiamo $\phi(4) = 2$ scelte per a_1 e 2 scelte (qualsiasi elemento di $\mathbb{Z}/2\mathbb{Z}$) per a_2 e quindi in totale 4 scelte.
- $\alpha_1 = 3$. Cerchiamo elementi di ordine 8 in H_2: è facile osservare che non ci sono coppie t e q (potenze di 2 minori rispettivamente di 4 e 2) con $[t, q] = 8$. Quindi ci sono 0 elementi di ordine 8 in H_2.

A questo punto sia d un divisore di 4840 e scriviamo il numero di elementi di ordine d in G a seconda dell'esponente α_1 di 2 nella fattorizzazione di d:

- Se $d = 5^{\alpha_2} \cdot 11^{\alpha_3}$ ci sono $\phi(5^{\alpha_2}) \cdot \phi(11^{\alpha_3})$ elementi di ordine d in G.
- Se $d = 2 \cdot 5^{\alpha_2} \cdot 11^{\alpha_3}$ ci sono $3 \cdot \phi(5^{\alpha_2}) \cdot \phi(11^{\alpha_3})$ elementi di ordine d in G.
- Se $d = 2^2 \cdot 5^{\alpha_2} \cdot 11^{\alpha_3}$ ci sono $4 \cdot \phi(5^{\alpha_2}) \cdot \phi(11^{\alpha_3})$ elementi di ordine d in G.
- Se $d = 2^3 \cdot 5^{\alpha_2} \cdot 11^{\alpha_3}$, allora ci sono 0 elementi di ordine d in G.

8. Automorfismi di gruppo

Abbiamo introdotto il concetto di omomorfismo tra due gruppi diversi $(G, *)$ e $(G', *')$. Particolare importanza hanno gli omomorfismi da un gruppo $(G, *)$ in sé.

Definizione 5.185. Un omomorfismo $f : G \longrightarrow G$ da un gruppo in se stesso si dice **un endomorfismo**. Se f è un endomorfismo bigettivo allora f è detto un **automorfismo**. Indicheremo con $Aut(G)$ l'insieme degli automorfismi di G.

Esercizio 5.186. *Dimostrare che l'insieme degli endomorfismi di un gruppo $(G, *)$ è un monoide.*

Proposizione 5.187. *$(Aut(G), \circ)$ è un gruppo.*

Dimostrazione. La conclusione è una conseguenza degli esercizi 5.117 e 5.139. □

Esempio 5.188. Studiamo da quali omomorfismi è composto il gruppo $Aut(\mathbb{Z})$. Essendo $\mathbb{Z}$ un gruppo ciclico generato da 1, sappiamo che un qualsiasi omomorfismo f definito su $\mathbb{Z}$ (Proposizione 5.119) è univocamente determinato una volta stabilito il valore k di $f(1)$. Infatti, scelto $k = f(1)$, si ha che, per ogni z in $\mathbb{Z}$, l'immagine di z tramite f è $f(z) = k \cdot z$. Viceversa, per ogni $k \in \mathbb{Z}$ la funzione $f_k : \mathbb{Z} \longrightarrow \mathbb{Z}$ che ad ogni intero z associa $k \cdot z$ è un omomorfismo, infatti:

$$f_k(x + y) = k \cdot (x + y) = k \cdot x + k \cdot y = f_k(x) + f_k(y)$$

Quindi l'insieme degli endomorfismi di $\mathbb{Z}$ è composto da tutte e sole le funzioni del tipo $f_k(z) = k \cdot z$ al variare di k in $\mathbb{Z}$.

Per capire quali tra questi siano automorfismi bisogna studiare l'iniettività e la surgettività degli omomorfismi f_k. Riguardo all'iniettività è facile osservare che:

$$Ker\ f_k = \begin{cases} k = 0 \rightarrow Ker\ f_0 = \mathbb{Z} \\ k \neq 0 \rightarrow Ker\ f_k = \{0\} \end{cases}$$

Perciò se $k \neq 0$, f_k è iniettiva. Dobbiamo studiare per quali $k \in \mathbb{Z} \setminus \{0\}$, f_k è surgettivo. Dal corollario 5.124 segue che f_k è surgettivo se e solo se $f_k(\mathbb{Z}) \supset \{1\}$, o equivalentemente se $1 \in Im(f_k)$. Perciò deve esistere $x \in \mathbb{Z}$ tale che:

$$f_k(x) = k \cdot x = 1 \leftrightarrow \begin{array}{c} x = k = 1 \\ x = k = -1 \end{array}$$

Concludendo $Aut(\mathbb{Z})$ è un insieme composto da due elementi: l'identità f_1 e l'isomorfismo f_{-1} che ad ogni $z \in \mathbb{Z}$ fa corrispondere $-z$.

Teorema 5.189. *Il gruppo $(Aut(\mathbb{Z}/m\mathbb{Z}), \circ)$ è isomorfo a $\mathbb{Z}/m\mathbb{Z}^*$.*

Dimostrazione. Sappiamo come sono fatti gli $Aut(\mathbb{Z}/m\mathbb{Z})$ (Esercizio 5.137): f_k è in $Aut(\mathbb{Z}/m\mathbb{Z})$ se e solo se $f_k([1]_m) = [k]_m$ con $(k, m) = 1$. Questo, da una parte implica che $|Aut(\mathbb{Z}/m\mathbb{Z})| = \phi(m)$, dall'altra fornisce l'idea per definire un isomorfismo da $(Aut(\mathbb{Z}/m\mathbb{Z}), \circ)$ a $\mathbb{Z}/m\mathbb{Z}^*$. Consideriamo infatti la funzione:

$$\begin{array}{l} \varphi : Aut(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathbb{Z}/m\mathbb{Z}^* \\ \varphi(f_k) = [k]_m \end{array}$$

È facile provare che φ è un isomorfismo. □

Proposizione 5.190. *Sia $(G, *)$ un gruppo e $g \in G$, la funzione φ_g da G in sé, definita da $\varphi_g(x) = gxg^{-1}$ per ogni x in G, è un automorfismo di G.*

DIMOSTRAZIONE. Per ogni $x, y \in G$ si ha:

$$\varphi_g(xy) = g(xy)g^{-1} = g(xey)g^{-1} = g(xg^{-1}gy)g^{-1} = \varphi_g(x)\varphi_g(y)$$

dunque φ_g è un omomorfismo.

Il nucleo di φ_g è composto dagli $x \in G$ tali che $gxg^{-1} = e$, ovvero $x = g^{-1}eg$, da cui $x = e$. Dunque $Ker\ \varphi_g$ è composto da un solo elemento, e φ_g è iniettiva.

Infine φ_g è surgettiva in quanto, per ogni $y \in G$, se consideriamo l'elemento $x = g^{-1}yg$ di G si ha:

$$\varphi_g(x) = gg^{-1}ygg^{-1} = y$$

□

Proposizione 5.191. *La funzione $\lambda : G \longrightarrow Aut(G)$, definita da: $\lambda(g) = \varphi_g$, dove φ_g è l'automorfismo introdotto nella Proposizione 5.190, è un omomorfismo di gruppi.*

DIMOSTRAZIONE. Dobbiamo mostrare che $\lambda(gh) = \lambda(g) \circ \lambda(h)$, ovvero che $\varphi_{gh} = \varphi_g \circ \varphi_h$:

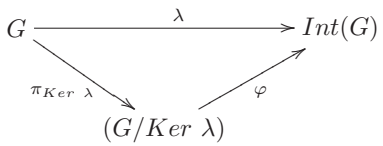
$$\forall x \in G\ \varphi_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = \varphi_g(hxh^{-1}) = (\varphi_g \circ \varphi_h)(x)$$

□

Corollario 5.192. *L'immagine $\lambda(G)$ di G tramite l'omomorfismo λ introdotto nella Proposizione 5.191 è un sottogruppo di $Aut(G)$, detto sottogruppo degli* **automorfismi interni** *di G (lo indicheremo con $Int(G)$).*

Osservazione 5.193. Se G è abeliano $Int(G) = \{id\}$.

Osservazione 5.194. Consideriamo il seguente diagramma:



Il teorema di omomorfismo di gruppi ci dice che φ è un isomorfismo, in quanto λ è surgettivo. È interessante dunque caratterizzare il nucleo di λ:

$$Ker\ \lambda = \{g \in G | \lambda(g) = \varphi_g = \text{funzione identità}\}$$

Cioè $g \in Ker\ \lambda$ se e solo se per ogni $x \in G$ si ha $\varphi_g(x) = gxg^{-1} = x$, ovvero $gx = xg$. $Ker\ \lambda$ è dunque costituito dagli elementi di G che commutano con ogni elemento di G, ovvero $Z(G)$. Si ha dunque:

$$G/Z(G) \cong Int(G)$$

Descrivendo il centro $Z(G)$ come nucleo di un omomorfismo, dalla Proposizione 5.129 segue che $Z(G)$ è normale, risultato che avevamo già dimostrato, ma a partire dalla definizione di sottogruppo normale, nell'Esercizio 5.101.

Esercizio 5.195. *Ogni sottogruppo H di G contenuto in $Z(G)$ è normale in G.*

Proposizione 5.196. *Sia $Z(G)$ il centro di un gruppo G. Sono fatti equivalenti:*

(1) $Z(G) = G$.

(2) $G/Z(G)$ *è ciclico.*
(3) G *è abeliano.*

DIMOSTRAZIONE. (1) $\Rightarrow$ (2) Se $Z(G) = G$, allora $G/Z(G)$ è il gruppo banale costituito dalla sola classe laterale $Z(G)$, ed è quindi ciclico.
(2) $\Rightarrow$ (3) Per ipotesi esiste un elemento $g \in G$ tale che $G/Z(G) =< gZ(G) >$. Questo implica che per ogni $x, y \in G$ si ha $xy = yx$. Infatti, essendo $gZ(G)$ un generatore di $G/Z(G)$, esistono a e b interi tali che:

$$\begin{array}{ll} xZ(G) = (gZ(G))^a & x \in g^a Z(G) \\ yZ(G) = (gZ(G))^b \quad \leftrightarrow & y \in g^b Z(G) \end{array}$$

Esistono dunque $h, k \in Z(G)$ tali che $x = g^a h$ e $y = g^b k$. Perciò:

$$xy = g^a h g^b k \underbrace{=}_{h \in Z(G)} g^a g^b h k \underbrace{=}_{k \in Z(G)} g^b g^a k h \underbrace{=}_{k \in Z(G)} g^b k g^a h = yx$$

(3) $\Rightarrow$ (1) È immediato per definizione di $Z(G)$. □

Corollario 5.197. *Se $(G, *)$ non è abeliano, allora $Int(G)$ non è ciclico (equivalentemente $Int(G)$ è ciclico se e solo se è uguale al sottogruppo banale $\{id\}$).*

DIMOSTRAZIONE. Dalla Proposizione 5.196 sappiamo che, se G non è abeliano, allora $G/Z(G)$ non è ciclico. La tesi segue dall'isomorfismo $G/Z(G) \cong Int(G)$. □

Esercizio 5.198. *Sia $(G, *)$ un gruppo, dimostrare che ogni sottogruppo normale H di G di ordine 2 è un sottogruppo di $Z(G)$.*

Svolgimento. $H = \{e, h\}$ e, per ogni $g \in G$, $gH = Hg$ (H è normale). A questo punto elenchiamo i due elementi delle due classi laterali in questione $gH = \{g, gh\}$, $Hg = \{g, hg\}$. Dovendo coincidere le due classi, deve essere $gh = hg$, cioè $h \in Z(G)$. Quindi $H < Z(G)$.

Definizione 5.199. Un sottogruppo K di un gruppo $(G, *)$ si dice **caratteristico** in G se per ogni $\varphi \in Aut(G)$ si ha $\varphi(K) = K$.

Osservazione 5.200. Un sottogruppo caratteristico K di un gruppo $(G, *)$ è normale in G, infatti per ogni g in G, considerando l'automorfismo interno φ_g, la definizione di gruppo caratteristico ci dice che $\varphi_g(K) = gKg^{-1}$ è uguale a K.

Osserviamo inoltre che, per verificare che un sottogruppo K di un gruppo $(G, *)$ è caratteristico, basta provare che per ogni $\varphi \in Aut(G)$ vale $\varphi(K) \subseteq K$. Infatti, essendo ogni φ in $Aut(G)$ invertibile, dalla relazione precedente si ha che, per ogni φ in $Aut(G)$, $K \subset \varphi^{-1}(K)$.

Esercizio 5.201. *I sottogruppi G, $\{e\}$, $[G, G]$ e $Z(G)$ sono caratteristici qualsiasi sia il gruppo $(G, *)$.*

Svolgimento. Mostriamo ad esempio che $Z(G)$ è caratteristico, ovvero che, per ogni $\tau \in Aut(G)$ e per ogni $x \in Z(G)$, $\tau(x) \in Z(G)$. Cioè per ogni g in G vogliamo che valga:

$$\forall g \in G \; g\tau(x) = \tau(x)g$$

τ è surgettivo, quindi per ogni $g \in G$ esiste $y \in G$ tale che $\tau(y) = g$. Dunque:

$$g\tau(x) = \tau(y)\tau(x) \underbrace{=}_{\tau \text{ omo.}} \tau(yx) \underbrace{=}_{x \in Z(G)} \tau(xy) = \tau(x)\tau(y) = \tau(x)g$$

In particolare, come corollario di questo esercizio, abbiamo che i 4 sottogruppi sono normali: risultato che conoscevano già per ognuno dei 4, e che avevamo dimostrato usando altre strade.

Esercizio 5.202. *Sia $(G, *)$ un gruppo finito e H, K sottogruppi di G. Se $G \cong H \times K$ e $|H| = n$, $|K| = m$ con $(m, n) = 1$, allora H e K sono caratteristici.*

Svolgimento. Possiamo mostrare che, per ogni $\tau \in Aut(G)$, $\tau(H \times \{e\}) \subseteq H \times \{e\}$ e che $\tau(\{e\} \times K) \subseteq \{e\} \times K$. La prova dei due contenimenti è essenzialmente la stessa, dunque ne mostriamo solo una. Sia $h \in H$ e $\tau(h, e) = (x, y)$. L'ordine di (h, e) è il minimo comun multiplo $[o(h), o(e)]$, ovvero $o(h)$, mentre l'ordine di (x, y) è il minimo comun multiplo $[o(x), o(y)]$. Essendo $\tau \in Aut(G)$, in particolare è iniettivo, perciò (Teorema 5.136) $o(h) = [o(x), o(y)]$.

In particolare $o(y)$ divide $o(h)$, e quindi è un divisore di n, ma essendo y un elemento di K, $o(y)$ deve dividere anche m. L'unico divisore comune di m e n è per ipotesi 1, quindi $o(y) = 1$, ovvero $y = e$.

Esercizio 5.203. *Sia $G = H \times K$, determinare sotto quali ipotesi:*

$$Aut(H \times K) \cong Aut(H) \times Aut(K)$$

Svolgimento. Per trovare le condizioni affinchè valga l'isomorfismo, consideriamo l'applicazione ϕ da $Aut(H) \times Aut(K)$ in $Aut(H \times K)$, definita da:

$$\phi((\varphi, \psi)) = \varphi \times \psi$$

Dove $\varphi \times \psi$ è l'automorfismo di $H \times K$ che ad ogni coppia (h, k) di $H \times K$ associa la coppia:

$$\varphi \times \psi(h, k) = (\varphi(h), \psi(k)) \in H \times K$$

Verifichiamo che la definizione di ϕ data è una buona definizione, ovvero che $\varphi \times \psi$ è un automorfismo di $H \times K$:

- $\varphi \times \psi$ è un omomorfismo:

  $\varphi \times \psi[(h_1, k_1)(h_2, k_2)] = \varphi \times \psi(h_1 h_2, k_1 k_2) = (\varphi(h_1 h_2), \psi(k_1 k_2))$

  ed essendo φ e ψ omomorfismi:

  $$(\varphi(h_1 h_2), \psi(k_1 k_2)) = (\varphi(h_1)\varphi(h_2), \psi(k_1)\psi(k_2))$$
  $$(\varphi(h_1)\varphi(h_2), \psi(k_1)\psi(k_2)) = (\varphi(h_1), \psi(k_1))(\varphi(h_2), \psi(k_2))$$

  Ovvero:

  $$\varphi \times \psi[(h_1, k_1)(h_2, k_2)] = (\varphi \times \psi(h_1, k_1)) \cdot (\varphi \times \psi(h_2, k_2))$$

- $\varphi \times \psi$ è iniettivo: cerchiamone il nucleo, ovvero le coppie (h, k) tali che $\varphi \times \psi(h, k) = (e_H, e_K)$:

  $$(\varphi(h), \psi(k)) = (e_H, e_K) \Leftrightarrow \begin{cases} \varphi(h) = e_H \\ \psi(k) = e_K \end{cases} \underbrace{\Leftrightarrow}_{\varphi, \psi \text{ iniettive}} \begin{cases} h = e_H \\ k = e_K \end{cases}$$

- $\varphi \times \psi$ è surgettivo: per ogni $h \in H$ e per ogni $k \in K$ esistono $x \in H$ e $y \in K$ tali che:

  $$\varphi(x) = h \text{ e } \psi(y) = k$$

  in quanto φ e ψ sono automorfismi rispettivamente di H e K. Perciò $\varphi \times \psi$ è surgettivo.

Dimostrato che ϕ è ben definito, verifichiamo che è un omomorfismo. Siano (φ, ψ) e (f, g) in $Aut(H) \times Aut(K)$:

$$\phi[(\varphi, \psi) \circ (f, g)] = \phi(\varphi \circ f, \psi \circ g) = (\varphi \circ f) \times (\psi \circ g)$$

mentre

$$\phi(\varphi, \psi) \circ \phi(f, g) = (\varphi \times \psi) \circ (f \times g)$$

Dobbiamo mostrare che per ogni coppia $(h, k) \in H \times K$ si ha la stessa immagine:

$$(\varphi \circ f) \times (\psi \circ g)(h, k) = (\varphi(f(h)), \psi(g(k)))$$
$$(\varphi \times \psi) \circ (f \times g)(h, k) = (\varphi \times \psi)(f(h), g(k)) = (\varphi(f(h)), \psi(g(k)))$$

Il nucleo di ϕ è:

$$Ker\ \phi = \{(\varphi, \psi) \in Aut(H) \times Aut(K) | \varphi \times \psi = id_{H \times K}\}$$

Supponiamo che (φ, ψ) sia un elemento di $Ker\ \phi$, quindi che per ogni coppia (h, k) in $H \times K$ si abbia:

$$(\varphi, \psi)(h, k) = (h, k) \Rightarrow \begin{cases} \forall h \in H\ \varphi(h) = h \\ \forall k \in K\ \psi(k) = k \end{cases} \Rightarrow \begin{cases} \varphi = id_H \\ \psi = id_K \end{cases}$$

L'omomorfismo ϕ è quindi sempre iniettivo, il seguente teorema, fornendo le condizioni sotto le quali ϕ è surgettivo, conclude l'esercizio.

Teorema 5.204. *ϕ è un isomorfismo se e solo se H e K sono sottogruppi caratteristici di $G = H \times K$.*

Dimostrazione. $\Rightarrow$) Mostriamo, come nell'Esercizio 5.202, che $H \times \{e_K\}$ è caratteristico. Se ϕ è un isomorfismo, allora per ogni $f \in Aut(H \times K)$ esiste $(\varphi, \psi) \in Aut(H) \times Aut(K)$ tale che $\varphi \times \psi = f$. Perciò:

$$f(H \times \{e_K\}) = \varphi \times \psi(H \times \{e_K\}) = (\varphi(H), \psi(\{e_K\})) = H \times \{e_K\}$$

$\Leftarrow$) Dimostriamo che per ogni τ automorfismo di $H \times K$ esistono $\tau_1 \in Aut(H)$ e $\tau_2 \in Aut(K)$ tali che:

$$\tau = \tau_1 \times \tau_2$$

Per ipotesi H e K sono caratteristici, perciò esistono $h_1 \in H$ e $k_1 \in K$ tali che:

$$\begin{cases} \tau(h, e_K) = (h_1, e_K) \\ \tau(e_H, k) = (e_H, k_1) \end{cases}$$

Se con π_H e π_K indichiamo la proiezione canonica rispettivamente su H e K, possiamo definire per ogni $h \in H$ e $k \in K$:

$$\tau_1(h) = \pi_H(\tau(h, e_K)) \text{ e } \tau_2(k) = \pi_K(\tau(e_H, k))$$

Per concludere basta mostrare che τ e $\tau_1 \times \tau_2$ sono lo stesso automorfismo di $H \times K$:

$$\tau(h, k) = \tau[(h, e_K)(e_H, k)] = \tau(h, e_K)\tau(e_H, k)$$

e per definizione di τ_1 e τ_2:

$$\tau(h, k) = (\tau_1(h), e_K)(e_H, \tau_2(k)) = (\tau_1(h), \tau_2(k))$$

ovvero:

$$\tau(h, k) = \tau_1 \times \tau_2(h, k)$$

□

Esercizio 5.205. *Tutti i sottogruppi di un gruppo ciclico G sono caratteristici.*

Svolgimento. Sappiamo che tutti i gruppi ciclici sono isomorfi a $\mathbb{Z}$ o a $\mathbb{Z}/m\mathbb{Z}$, quindi distinguiamo questi due casi:

(1) $G \cong \mathbb{Z}/m\mathbb{Z}$. Sia $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ un automorfismo e H un sottogruppo di $\mathbb{Z}/m\mathbb{Z}$. $\varphi(H) = H'$ ha la stessa cardinalità di H ed è un sottogruppo di $\mathbb{Z}/m\mathbb{Z}$, allora $H = H'$.
(2) $G \cong \mathbb{Z}$. $Aut(\mathbb{Z}) = \{id, -id\}$ e $-id(m\mathbb{Z}) = -m\mathbb{Z} = m\mathbb{Z}$ e quindi i sottogruppi di $\mathbb{Z}$ che sono tutti della forma $m\mathbb{Z}$ sono invarianti per ogni automorfismo di $\mathbb{Z}$.

Esercizio 5.206. *Siano $(G, *)$ un gruppo e T un sottogruppo normale e ciclico. Allora $H < T$ implica $H \lhd G$.*

Svolgimento. Per l'Esercizio 5.205 sappiamo che H è caratteristico in T. Dobbiamo mostrare che per ogni $\varphi \in Int(G)$, si ha: $\varphi(H) = H$.

$$T \lhd G \Rightarrow \varphi(T) = T \Rightarrow \varphi|_T(T) = T \quad \text{e } \varphi|_T \in Aut(T)$$

Quindi per l'osservazione iniziale $\varphi|_T(H) \underbrace{=}_{T \supset H} \varphi(H) = H$.

9. Azione di un gruppo su un insieme

Siano G un gruppo e X un insieme. Ricordiamo che con $S(X)$ indichiamo l'insieme delle funzioni da X in X bigettive.

Definizione 5.207. Un omomorfismo $\varphi : G \longrightarrow S(X)$ si dice **azione del gruppo G sull'insieme X.**

Notazione: indicheremo con φ_g l'elemento $\varphi(g) \in S(X)$.

Esempio 5.208. Consideriamo il gruppo $(G, \circ)$ composto dalle isometrie del piano. L'identità da G a $S(\mathbb{R}^2)$ è un'azione di G su $\mathbb{R}^2$.

Definizione 5.209. Data φ azione di G su X, e fissato $x \in X$, si dice **stabilizzatore di** x il sottoinsieme di G:

$$St(x) = \{g \in G | \varphi_g(x) = x\}$$

Si dice **orbita di** x il sottoinsieme di X:

$$Orb(x) = \{y \in X | \exists g \in G : \varphi_g(x) = y\}$$

Esempio 5.210. Sia $X = \mathbb{R}^2$, e G il gruppo delle rotazioni intorno all'origine. Consideriamo l'identità come azione di G su X. Allora:

- se $x = (0, 0)$, allora $St(x) = G$ e $Orb(x) = (0, 0)$,
- se $x \neq (0, 0)$, allora $St(x)$ contiene la solo identità (una rotazione ha come unico punto fisso il centro, in questo caso l'origine di $\mathbb{R}^2$), e $Orb(x)$ è l'insieme dei punti del piano che stanno sulla circonferenza di centro l'origine e raggio la distanza di x dall'origine.

Proposizione 5.211. *Siano $(G, *)$ un gruppo, X un insieme e φ un'azione di G su X, allora per ogni $x \in G$: $St(x) < G$.*

DIMOSTRAZIONE. Essendo φ un omomorfismo, φ_e (dove con e indichiamo l'elemento neutro di G) è l'identità di $S(X)$. Dunque $e \in St(x)$, e $St(x)$ è non vuoto.

Supponiamo $g, h \in St(x)$ e mostriamo che $g * h^{-1} \in St(x)$. Consideriamo dunque $\varphi_{g*h^{-1}}$, per ogni x in G si ha:

$$\varphi_{g*h^{-1}}(x) \underbrace{=}_{\varphi \text{ omo.}} \varphi_g \circ {\varphi_h}^{-1}(x) \underbrace{=}_{h \in St(x)} \varphi_g(x) \underbrace{=}_{g \in St(x)} x$$

□

Esercizio 5.212. *Dimostrare che, in generale, $St(x)$ non è un sottogruppo normale di G.*

Proposizione 5.213. *Siano $(G, *)$ un gruppo, X un insieme e φ un'azione di G su X, allora la relazione su X definita da $x \sim y$ se e solo se $y \in Orb(x)$ è di equivalenza.*

DIMOSTRAZIONE. **Riflessività**: $\varphi_e(x) = x$, quindi $x \in Orb(x)$, cioè per definizione $x \sim x$.
Simmetria: supponiamo $x \sim y$, cioè esiste $g \in G$ tale che $\varphi_g(x) = y$, allora $x = \varphi_g^{-1}(y) = \varphi_{g^{-1}}(y)$. Quindi $x \in Orb(y)$, ovvero $y \sim x$.
Transitività: supponiamo $x \sim y$ e $y \sim z$, cioè esistono $g, h \in G$ tali che $\varphi_g(x) = y$ e $\varphi_h(y) = z$. Allora $z = \varphi_h(\varphi_g(x)) = \varphi_{hg}(x)$, cioè $x \sim z$. □

Corollario 5.214. *Le orbite dell'azione φ di un gruppo $(G, *)$ su un insieme X formano una partizione di X.*

Proposizione 5.215. *Siano $(G, *)$ un gruppo, X un insieme e φ un'azione di G su X, allora $\varphi_g(x) = \varphi_h(x)$ se e solo se $gSt(x) = hSt(x)$.*

DIMOSTRAZIONE. La proposizione afferma che le bigezioni corrispondenti a due elementi g, h di G tramite l'azione φ coincidono su un elemento x di X se e solo se sono uguali le corrispondenti classi laterali sinistre dello stabilizzatore di x.

Mostriamo il teorema con una catena di doppie implicazioni. Osserviamo che $\varphi_g(x) = \varphi_h(x)$ se e solo se $\varphi_{h^{-1}g}(x) = x$ (Proposizione 5.26, *moltiplicando* a sinistra per $\varphi_{h^{-1}}$). Quindi $\varphi_g(x) = \varphi_h(x)$ è equivalente al fatto che $h^{-1}g \in St(x)$, che a sua volta equivale a dire che $g \in hSt(x)$, ovvero $gSt(x) = hSt(x)$. □

Corollario 5.216. *Le classi laterali sinistre di $St(x)$ sono in corrispondenza biunivoca con $Orb(x)$. In particolare, se $G < \infty$, per ogni x in X vale:*

$$|St(x)| \cdot |Orb(x)| = |G|$$

Esercizio 5.217. *Consideriamo l'azione λ del gruppo D_4 (vedi Esempio 5.15) sull'insieme D_4, che ad ogni g di D_4 associa φ_g. Il gruppo diedrale delle isometrie del piano che mandano il quadrato in sé ha i seguenti 8 elementi:*

$$D_4 = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\}$$

dove x è la rotazione di 90 gradi, mentre y è la simmetria rispetto ad un asse del quadrato. Determinare stabilizzatore e orbita di x e y.

Svolgimento. Il centro di D_4 è formato dai due elementi e ed x^2. Dunque, per quello che abbiamo osservato $St(x) \supseteq \{e, x, x^2, x^3\}$.

D'altra parte, essendo $St(x)$ un sottogruppo di D_4 ha ordine che divide 8, inoltre $x \notin Z(D_4)$ dunque $St(x) \neq D_4$. Da questo si può concludere che $St(x) = \{e, x, x^2, x^3\}$.

Questo implica (Corollario 5.216) che $|Orb(x)| = 2$, in particolare:

$$x \circ x \circ x^{-1} = x \in Orb(x)$$
$$y \circ x \circ y^{-1} = x^{-1} \circ y \circ y^{-1} = x^{-1} = x^3 \in Orb(x)$$

Perciò $Orb(x) = \{x, x^3\}$.
Anche per y lo stabilizzatore non può essere tutto D_4, in quanto $y \notin Z(D_4)$, inoltre $St(y) \supseteq < y, Z(D_4) >= \{y, e, x^2, x^2y\}$. Dunque, analogamente al caso di x, $St(y) = \{y, e, x^2, x^2y\}$. Anche in questo caso $|Orb(y)| = 2$, ed in particolare:

$$y \circ y \circ y^{-1} = y \in Orb(y)$$
$$x \circ y \circ x^{-1} = x^2 \circ y \in Orb(y)$$

Quindi $Orb(y) = \{y, x^2y\}$.

Esercizio 5.218. *Trovare stabilizzatore e orbita di tutti gli elementi di D_4.*

Esempio 5.219 (Il coniugio nei gruppi)**.** Sappiamo già che se $(G, *)$ è un gruppo e $g \in G$, l'applicazione $\varphi_g : G \longrightarrow G$ che ad ogni x di G associa gxg^{-1} è un automorfismo interno di G. Possiamo dunque considerare l'azione λ del gruppo G sull'*insieme* G che ad ogni g di G associa φ_g.

Cerchiamo di determinare l'orbita di un elemento $x \in G$, secondo l'azione che associa a $g \in G$ l'automorfismo interno φ_g:

$$Orb(x) = \{y \in G | \exists g \in G \;\; \varphi_g(x) = y\} = \{y \in G | \exists g \in G \;\; gxg^{-1} = y\}$$

Dalla Proposizione 5.213, sappiamo che la relazione in G:

$$x \sim y \Leftrightarrow \exists g \in G \;\; y = gxg^{-1}$$

è di equivalenza. La relazione appena introdotta si chiama **coniugio**, e due elementi equivalenti secondo il coniugio si dicono **coniugati**. Possiamo dunque dire che l'orbita di un elemento $x \in G$, secondo l'azione che associa a g l'automorfismo interno φ_g, è la classe di equivalenza di x per la relazione di coniugio.

Lo stabilizzatore $St(x)$, invece, è formato dai g in G tali che $\varphi_g(x) = x$, ovvero $gxg^{-1} = x$, cioè $St(x)$ contiene tutti e soli gli elementi g di G che commutano con x (tali che $gx = xg$). L'insieme $C(x)$ degli elementi di un gruppo che commutano con l'elemento x del gruppo è detto **centralizzatore** di x.

$St(x)$ è un sottogruppo di G che, in questo caso specifico (in cui l'insieme X coincide con il gruppo G) contiene sempre x e (per come è definita l'azione di coniugio) $Z(G)$. Dunque $St(x)$ contiene il sottogruppo generato da x e $Z(G)$.

Inoltre, se consideriamo $x \in Z(G)$ si ha, per definizione di $Z(G)$, che lo $St(x)$ è tutto G. Viceversa, se $x \notin Z(G)$, allora esiste un elemento g di G che non commuta con x, e dunque $St(x)$ è contenuto strettamente in G.

Possiamo enunciare il Corollario 5.216 nel caso specifico del coniugio, affermando che, se $(G, *)$ è un gruppo finito, allora per ogni x in G la cardinalità della classe di coniugio $Orb(x)$ è uguale all'indice di $C(x)$ in G, ovvero:

$$|Orb(x)| = [G : \underbrace{C(x)}_{St(x)}] = \frac{|G|}{|C(x)|}$$

Esercizio 5.220. *Siano G un gruppo finito di ordine $n > 1$ e p il più piccolo primo che divide n. Sia H un sottogruppo normale di G di ordine p. Dimostrare che H è contenuto nel centro di G.*

Svolgimento. Mostriamo che, per ogni elemento x di H, l'orbita di x rispetto al coniugio è di un solo elemento, ovvero $x \in Z(G)$. Intanto osserviamo che essendo H ciclico di ordine p, $Aut(H) \cong \mathbb{Z}_p^*$ (Teorema 5.189). Inoltre, essendo H un sottogruppo normale di G, se indichiamo con $\varphi_{y_{|_H}}$ la restrizione di φ_y ad H, per ogni y in G si ha $yxy^{-1} \in H$, ovvero $\varphi_{y_{|_H}} \in Aut(H)$. Questo equivale a::

$$o(\varphi_{y_{|_H}})|p-1 \Rightarrow o(\varphi_{y_{|_H}}) = 1 \Rightarrow \varphi_{y_{|_H}} = id.$$

10. Formula delle classi e sue conseguenze

Essendo la relazione di coniugio su un gruppo $(G, *)$ (introdotta nell'Esempio 5.219) di equivalenza, sappiamo che le classi di equivalenza rispetto a questa relazione (dette anche **classi di coniugio**) formano una partizione di G e possono essere viste come le orbite degli elementi di G. Dunque scelto un insieme R di rappresentanti per $\sim$ si ha:

$$|G| = \sum_{x \in R} |Orb(x)| = \sum_{x \in R} [G : C(x)]$$

Teorema 5.221 (Formula delle classi)**.** *Siano G un gruppo finito e R un insieme di rappresentanti per il coniugio, si ha:*

$$|G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} [G : C(x)]$$

Dimostrazione. Abbiamo già osservato che nel caso x appartenga a $Z(G)$ si ha $C(x) = G$, dunque:

$$|Orb(x)| = [G : C(x)] = 1$$

□

Dalla formula delle classi seguono alcuni risultati interessanti sui gruppi $(G, *)$ di ordine una potenza di un primo e soprattutto la generalizzazione del teorema di Cauchy, ovvero senza l'ipotesi che il gruppo preso in considerazione sia abeliano.

Proposizione 5.222. *Sia G un gruppo con $|G| = p^n$, allora $|Z(G)|$ è un multiplo non nullo di p. In particolare $Z(G)$ non è banale, ovvero $Z(G) \neq \{e\}$.*

Dimostrazione. Dalla formula delle classi e dall'ipotesi sulla cardinalità di G si ha:

$$|G| = p^n = |Z(G)| + \sum_{x \in R \setminus Z(G)} [G : C(x)]$$

Osserviamo che, se x non è un elemento di $Z(G)$, allora esiste almeno un elemento h di G con cui x non commuta e dunque $C(x)$ è un sottogruppo proprio di G. Dal teorema di Lagrange sappiamo che $|C(x)|$ divide $|G|$, dunque esiste n_x (che dipende da x) minore di n (perché $C(x)$ è sottogruppo proprio) tale che $|C(x)| = p^{n_x}$. Si ha dunque:

$$p^n = |Z(G)| + \sum_{x \in R \setminus Z(G)} p^{n-n_x}$$

Ovvero

$$|Z(G)| = p^n - \sum_{x \in R \setminus Z(G)} p^{n-n_x} = p^{\overbrace{n - n_x}^{>0}}(p^{n_x} + \sum_{x \in R \setminus Z(G)} 1)$$

□

Esercizio 5.223. *Dimostrare che un gruppo G di ordine p^2 è abeliano.*

Svolgimento. Dalla Proposizione 5.222 sappiamo che $Z(G)$ può avere cardinalità p o p^2. Vogliamo escludere il caso $|Z(G)| = p$ per avere che $|Z(G)| = |G|$, dunque $Z(G) = G$ (ovvero G abeliano).

Se $Z(G)$ avesse ordine p, allora anche il gruppo $G/Z(G)$ delle classi laterali di $Z(G)$ avrebbe ordine p e dunque sarebbe ciclico. Ma dalla Proposizione 5.196 sappiamo che $G/Z(G)$ è ciclico se e solo se $Z(G) = G$.

Osservazione 5.224. Sappiamo che i gruppi $\mathbb{Z}/p^2\mathbb{Z}$ e $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ non sono isomorfi tra loro in quanto il primo, a differenza del secondo, è ciclico.

Dall'Esercizio 5.223 segue che un qualsiasi gruppo di ordine p^2 è abeliano, e dunque (Teorema 5.179) isomorfo ad uno di questi due gruppi.

Concludiamo il paragrafo dimostrando, attraverso la formula delle classi, le generalizzazioni del teorema di Cauchy e di Sylow per gruppi G non necessariamente abeliani.

Teorema 5.225 (Teorema di Cauchy)**.** *Sia G un gruppo finito di ordine $n > 1$. Sia p un primo che divide n, allora esiste $x \in G$ tale che $o(x) = p$.*

Dimostrazione. Sia $|G| = p \cdot m$, procediamo per induzione su m. Il passo base ($m = 1$) è ovvio in quanto se $|G| = p$ allora G è ciclico e quindi esiste un elemento di ordine p.

Supponiamo adesso la tesi vera per $m' < m$ e dimostriamola per m, distinguendo due casi a seconda che G abbia o meno un sottogruppo proprio H di ordine un multiplo di p.

- Se G ha un sottogruppo proprio H di ordine un multiplo di p, allora $|H| = pm'$ con $m' < m$ e si può quindi applicare l'ipotesi induttiva sul gruppo H. Esiste dunque x in H di ordine p. Essendo $H \subset G$, x è in particolare un elemento di G.
- Se G non ha sottogruppi propri di ordine un multiplo di p, allora utilizziamo la formula delle classi:

  $$|Z(G)| = \underbrace{p \cdot m}_{|G|} - \sum_{x \in R \setminus Z(G)} [G : C(x)]$$

  In particolare se n_x è l'ordine di $C(x)$ (che è un sottogruppo proprio di G) per ipotesi p non divide n_x. Dunque, gli addendi nella sommatoria, che sono tutti del tipo $\dfrac{p \cdot m}{n_x}$, sono multipli di p, e la sommatoria è divisibile per p. Di conseguenza anche $|Z(G)|$ lo è. Ma $|Z(G)|$ è un sottogruppo di G, e per ipotesi non può essere proprio (siamo nel caso G senza sottogruppi propri di ordine multiplo di p). Dunque $G = Z(G)$, cioè G è abeliano, e per gruppi abeliani abbiamo già mostrato il teorema di Cauchy (Teorema 5.149) che garantisce l'esistenza di un elemento x di ordine

p in G. Facciamo notare che, proprio per Cauchy, in questo caso $G = \mathbb{Z}_p$ (tra l'altro lo si poteva ricavare anche dal fatto che $< x >$ di ordine p è un sottogruppo di G, e quindi non può essere proprio, dunque G è un gruppo ciclico di ordine p...).

□

Teorema 5.226 (Teorema di Sylow)**.** *Sia G un gruppo finito di ordine $n > 1$. Per ogni p primo che divide n esiste un p-sottogruppo di Sylow H di G (ovvero un sottogruppo di ordine p^m, massima potenza di p che divide n).*

DIMOSTRAZIONE. Possiamo scrivere $|G| = p^m \cdot k$ con k non divisibile per p. Anche in questo caso, analogamente a quanto fatto per il teorema di Cauchy, procediamo per induzione, ma questa volta sull'ordine di G.
Passo base. Se $|G| = 2$, allora l'unica potenza di primo che divide l'ordine del gruppo è 2 ed esiste un sottogruppo di ordine 2: G stesso.
Passo induttivo. Supponiamo ora vero il teorema per tutti i gruppi di ordine minore di n e dimostriamolo per G. Se G è abeliano abbiamo già dimostrato questo teorema, se G non è abeliano allora $G \neq Z(G)$ e dunque nella formula delle classi:

$$|Z(G)| = p^m \cdot k - \sum_{x \in R \setminus Z(G)} [G : C(x)]$$

la sommatoria a destra non è nulla. Distinguiamo due casi:

- Se esiste un x in $R \setminus Z(G)$ tale che p non divide $[G : C(x)]$, allora:

  $$|C(x)| = |G|/[G : C(x)] = p^m \cdot r \quad r < k$$

  Infatti essendo $x \notin Z(G)$, x non commuta con tutti gli elementi di G e dunque $C(x)$ è un sottogruppo proprio di G. Applicando l'ipotesi induttiva al gruppo $C(x)$ di ordine $p^m \cdot r$ con $r < k$, si ha la tesi.
- Se per ogni x in $R \setminus Z(G)$, p divide $[G : C(x)]$, allora dalla formula delle classi segue che p divide $|Z(G)|$. Dunque esiste un elemento $h \in Z(G)$ di ordine p. Sappiamo, dall'Esercizio 5.195, che $H =< h >$ è un sottogruppo normale di G. Possiamo dunque considerare il gruppo quoziente G/H il cui ordine è $p^{m-1} \cdot k$ (infatti H ha ordine p). Dunque p^{m-1} divide $|G/H|$ e p^m non divide $|G/H|$, ed essendo $|G/H| < |G|$ per ipotesi induttiva, da questo segue che esiste un sottogruppo $\bar{K}$ di G/H di ordine p^{m-1}. Consideriamo adesso:

  $$K = \{g \in G | gH \in \bar{K}\} = {\pi_H}^{-1}(\bar{K})$$

  K è un sottogruppo di G (Esercizio 5.125) e inoltre $\bar{K} = \pi_H(K)$, dunque dal teorema di omomorfismo per gruppi segue che $\bar{K} \cong K/H$. Perciò:

  $$p^{m-1} = |\bar{K}| = \frac{|K|}{|H|} = \frac{|K|}{p}$$

  Da questo si ricava $|K| = p^m$.

□

Corollario 5.227. *Sia G un gruppo finito, se p è un primo tale che p^m divide l'ordine di G, allora esiste un sottogruppo H di G di ordine p^m.*

DIMOSTRAZIONE. Sia p^s la massima potenza di p che divide $|G|$, allora dal Teorema 5.226 sappiamo che esiste un sottogruppo K di G di ordine p^s. Mostriamo che, per ogni $0 \leq m \leq s$, K (e dunque G) ha un sottogruppo di ordine p^m.

Procediamo per induzione su s.

Passo base. Se $s = 1$ non c'è niente da dimostrare, infatti esiste un sottogruppo H di ordine $p^0 = 1$ che è il sottogruppo banale $H = \{e\}$ ed un sottogruppo di ordine p che è K stesso.

Passo induttivo. Supponiamo vera la tesi per i gruppi di cardinalità p^r con $r < s$ e dimostriamola per K di ordine p^s.

Consideriamo $Z(G)$: dal Teorema 5.222 sappiamo che ha ordine un multiplo di p, quindi esiste un elemento $h \in Z(G)$ di ordine p. $H =< h >$ è un sottogruppo normale di G e G/H è un gruppo con p^{s-1} elementi. Dunque, per ipotesi induttiva, in G/H esiste un sottogruppo $\bar{W}_t$ di ordine p^t, per ogni t tale che $0 \leq t \leq s-1$. Analogamente alla dimostrazione precedente consideriamo:

$$W_t = \{g \in G | gH \in \bar{W}_t\} = {\pi_H}^{-1}(\bar{W}_t)$$

Tali W_t sono sottogruppi di G e inoltre $\bar{W}_t \cong W_t/H$ per cui:

$$p^t = |\bar{W}_t| = \frac{|W_t|}{|H|} = \frac{|W_t|}{p}$$

da cui segue che i W_t sono sottogruppi di G di cardinalità p^{t+1}. Ovvero abbiamo mostrato che esistono sottogruppi di G di ordine p^t con $1 \leq t \leq s$. Per concludere basta osservare che G ha sempre un sottogruppo di ordine $p^0 = 1$ che è il sottogruppo banale $\{e\}$. □

11. Gruppi di permutazioni

Concludiamo il capitolo andando a studiare più da vicino il gruppo $(S(X), \circ)$ delle funzioni bigettive di un insieme X in se stesso. Tale gruppo è particolarmente interessante per due motivi: fornisce un esempio non banale di gruppo non abeliano e inoltre, dal teorema di Cayley, sappiamo che ogni gruppo G è isomorfo ad un sottogruppo di $S(G)$. Ci interesseremo in particolare di gruppi di permutazioni finiti, ma prima mostriamo come il gruppo $(S(X), \circ)$ non sia abeliano se $|X| > 2$.

Proposizione 5.228. *Se $|X| > 2$, il gruppo $S(X)$ non è abeliano.*

DIMOSTRAZIONE. Siano $a, b, c \in X$ e consideriamo i seguenti due elementi σ_1, σ_2 di $S(X)$:

$$\sigma_1(x) = \begin{cases} a \text{ se } x = b \\ b \text{ se } x = a \\ x \text{ altrimenti} \end{cases} \qquad \sigma_2(x) = \begin{cases} c \text{ se } x = b \\ b \text{ se } x = c \\ x \text{ altrimenti} \end{cases}$$

In pratica σ_1 scambia a con b e lascia fissi tutti gli altri elementi di X, analogamente σ_2 scambia b con c e lascia fisso tutto il resto. Allora si ha che:

$$(\sigma_1 \circ \sigma_2)(x) = \begin{cases} b \text{ se } x = a \\ c \text{ se } x = b \\ a \text{ se } x = c \\ x \text{ altrimenti} \end{cases} \qquad (\sigma_2 \circ \sigma_1)(x) = \begin{cases} c \text{ se } x = a \\ a \text{ se } x = b \\ b \text{ se } x = c \\ x \text{ altrimenti} \end{cases}$$

Da cui segue che $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$. □

Se X è finito di cardinalità n, esiste un'applicazione bigettiva f da X a $\mathbb{N}_n = \{1, 2, \ldots, n\}$. Dunque $S(X)$ e $S(\mathbb{N}_n)$ sono in corrispondenza biunivoca, basta associare ad ogni elemento ϕ di $S(\mathbb{N}_n)$ l'elemento ψ di $S(X)$ definito, per ogni x in X, da:

$$\psi(x) = f^{-1}(\phi(f(x)))$$

Per studiare i gruppi di permutazioni di un insieme di n elementi, possiamo dunque limitarci al gruppo di permutazioni di $\mathbb{N}_n$.

Definizione 5.229. L'insieme $S(N_n)$ è detto **gruppo simmetrico** o **gruppo delle permutazioni** di n elementi e lo indicheremo con il simbolo $\mathcal{S}_n$.

Osservazione 5.230. Abbiamo già visto nel paragrafo sul calcolo combinatorio che $\mathcal{S}_n$ è un gruppo finito di cardinalità $n!$.

Come succede spesso in matematica, una buona notazione può essere molto di aiuto nella manipolazione degli oggetti matematici in gioco. In questo caso, come possiamo rappresentare gli elementi di $\mathcal{S}_n$ in modo che sia immediato *vedere* quale è l'immagine di ogni elemento di $\mathbb{N}_n$? La scelta che faremo sarà quella di indicare un generico $\sigma \in \mathcal{S}_n$ come segue:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

In questo modo l'immagine tramite σ di un qualsiasi elemento di $\mathbb{N}_n$ è scritta sotto l'elemento stesso. Vediamo un esempio.

Esempio 5.231. Consideriamo $\sigma \in \mathcal{S}_7$ descritto da:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 2 & 7 & 6 & 4 \end{pmatrix}$$

σ lascia fissi 1 e 6, e manda il 2 in 3, il 3 in 5, il 4 in 2, il 5 in 7 e il 7 in 4.

La notazione introdotta ci permette di calcolare piuttosto semplicemente la composizione di permutazioni e l'inversa di una permutazione, vediamo come con un altro esempio.

Esempio 5.232. Consideriamo gli σ_1, σ_2 elementi di $\mathcal{S}_5$ definiti da:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$$

Sappiamo che per calcolare $\sigma_1 \circ \sigma_2$ dobbiamo prima applicare σ_2 e poi σ_1, allora scriviamo σ_2 con la notazione introdotta e aggiungiamo una terza riga in cui mettiamo l'immagine degli elementi della seconda riga tramite σ_1:

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$$

A questo punto $\sigma_1 \circ \sigma_2$ è descritta da:

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$$

Analogo discorso per $\sigma_2 \circ \sigma_1$, per cui si ha:

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

Anche in questo caso notiamo che σ_1 e σ_2 non commutano.
Per trovare l'inverso è ancora più semplice: l'inverso di una permutazione *deve rimettere tutto a posto*, quindi se a è andato in b tramite una permutazione, la permutazione inversa deve *rimettere* b in a. Dunque, per scrivere l'inverso di σ_1 con la notazione introdotta, si deve scambiare la prima riga con la seconda e poi riordinare le colonne verticali in modo che nella prima riga i numeri compaiano in ordine crescente:

$$\text{scambio righe} = \begin{pmatrix} 1 & 3 & 5 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \to (\sigma_1)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

Esercizio 5.233. *Scrivere l'inversa di* σ_2.

Definizione 5.234. Due permutazioni σ, φ di $\mathcal{S}_n$ si dicono **disgiunte** se sono disgiunti i sottoinsiemi H_σ e H_φ di $\mathbb{N}_n$ degli elementi non lasciati fissi rispettivamente da σ e φ. Ovvero:

$$\underbrace{\{i \in \mathbb{N}_n | \sigma(i) \neq i\}}_{H_\sigma} \cap \underbrace{\{i \in \mathbb{N}_n | \varphi(i) \neq i\}}_{H_\varphi} = \emptyset$$

Osservazione 5.235. Osserviamo che dato $\sigma \in \mathcal{S}_n$, se $i \in H_\sigma$ allora anche $\sigma(i) \in H_\sigma$. Infatti se $\sigma(i)$ fosse lasciato fisso da σ avremmo:

$$\sigma(\sigma(i)) = \sigma(i)$$

Per l'iniettività di σ questo implicherebbe $\sigma(i) = i$, contro l'ipotesi che $i \in H_\sigma$.

Osservazione 5.236. Abbiamo osservato che se $n > 2$ il gruppo $\mathcal{S}_n$ non è abeliano. È vero però che due permutazioni disgiunte σ e φ di $\mathcal{S}_n$ commutano, ovvero $\sigma \circ \varphi = \varphi \circ \sigma$. Infatti, per ogni i appartenente a $\mathbb{N}_n$, si possono avere 3 casi:

(1) Se $i \notin H_\sigma \cup H_\varphi$, allora i viene lasciato fisso sia da σ che da φ e dunque:
$$\sigma \circ \varphi(i) = \sigma(\varphi(i)) = \sigma(i) = i = \varphi(i) = \sigma(\varphi(i)) = \sigma \circ \varphi(i)$$

(2) Se $i \in H_\sigma$, allora per l'osservazione 5.235 anche $\sigma(i) \in H_\sigma$ e per l'ipotesi di *disgiunzione* questo significa che sia i che $\sigma(i)$ vengono lasciate fisse da φ. Si ha dunque:
$$\sigma(\varphi(i)) = \sigma(i) = \varphi(\sigma(i))$$

(3) Se $i \in H_\varphi$, si ragiona in maniera del tutto analoga al caso precedente.

Sia $\sigma \in \mathcal{S}_n$ e introduciamo la seguente relazione binaria su $\mathbb{N}_n$:

$$a \sim_\sigma b \overset{def.}{\leftrightarrow} \exists i \in \mathbb{N} \; a = \sigma^i(b)$$

Esercizio 5.237. *La relazione binaria* $\sim_\sigma$ *su* $\mathbb{N}_n$*, introdotta a partire da una permutazione* $\sigma \in \mathcal{S}_n$*, è una relazione di equivalenza su* $\mathbb{N}_n$.

Definizione 5.238. Sia σ in $\mathcal{S}_n$ e i un elemento di $\mathbb{N}_n$. La classe di equivalenza di i rispetto alla relazione $\sim_\sigma$ è chiamata **orbita** di i tramite σ. Se i è lasciata fissa da σ, la sua classe di equivalenza è l'insieme che contiene solo i e l'orbita viene detta **banale**.

Osservazione 5.239. Consideriamo σ in $\mathcal{S}_n$ e i un elemento di $\mathbb{N}_n$. L'orbita di i è un insieme finito (ha al più n elementi), quindi per il principio dei cassetti, esistono h, k in $\mathbb{N}$ con $h < k \leq n$ tali che $\sigma^h(i) = \sigma^k(i)$. Questo è equivalente al fatto che $\sigma^{k-h}(i) = i$, da cui segue che l'insieme $S = \{s \in \mathbb{N}^+ | \sigma^s(i) = i\}$ non è vuoto.

Per il principio del buon ordinamento, S ha un minimo l, questo ci dice che $i, \sigma(i), \ldots, \sigma^{l-1}(i)$ sono tutti elementi distinti dell'orbita di i.

Sia ora z un intero qualsiasi e calcoliamo $\sigma^z(i)$. Eseguiamo la divisione euclidea tra z e l:

$$z = q \cdot l + r \quad 0 \leq r < l$$

Dunque:

$$\sigma^z(i) = \sigma^{q \cdot l + r}(i) = \sigma^r(\sigma^{q \cdot l}(i)) = \sigma^r(i)$$

Ovvero gli elementi $i, \sigma(i), \ldots, \sigma^{l-1}(i)$ sono tutti e soli gli elementi dell'orbita di i.

Esempio 5.240. Consideriamo la seguente permutazione in $\mathcal{S}_7$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 7 & 6 & 2 & 4 & 5 \end{pmatrix}$$

Calcoliamo le orbite di ogni elemento di $\mathbb{N}_7$ tramite σ.

- L'orbita di 1 è l'orbita banale $\{1\}$.
- L'orbita di 2 è l'insieme:

$$[2]_\sigma = \{2, \underbrace{\sigma(2)}_{3}, \underbrace{\sigma(\sigma(2)) = \sigma(3)}_{7}, \underbrace{\sigma(\sigma(\sigma(2))) = \sigma(7)}_{5}\}$$

  Osserviamo che $\sigma(5) = 2$ e che l'orbita di tutti gli elementi della stessa classe di equivalenza di 2 è, per definizione di classe di equivalenza, la stessa di 2.
- L'orbita di 4 è l'insieme:

$$[4]_\sigma = \{4, \underbrace{\sigma(4)}_{6}\}$$

Abbiamo finito e come deve essere le tre orbite (classi di equivalenza) formano una partizione di $\mathbb{N}_7$, ovvero sono disgiunte e la loro unione è tutto $\mathbb{N}_7$.

Definizione 5.241. Una permutazione σ di $\mathcal{S}_n$ si dice **ciclica** o un **ciclo** se possiede al più[7] una orbita non banale. La cardinalità l dell'orbita è detta **lunghezza** del ciclo.

Osservazione 5.242. Se σ è una permutazione ciclica di lunghezza l di $\mathcal{S}_n$, allora la sua unica orbita corrisponde all'insieme H_σ (infatti tutte le altre orbite sono banali e quindi i loro elementi sono tutti e solo quelli che vengono lasciati fissi da σ). Possiamo in questo caso usare per σ la notazione $(i_1, i_2, \ldots, i_l)$, dove gli i_j al variare di j tra 1 e l, sono tutti gli elementi di H_σ, intendendo che:

$$\sigma(i_j) = \begin{cases} i_{j+1} \text{ se } & j < l \\ i_1 \text{ se } & j = l \end{cases}$$

[7]Scrivendo "al più" in luogo di "esattamente" scegliamo di considerare tra le permutazioni cicliche anche l'identità, che è l'unica permutazione che ha tutte orbite banali. Per convenzione assegnamo lunghezza 1 all'identità.

Esempio 5.243. La permutazione ciclica di $\mathcal{S}_7$ indicata con $(3,6,2,7)$, usando la notazione introdotta nell'Osservazione 5.242, si scrive come segue:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 6 & 4 & 5 & 2 & 3 \end{pmatrix}$$

Osserviamo che la rappresentazione come ciclo non è unica, avremmo potuto indicare la stessa permutazione scrivendo $(2,7,3,6)$ o $(7,3,6,2)$ o infine $(6,2,7,3)$. Questo non deve sorprendere: nel ciclo quello che conta è l'ordine, non quale sia il primo elemento (perché arrivati all'ultimo si riparte dal primo, quindi non c'è un elemento *privilegiato*). Dunque possiamo rappresentare uno stesso ciclo in l modi diversi, dove l è la lunghezza del ciclo (nel nostro caso particolare $l = 4$), uno per ogni scelta possibile di un primo elemento.

Definizione 5.244. Un ciclo di lunghezza 2 è detto **trasposizione**. Talvolta useremo la notazione $\tau_{i,k}$ per indicare la trasposizione che scambia l'elemento i con l'elemento k. Se $k = i + 1$ (cioè τ scambia due elementi consecutivi di $\mathbb{N}_n$) la trasposizione si dice **adiacente**.

Proposizione 5.245. *Una trasposizione $\tau_{i,i+k}$ può essere scritta come la composizione di $2k-1$ trasposizioni adiacenti.*

Dimostrazione. Basta osservare che:

$$\tau_{i,i+k} = \tau_{i,i+1} \circ \tau_{i+1,i+2} \circ \ldots \circ \tau_{i+k-1,i+k} \circ \ldots \circ \tau_{i+1,i+2} \circ \tau_{i,i+1}$$

□

Proposizione 5.246. *Ogni ciclo può essere scritto come composizione di trasposizioni.*

Dimostrazione. Basta osservare che il ciclo di lunghezza l $(i_1, \ldots, i_l)$ è certamente uguale al prodotto delle seguenti $l-1$ trasposizioni:

$$(i_1, i_l) \circ (i_1, i_{l-1}) \circ \ldots \circ (i_1, i_3) \circ (i_1, i_2)$$

Infatti con la prima trasposizione i_1 si scambia con i_2 e poi i_1 rimane fisso, in quanto nelle altre $l-2$ trasposizioni i_2 non compare più. A questo punto con la seconda trasposizione il *nuovo* i_1, che è l'originario i_2, si scambia con i_3 e qui rimane fermo. Iterando questa considerazione si arriva a mostrare l'uguaglianza tra il ciclo e il prodotto di trasposizioni dato. □

Proposizione 5.247. *L'ordine di una permutazione ciclica di lunghezza l, come elemento del gruppo $(\mathcal{S}_n, \circ)$ è esattamente l.*

Definizione 5.248. Dato σ in $\mathcal{S}_n$, siano $A_1, \ldots, A_k$ le orbite non banali di σ. Si chiamano **cicli di** σ le k permutazioni cicliche σ_k così definite:

$$\forall i \in \mathbb{N}_n \quad \sigma_k(i) = \begin{cases} \sigma(i) \text{ se } i \in A_k \\ i \text{ altrimenti} \end{cases}$$

Ovvero un ciclo di σ è una permutazione ciclica, che ristretta ad una delle orbite non banali A_j, coincide con σ e fuori da essa è l'identità.

Esempio 5.249. Scrivere i cicli della permutazione sotto σ in $\mathcal{S}_9$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 1 & 3 & 2 & 5 & 7 & 6 & 9 \end{pmatrix}$$

Il ciclo legato all'orbita di 1 è $(1,4,3)$. Il ciclo legato all'orbita di 2 è $(2,8,6,5)$ e poi ci sono 7 e 9 lasciati fissi da σ.

La permutazione σ è uguale alla composizione dei due cicli di s:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 1 & 3 & 2 & 5 & 7 & 6 & 9 \end{pmatrix} = (1,4,3) \circ (2,8,6,5)$$

È un caso? La risposta è contenuta nella seguente proposizione.

Proposizione 5.250. *Ogni permutazione $\sigma \in \mathcal{S}_n$ diversa dall'identità si può scrivere in modo unico (a meno dell'ordine*[8]*) come composizione di cicli disgiunti.*

Dimostrazione. Siano $A_1, \ldots, A_k$ le orbite non banali di σ e $\sigma_1, \ldots, \sigma_k$ i rispettivi cicli. Una decomposizione in cicli disgiunti di σ esiste, infatti si ha:

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_k$$

L'osservazione chiave (già fatta) è che, se $i \in A_j$ allora anche $s_j(i) \in A_j$, dunque sia i che $s_j(i)$ vengono lasciati fissi da tutti i cicli s_h con $h \neq j$. Se $i \in A_j$ si ha:

$$(\sigma_1 \circ \ldots \circ \sigma_k)(i) = \sigma_j(i)$$

σ_j è per definizione uguale a σ su A_j, quindi:

$$(\sigma_1 \circ \ldots \circ \sigma_k)(i) = \sigma(i)$$

D'altra parte, se $i \notin \cup_{j=1}^{k} A_j$, allora i viene lasciato fisso da σ e da ogni σ_j e dunque:

$$(\sigma_1 \circ \ldots \circ \sigma_k)(i) = i = \sigma(i)$$

Per dimostrare l'unicità, supponiamo di avere un ulteriore scomposizione di σ in cicli disgiunti:

$$\sigma = \varphi_1 \circ \ldots \circ \varphi_m$$

Osserviamo però che σ individua univocamente le orbite e quindi il numero k di cicli disgiunti da cui deve essere composto: da questo segue che $m = k$. Inoltre, se enumeriamo le φ_j in modo tale che φ_j sia il ciclo che *muove* l'orbita A_j, si ha che φ_j deve essere uguale a σ su A_j, cioè φ_j deve essere uguale a σ_j. □

Esercizio 5.251. *Dimostrare che l'ordine di una permutazione σ è uguale al minimo comun multiplo degli ordini dei cicli disgiunti che la compongono.*

Esercizio 5.252. *Dimostrare che se $\mathcal{S} = (i_1, i_2, \ldots, i_l)$ è una permeutazione ciclica in $\mathcal{S}_n$, allora $\mathcal{S}^{-1}$ è la permutazione ciclica descritta da $(i_l, i_{l-1}, \ldots, i_2, i_1)$ (ottenuta* leggendo *$\mathcal{S}$ da destra a sinistra).*

Definizione 5.253. Sia $\sigma \in \mathcal{S}_n$ e $\sigma_1 \circ \ldots \sigma_k$ la decomposizione di σ in cicli disgiunti. Indichiamo con l_i la lunghezza del ciclo σ_i. Si dice **segnatura** di σ il numero:

$$\sum_{i=1}^{k} (l_i - 1)$$

Indichiamo con $N(\sigma)$ la segnatura di σ. Si chiama **segno** di σ (che indicheremo con $SGN(\sigma)$) la classe di equivalenza modulo 2 di $N(\sigma)$.

Proposizione 5.254. *Ogni permutazione σ si può scrivere come composizione di trasposizioni.*

[8] Ordine che è ininfluente, visto che permutazioni disgiunte commutano.

Dimostrazione. È un'immediata conseguenza delle proposizioni 5.246 e 5.250 che una permutazione σ possa essere scritta come la composizione di trasposizioni. □

È importante osservare che, data una permutazione σ, non c'è unicità nella decomposizione in trasposizioni.

Esempio 5.255. Consideriamo la seguente permutazione:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Possiamo scriverla come $(1,4) \circ (2,3)$ ma anche come $(1,2) \circ (2,4) \circ (2,3) \circ (1,3)$.

La scrittura di una permutazione come prodotto di trasposizioni ha però un invariante.

Teorema 5.256. *Sia $\sigma \in \mathcal{S}_n$. In qualsiasi scrittura di σ come composizione di trasposizioni la parità del numero di trasposizioni usate è un'invariante di σ. Ovvero, se α_i e β_j sono trasposizioni tali che:*

$$\sigma = \alpha_1 \circ \ldots \circ \alpha_h = \beta_1 \circ \ldots \circ \beta_k$$

allora $h \equiv k$ (2).

Dimostrazione. Definiamo la seguente funzione $f : \mathcal{S}_n \longrightarrow \{-1, 1\}$:

$$f(\sigma) = \prod_{\{i,j\} \subset \mathbb{N}_n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Essendo σ una permutazione, si ha:

$$\prod_{\{i,j\} \subset \mathbb{N}_n} (\sigma(i) - \sigma(j)) = \pm \prod_{\{i,j\} \subset \{1,\ldots,n\}} (i - j)$$

ovvero che effettivamente f è a valori nell'insieme $\{-1, 1\}$. Inoltre f è un omomorfismo, siano infatti $\sigma, \tau \in \mathcal{S}_n$ e consideriamo $f(\sigma \circ \tau)$:

$$f(\sigma \circ \tau) = \prod_{\{i,j\} \subset \mathbb{N}_n} \frac{\sigma \circ \tau(i) - \sigma \circ \tau(j)}{i - j}$$

Possiamo riscrivere $f(\sigma \circ \tau)$ come:

$$f(\sigma \circ \tau) = \prod_{\{i,j\} \subset \mathbb{N}_n} \frac{\sigma \circ \tau(i) - \sigma \circ \tau(j)}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j}$$

A questo punto separando i fattori, e facendo variare gli indici su $\{\tau(i), \tau(j)\}$ in luogo di $\{i, j\}$ (cosa che non cambia niente perché τ è una permutazione di $\mathcal{S}_n$), si ha:

$$f(\sigma \circ \tau) = \underbrace{\prod_{\{\tau(i),\tau(j)\} \subset \mathbb{N}_n} \frac{\sigma \circ \tau(i) - \sigma \circ \tau(j)}{\tau(i) - \tau(j)}}_{f(\sigma)} \cdot \underbrace{\prod_{\{i,j\} \subset \mathbb{N}_n} \frac{\tau(i) - \tau(j)}{i - j}}_{f(\tau)}$$

Ovvero f è un omomorfismo.

Dopo aver definito f, mostriamo che f, valutato su una trasposizione $\tau = (a\ b)$, ha valore -1, infatti:

- Considerando le coppie di indici del tipo (a, i) si ottengono in f i fattori del seguente tipo (al variare di i):
$$\frac{\tau(a) - \tau(i)}{a - i} = \frac{b - i}{a - i}.$$
- Considerando le coppie di indici del tipo (i, b) si ottengono i fattori del tipo:
$$\frac{\tau(b) - \tau(i)}{b - i} = \frac{a - i}{b - i}.$$
Osserviamo quindi che il prodotto dei fattori relativi alle coppie (a, i) in f si cancella con i fattori relativi alle coppie (i, b).
- I fattori relativi alle coppie (i, j) con $i, j \notin \{a, b\}$ sono ovviamente uguali a 1 perchè τ è l'identità sugli elementi diversi da i e j:
$$\frac{\tau(i) - \tau(j)}{i - j} = \frac{i - j}{i - j} = 1.$$
- Rimane da considerare il valore del fattore corrispondente alla coppia (a, b):
$$f(\tau) = \prod_{\{i,j\} \subset \mathbb{N}_n} \frac{\tau(i) - \tau(j)}{i - j} = \frac{a - b}{b - a} = -1.$$

A questo punto, sfruttando il fatto che f è un omomorfismo, si ha:
$$f(\sigma) = \underbrace{\prod_{i=0}^{h} f(\alpha_i)}_{(-1)^h} = \underbrace{\prod_{j=0}^{k} f(\beta_j)}_{(-1)^k}$$

Dunque $(-1)^h = (-1)^k$, ovvero $h \equiv k$ (2). □

Definizione 5.257. Una permutazione si dice **pari** se si può scrivere come composizione di un numero pari di trasposizioni. Una permutazione si dice **dispari** se non è pari.

Osservazione 5.258. L'insieme delle permutazioni pari A_n di n elementi (con $n > 1$) è un sottogruppo normale di $\mathcal{S}_n$ (è infatti il nucleo dell'omomorfismo f introdotto nella dimostrazione del Teorema 5.256) ed ha $\frac{n!}{2}$ elementi.

Osservazione 5.259. Il Teorema 5.256 afferma che, se conosciamo una scomposizione in trasposizioni di una permutazione, possiamo stabilire se la permutazione è pari o dispari.

In particolare, un ciclo di lunghezza l è pari se e solo se l è dispari: abbiamo visto infatti (Proposizione 5.246) che un ciclo di lunghezza l può essere scritto come la composizione di $l - 1$ trasposizioni.

Più in generale:

Proposizione 5.260. *Una permutazione σ è pari se e solo se $SGN(\sigma) = [0]_2$.*

Dimostrazione. Dalla Proposizione 5.254 e dalla dimostrazione della Proposizione 5.246, sappiamo che c'è un modo per scrivere σ come la composizione di $N(\sigma)$ trasposizioni. Quindi σ è pari se e solo se $N(\sigma)$ è pari, ovvero se e solo se $SGN(\sigma) = [0]_2$. □

Proposizione 5.261. *Siano $\sigma, \gamma \in \mathcal{S}_n$ allora:*

$$SGN(\sigma \circ \gamma) = SGN(\sigma) + SGN(\gamma)$$

Detto altrimenti, SGN è un omomorfismo da $(\mathcal{S}_n, \circ)$ in $(\mathbb{Z}/2\mathbb{Z}, +)$.

Dimostrazione. $SGN(\sigma \circ \gamma) = 1$ se e solo se $\sigma \circ \gamma$ è pari, ovvero se e solo se σ e γ sono entrambe pari o entrambe dispari. Questo equivale a $SGN(\sigma) = SGN(\gamma)$, ovvero $SGN(\sigma) + SGN(\gamma) = [0]_2$. □

Esercizio 5.262. *Consideriamo in $\mathcal{S}_9$ le due seguenti permutazioni:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 6 & 7 & 4 & 5 & 2 & 1 & 8 \end{pmatrix} \quad \tau = (13529)(861)(29)$$

Determinare ordine e segno di σ, τ, $\tau^{-1}\sigma$ e $\sigma^{-1}\tau$.

Svolgimento. Innanzitutto cerchiamo di capire meglio l'azione di τ, che è la composizione di tre cicli non disgiunti:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 9 & 3 & 4 & 5 & 6 & 7 & 8 & 2 \\ 8 & 9 & 3 & 4 & 5 & 1 & 7 & 6 & 2 \\ 8 & 1 & 5 & 4 & 2 & 3 & 7 & 6 & 9 \end{pmatrix}$$

Ovvero:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 5 & 4 & 2 & 3 & 7 & 6 & 9 \end{pmatrix}$$

Cercando i cicli disgiunti di σ e τ si osserva che sono due permutazioni cicliche di lunghezza rispettivamente 2 e 6:

$$\sigma = (2, 9) \quad \tau = (1, 8, 6, 3, 5, 2)$$

Abbiamo dunque (Proposizione 5.247) che l'ordine di σ è 2 e quello di τ è 6. Per definizione di segno, $SGN(\sigma) = [2-1]_2 = [1]_2$ e $SGN(\tau) = [6-1]_2 = [1]_2$.

Essendo σ e τ permutazioni cicliche, è molto semplice scrivere le loro inverse:

$$\sigma^{-1} = \sigma = (2, 9) \quad \tau^{-1} = (2, 5, 3, 6, 8, 1)$$

Determiniamo $\tau^{-1}\mathcal{S}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 9 & 3 & 4 & 5 & 6 & 7 & 8 & 2 \\ 2 & 9 & 6 & 4 & 3 & 8 & 7 & 1 & 5 \end{pmatrix} \to \mathcal{S}^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 6 & 4 & 3 & 8 & 7 & 1 & 5 \end{pmatrix}$$

Dunque $\tau^{-1}\mathcal{S} = (1, 2, 9, 5, 3, 6, 8)$, da cui $o(\tau^{-1}\mathcal{S}) = 7$ e $SGN(\tau^{-1}\mathcal{S}) = [1]_2$.

Calcoliamoci adesso $\mathcal{S}^{-1}\tau$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 5 & 4 & 2 & 3 & 7 & 6 & 9 \\ 8 & 1 & 5 & 4 & 9 & 3 & 7 & 6 & 2 \end{pmatrix} \to \mathcal{S}^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 5 & 4 & 9 & 3 & 7 & 6 & 2 \end{pmatrix}$$

Dunque $\mathcal{S}^{-1}\tau = (1, 8, 6, 3, 5, 9, 2)$ e dunque $o(\mathcal{S}^{-1}\tau) = 7$ e $SGN(\mathcal{S}^{-1}\tau) = [1]_2$. Osservando che $\tau^{-1}\mathcal{S} = (\mathcal{S}^{-1}\tau)^{-1}$, si poteva concludere, senza ulteriori conti (sfruttando le proprietà degli omomorfismi, quale quello che associa ad ogni elemento in $\mathcal{S}_n$ il suo segno in $\mathbb{Z}_2$, e il legame tra ordine di un elemento e del suo inverso in un gruppo), che $\tau^{-1}\mathcal{S}$ ha stesso ordine e segnatura di $\mathcal{S}^{-1}\tau$.

Esercizio 5.263. *Sia $K \subset \mathcal{S}_5$ il sottoinsieme delle permutazioni di $\{1,2,3,4,5\}$ che lasciano fisso 1.*

(1) *Dimostrare che K è sottogruppo di $\mathcal{S}_5$.*
(2) *Considerata $f : K \longrightarrow K$ che associa ad ogni k in K l'elemento $k \circ (3,5)$ dimostrare che $f(K) = K$ e dire se f è omomorfismo di gruppi da K in K.*

Svolgimento. Per mostrare che K è sottogruppo di $\mathcal{S}_5$, essendo K non vuoto e $\mathcal{S}_5$ finito, basta dimostrare che è chiuso per composizione. È facile osservare che la composizione di due permutazioni che lasciano fisso 1 continua a lasciare fisso 1.

L'applicazione f non è un omomorfismo da K in K, in particolare perché $f(id) = (3,5) \neq id$. Che l'applicazione f sia surgettiva lo possiamo mostrare in tanti modi: per esempio osservando che se σ e α sono in K allora:

$$\underbrace{\sigma \circ (3,5)}_{f(\sigma)} = \underbrace{\alpha \circ (3,5)}_{f(\alpha)} \leftrightarrow \sigma = \alpha$$

In quanto essendo $\mathcal{S}_5$ un gruppo vale la legge di cancellazione (tutti gli elementi sono invertibili). Perciò f è iniettiva ma essendo tra insiemi finiti della stessa cardinalità questo implica f surgettiva.

Si poteva provare direttamente la surgettività notando che per ogni $\sigma \in K$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) \end{pmatrix}$$

La permutazione α:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & \sigma(2) & \sigma(5) & \sigma(4) & \sigma(3) \end{pmatrix}$$

Appartiene a K e $f(\alpha) = \sigma$.

Esercizio 5.264. *Siano dati i gruppi $A = A_4$, $B = \mathbb{Z}_{24}^*$, $C = \mathbb{Z}_{13}^*$, $D = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ ed $E = \mathbb{Z}_9^* \times \mathbb{Z}_4^*$. Determinare le relazioni di isomorfismo di gruppo tra di essi, giustificando perché due gruppi non siano isomorfi e viceversa esplicitando gli isomorfismi tra gruppi isomorfi.* Ricordiamo che con A_4 indichiamo il sottogruppo di degli elementi di $\mathcal{S}_4$ generati da un numero pari di trasposizioni.

Svolgimento. A è un sottogruppo di $\mathcal{S}_4$ non abeliano, quindi non può essere isomorfo a nessuno degli altri: B, C, D, E sono tutti abeliani. Per questo proviamo a sfruttare il teorema di struttura e scrivere a quali prodotti diretti di gruppi ciclici sono isomorfi, sfruttando il teorema cinese del resto

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{m \cdot n} \Leftrightarrow (m,n) = 1$$

e l'osservazione che se H, T sono due anelli allora:

$$(H \times T)^* = H^* \times T^*$$

.

(1) $B \cong (\mathbb{Z}_8)^* \times (\mathbb{Z}_3)^*$ Ora $\mathbb{Z}_3^*$ è un gruppo di due elementi ed è dunque isomorfo a $\mathbb{Z}_2$. Inoltre tutti gli elementi di $\mathbb{Z}_8^*$ hanno ordine uno (l'identità $[1]_8$) o due ($[3]_8$, $[5]_8$, $[7]_8$) quindi è un gruppo di 4 elementi non ciclico, ovvero è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Concludendo per la transitività degli isomorfismi:
$$B \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_2$$

(2) C sappiamo che è ciclico (è uno $\mathbb{Z}_p^*$ con p primo) con 12 elementi, perciò $C \cong \mathbb{Z}_{12}$. In particolare non è isomorfo a B (hanno anche cardinalità diverse).
(3) D è già scritto come prodotto diretto di gruppi ciclici e non è isomorfo a B (cardinalità diverse) e nemmeno a C che è ciclico (mentre l'ordine massimo di un elemento in D è 6).
(4) $\mathbb{Z}_9^*$ è ciclico di 6 elementi (ad esempio $[2]_9$ è un generatore) e quindi è isomorfo a $\mathbb{Z}_6$. $\mathbb{Z}_4^*$ ha due elementi e dunque è isomorfo a $\mathbb{Z}_2$, perciò:

$$E \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

Dunque l'unico isomorfismo λ che sussiste è quello tra E ed D proviamo ad esplicitarlo. Basta definire λ su un insieme di generatori di E (che non è ciclico ma generato da due elementi), ad esempio $([2]_9, [1]_4)$ e $([1]_9, [3]_4)$. Tali elementi devono andare elementi dello stesso ordine e in modo tale che il sottogruppo generato da $\lambda([2]_9, [1]_4)$ e quello generato da $\lambda([1]_9, [3]_4)$ abbiano come unica intersezione l'identità di D. Un esempio è dato dunque da:

$$\lambda([2]_9, [1]_4) = ([0]_2, [1]_2, [1]_3)$$
$$\lambda([1]_9, [3]_4) = ([1]_2, [0]_2, [0]_3)$$

Esercizio 5.265. *Descrivere l'insieme $\mathcal{S}_5$.*

Svolgimento. Una permutazione di 5 elementi può essere di 6 tipi diversi:

(1) **Un ciclo di lunghezza 5:** $(a\ b\ c\ d\ e)$. Quanti cicli di lunghezza 5 distinti ci sono? Possiamo fissare l'elemento iniziale e far girare gli altri 4 nelle restanti posizioni del ciclo. Quindi esistono $4! = 24$ cicli di lunghezza 5 distinti. Un ciclo di lunghezza 5 può essere scritto come il prodotto di 4 trasposizioni, dunque è pari.
(2) **Un ciclo di lunghezza 4:** $(a\ b\ c\ d)$. Per contare i possibili cicli di lunghezza 4, dobbiamo innanzitutto fissare quali elementi sono nel ciclo, o equivalentemente l'elemento fisso non incluso nel ciclo: abbiamo quindi 5 modi diversi di fissare i 4 elementi all'interno del ciclo. Per ognuno di queste scelte, abbiamo $3! = 6$ permutazione distinte, ottenute fissando il primo elemento tra i quattro scelti, e facendo girare gli altri 3 nelle restanti posizioni del ciclo. In tutto ci sono 30 permutazioni di questo tipo: permutazioni dispari, perchè si possono scrivere come la composizione di 3 trasposizioni.
(3) **Un ciclo di lunghezza 3 composto con un ciclo di lunghezza 2:** $(a\ b\ c)(d\ e)$. Dobbiamo scegliere i 2 elementi su 5 del ciclo di lunghezza 2 (o equivalentemente i 3 su 5 del ciclo di lunghezza 3: una volta scelti gli uni, gli altri sono univocamente determinati). Ci sono $\begin{pmatrix} 5 \\ 2 \end{pmatrix} = 10$ modi per fare questa scelta. Una volta scelti gli elementi che stanno nei due cicli, abbiamo una sola trasposizione e 2! 3-cicli diversi possibili. Quindi ci sono 20 permutazioni di questo tipo, permutazioni che sono dispari.
(4) **Un ciclo di lunghezza 3:** $(a\ b\ c)$. In questo caso, numericamente non cambia niente rispetto al caso precedente: ci sono 20 permutazioni di questo tipo. Quello che cambia è che, non essendo composte con un 2-ciclo (una trasposizione), queste permutazioni sono pari.
(5) **Due cicli di lunghezza 2:** $(a\ b)(c\ d)$. Fissiamo un elemento che rimane fisso tramite questa permutazione: ci sono 5 modi di sceglierlo. Fissati i 4

elementi che vengono scambiati, si tratta di contare le possibili coppie che si possono formare (senza interessarsi dell'ordine). Fissato uno dei quattro elementi, dobbiamo contare quante coppie possibili si possono formare con questo elemento (l'altra coppia sarà univocamente determinata da questa scelta): la risposta è 3. Ci sono quindi $3 \cdot 5 = 15$ di questo tipo di permutazioni, che sono pari perchè composizione di due trasposizioni.

(6) **Un ciclo di lunghezza 2:** $(a\ b)$. Dobbiamo scegliere 2 elementi su 5, ci sono 10 modi di farlo, poi non abbiamo altra scelta, perchè una volta fissati due elementi, la trasposizione è fissata. Essendo composte da un'unica trasposizione, queste permutazioni sono dispari.

(7) **Un ciclo di lunghezza** 1. Ovvero l'identità, che sappiamo essere unica, e pari (la possiamo infatti vedere come la composizione di due trasposizioni identiche).

12. Prodotto semi-diretto

Siano A e B gruppi, un **prodotto semidiretto** tra A e B è il dato dell'insieme $A \times B$ e di un omomorfismo $\varphi : B \longrightarrow Aut(A)$. Il prodotto semidiretto tra A e B di omomorfismo φ si indica con $A \rtimes_\varphi B$. Definiamo su $G = A \rtimes_\varphi B$ la seguente operazione:

$$(a_1, b_1) \cdot (a_2, b_2) \stackrel{def}{=} (a_1 \varphi_{b_1}(a_2), b_1 b_2).$$

In particolare il prodotto semidiretto di omomorfismo φ coincide con il prodotto diretto se e solo se per ogni $a \in A$ e per ogni $b \in B$: $\varphi_b(a) = a$, cioè quando φ è l'omomorfismo banale che manda ogni elemento di B nell'identità di $Aut(A)$.

Osservazione 5.266. Il prodotto semidiretto tra A e B, con l'operazione appena definita è un gruppo. Infatti, lasciando per esercizio il fatto che l'operazione è associativa, mostriamo che esiste l'elemento neutro, e per ogni coppia in $A \rtimes_\varphi B$ esiste l'inverso.

$$(a, b) \cdot (e_A, e_B) = (a \cdot \varphi_b(e_A), b \cdot e_B) \underbrace{=}_{\varphi_b \in Aut(A)} (a \cdot e_A, b) = (a, b)$$

$$(e_A, e_B) \cdot (a, b) = (e_A \cdot \varphi_{e_B}(a), e_B \cdot b) \underbrace{=}_{\varphi\ omo.} (e_A \cdot a, b) = (a, b)$$

quindi (e_A, e_B) è l'elemento neutro. Per l'inverso dimostriamo che, data la coppia $(a, b) \in A \rtimes_\varphi B$, possiamo sempre risolvere l'equazione $(a, b) \cdot (x, y) = (e_A, e_B)$, ovvero:

$$(a\varphi_b(x), by) = (e_A, e_B) \rightarrow \begin{cases} \varphi_b(x) = a^{-1} \rightarrow x = \varphi_b^{-1}(a^{-1}) = \varphi_{b^{-1}}(a^{-1}) \\ y = b^{-1} \end{cases}$$

Definiamo gli insiemi $\tilde{A}, \tilde{B}$:

$$\tilde{A} = A \times \{e_B\} \quad \tilde{B} = \{e_A\} \times B.$$

È facile osservare che $\gamma : A \longrightarrow \tilde{A}$ definito da: $\gamma(a) = (a, e_B)$ è un isomorfismo tra A e $\tilde{A}$, e analoga osservazione vale per $\tilde{B}$ e B. Inoltre:

- $(e_A, e_B) \in \tilde{A}$, in particolare $\tilde{A} \neq 0$.
- $\tilde{A}$ è chiuso per l'operazione $\cdot$:

$$(a_1, e_B) \cdot (a_2, e_B) = (a_1 \cdot \varphi_e(a_2), e_B \cdot e_B) = (a_1 \cdot a_2, e_B) \in A.$$

- $(a, e_B^{-1})^{-1} = (\varphi_{e_B}(a^{-1}), e_B) = (a^{-1}, e_B) \in \tilde{A}$.

Quindi $\tilde{A}$ (e analogamente per $\tilde{B}$) è un sottogruppo di $G = A \rtimes_\varphi B$.

Osservazione 5.267. Come nel caso del prodotto diretto, se $G = A \rtimes_\varphi B$ allora:

(1) $\tilde{A} \cdot \tilde{B} = G$ infatti, se $(a, b) \in G$, allora $(a, b) = (a, e_B) \cdot (e_A, b)$.
(2) $\tilde{A} \cap \tilde{B} = \{e_G\}$.

Osservazione 5.268. Se $G = A \rtimes_\varphi B$ allora $\tilde{A} \triangleleft G$. Infatti per ogni $g = (a, b)$ in G e per ogni $x = (s, e_B) \in \tilde{A}$ si ha:

$$(a, b)(s, e_B)(\varphi_{b^{-1}}(a^{-1}), b^{-1}) = (a\varphi_b(s)\varphi_b(\varphi_{b^{-1}}(a^{-1})), e_B) = (a\varphi_b(s)a^{-1}, e_B) \in \tilde{A}.$$

Mentre in generale $\tilde{B}$ non è un sottogruppo normale di G.

Teorema 5.269. *Siano G un gruppo e H, K sottogruppi di G tali che:*

(1) $H \triangleleft G$.
(2) $H \cap K = \{e\}$.
(3) $H \cdot K = G$.

Allora $G \cong H \rtimes_\varphi K$ dove $\varphi : K \longrightarrow Aut(H)$ è l'omomorfismo che associa ad ogni $k \in K$ l'automorfismo φ_k: $\varphi_k(h) = khk^{-1}$.[9]

Dimostrazione. Consideriamo l'applicazione $f : H \rtimes_\varphi K \longrightarrow G$ definita da:

$$f(h, k) = hk$$

e dimostriamo che è un isomorfismo.[10]

- f è un omomorfismo, infatti usando la definizione dell'operazione $\cdot$ nel prodotto semidiretto si ha che:

  $$f[(h, k) \cdot (h', k')] = f(h\varphi_k(h'), kk') = h(kh'k^{-1})kk'$$

  e per la proprietà associativa:

  $$f[(h, k) \cdot (h', k')] = h(kh'k^{-1})kk' = hkh'k' = f(h, k) \cdot f(h', k').$$

- f è iniettivo:

  $$f(h, k) = e \leftrightarrow hk = e \leftrightarrow \underbrace{h}_{\in H} = \underbrace{k^{-1}}_{\in K} \leftrightarrow h = k = e \in H \cap K.$$

- f è surgettiva, infatti per ipotesi $H \cdot K = G$.

□

Osserviamo che se anche K è un sottogruppo normale, allora (lemma 5.163) ogni elemento di H commuta con ogni elemento di K, perciò $khk^{-1} = h$ e quindi φ_k è sempre l'omomorfismo banale per ogni k, cioè, come sapevamo già, G è isomorfo al prodotto diretto tra H e K.

---

[9] Dato un gruppo G, ad ogni elemento $g \in G$ è possibile associare l'automorfismo φ_g, tale che $\forall h \in G : \ \varphi_g(h) = ghg^{-1}$. L'insieme di questi automorfismi è un sottogruppo di $Aut(G)$, detto sottogruppo degli **automorfismi interni** di G.

[10] È bene sottolineare che in questi passaggi indichiamo con lo stesso simbolo $\cdot$ due operazioni diverse: l'operazione per cui G è un gruppo, e l'operazione di prodotto semidiretto.

Esempio 5.270 (Costruzione di prodotto semidiretto)**.** Consideriamo il gruppo $D_n =< x, y >$ con x rotazione di angolo $\frac{2\pi}{n}$ e y simmetria rispetto ad un asse del poligono. Sappiamo (vedi appendice) che il sottogruppo delle rotazioni H è normale in D_n e consideriamo $K = \{e, y\} < D_n$. Allora $H \cdot K = D_n$ e $H \cap K = \{e\}$, quindi: $D_n \cong H \rtimes_\varphi K$ con:

$$\varphi_e = id \text{ e } \varphi_y(x) = yxy^{-1} \text{ ma in } D_n \ yx = x^{-1}y \text{ quindi } \varphi_y(x) = x^{-1}.$$

H è un sottogruppo ciclico di ordine n e K è isomorfo al sottogruppo di $Aut(H)$ composto dall'identità e dall'automorfismo che ad ogni elemento associa l'inverso, perciò:

$$D_n \cong \mathbb{Z}/_{n\mathbb{Z}} \rtimes_\varphi \mathbb{Z}/_{2\mathbb{Z}}.$$

Esempio 5.271. Sia G un gruppo di ordine $p \cdot q$ con p, q primi e $p > q$. Dal teorema di Cauchy segue che:

$$\begin{cases} \exists x \in G : ord(x) = p \\ \exists y \in G : ord(y) = q \end{cases}$$

Consideriamo $H =< x >$ e $K =< y >$, questi due sottogruppi di G sono tali che:

$$H \cap K = \{e\} \quad \text{e} \quad H \cdot K = G$$

infatti un elemento in comune tra H e K deve avere ordine che divide p e q che sono primi distinti, e quindi deve avere ordine 1. Inoltre:

$$ord(HK) = \frac{ord(H) \cdot ord(K)}{ord(H \cap K)} = p \cdot q = ord(G).$$

Questo ci dice anche che gli elementi del tipo hk con $h \in H$ e $k \in K$ sono tutti distinti.[11]

Osserviamo inoltre che il sottogruppo tra H e K con più elementi (in questo caso H perchè abbiamo supposto $p > q$) è un sottogruppo normale di G. Fissato un qualsiasi $g \in G$ consideriamo infatti l'automorfismo di G, σ_g, che associa ad ogni $x \in G$ l'elemento gxg^{-1}. Allora $\sigma_g(H) = H'$ è un sottogruppo di ordine p di G come H. Ma questo dimostreremo che implica $H' = H$, e quindi per ogni $g \in G$ si ha:

$$gHg^{-1} = H$$

cioè $H \lhd G$. Supponiamo per assurdo che esista $L < G$ di ordine p e $L \neq H$, allora $H \cap L = \{e\}$ in quanto l'ordine dell'intersezione (essendo l'intersezione di gruppi un sottogruppo) è un divisore comune dei gruppi, quindi o 1 oppure p, ma se fosse p avremmo $L = H$ contro l'ipotesi che i due sottogruppi siano distinti. $H \cdot L$ ha $p \cdot p = p^2$ elementi (la dimostrazione che sono distinti è identica a quella fatta nella nota precedente), ma $H \cdot L \subseteq G$ che ha $p \cdot q$ elementi. Assurdo.

Conclusione: se G è un gruppo con $p \cdot q$ elementi ($p > q$ numeri primi) allora G è isomorfo al prodotto semidiretto tra i gruppi H e K generati da un elemento di ordine rispettivamente p e q:

$$G \cong H \rtimes_\varphi K$$

---

[11] Possiamo provarlo anche direttamente, osservando che se $hk = h'k'$ allora

$$h'^{-1}h = k'k^{-1} \in H \cap K$$

e quindi è uguale all'identità ovvero

$$h'^{-1}h = e = k'k^{-1}$$

da cui $h = h'$ e $k = k'$.

con $K \cong \mathbb{Z}/_{q\mathbb{Z}}$ (tramite l'isomorfismo che associa a $y^j \in K$ l'elemento $j \in \mathbb{Z}/_{q\mathbb{Z}}$) e $H \cong \mathbb{Z}/_{p\mathbb{Z}}$, quindi:

$$\varphi : K \longrightarrow Aut(H) \cong Aut(\mathbb{Z}/_{p\mathbb{Z}}) \cong (\mathbb{Z}/_{p\mathbb{Z}})^*$$

L'omomorfismo φ può essere di due tipi:

(1) *primo tipo:* Se φ è banale, cioè a tutti gli elementi di K corrisponde l'identità, allora:

$$G \cong H \times K \cong \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{q\mathbb{Z}} \underbrace{\cong}_{teo.4.105} \mathbb{Z}/_{pq\mathbb{Z}}$$

Quindi se φ è banale G è ciclico.

(2) *secondo tipo:* Se φ non è banale allora φ è iniettivo, infatti essendo K ciclico di ordine un primo ogni suo elemento diverso da e genera K e φ e un omomorfismo, quindi se un elemento $k \in K$ diverso da e è tale che $\varphi(k) = id$, allora:

$$K =< k > \subseteq Ker(\varphi) \Rightarrow \ Ker(\varphi) = K$$

e φ sarebbe l'omomorfismo banale, contro la nostra ipotesi. Questo implica che $\varphi(K) = L \subseteq (\mathbb{Z}/_{p\mathbb{Z}})^*$ ha ordine q, e quindi che $q|(p-1)$. (L è l'unico sottogruppo di $(\mathbb{Z}/_{p\mathbb{Z}})^*$ di ordine q, in quanto $(\mathbb{Z}/_{p\mathbb{Z}})^*$ è ciclico.) Inoltre L è ciclico generato da $z = \varphi(1)$ (infatti $\varphi(m) = z^m$).
Indichiamo con $\cdot$ il prodotto semidiretto e con $\cdot_G$ il prodotto tra elementi di G e consideriamo l'isomorfismo $f : H \rtimes_\varphi K \longrightarrow G$ definito da: $f(h,k) = h \cdot_G k$, allora siano $(x^i, y^j), (x^t, y^s) \in H \rtimes_\varphi K$:

$$f[(x^i, y^j) \cdot (x^t, y^s)] \underbrace{=}_{f \text{ è omomorfismo}} f(x^i, y^j) \cdot_G f(x^t, y^s)$$

e quindi:

$$f[(x^i, y^j) \cdot (x^t, y^s)] = x^i \cdot_G y^j \cdot_G x^t \cdot_G y^s$$

D'altra parte, calcolando prima il prodotto semidiretto all'interno della parentesi quadra, si ottiene che $f[(x^i, y^j) \cdot (x^t, y^s)]$ è uguale anche a:

$$f(x^i \cdot_G \varphi_{y^j}(x^t), y^j \cdot_G y^s) = x^i \cdot_G \varphi_{y^j}(x^t) \cdot_G y^j \cdot_G y^s$$

E dunque, indicando con z l'immagine di 1 tramite φ:

$$\varphi(y^j)(x^t) = \varphi_{y^j}(x^t) = x^{z^j t}$$

Questo fornisce la regola del gruppo:

$$x^{z^j t} \cdot_G y^j = y^j \cdot_G x^t.$$

Esempio 5.272. Sia G un gruppo di ordine $2p$ con p primo diverso da 2. Allora $q = 2|(p-1)$ e quindi $G \cong \mathbb{Z}/_{p\mathbb{Z}} \rtimes_\varphi \mathbb{Z}/_{2\mathbb{Z}}$. Per esempio $ord(D_p) = 2p$ e quindi $D_p \cong \mathbb{Z}/_{p\mathbb{Z}} \rtimes_\varphi \mathbb{Z}/_{2\mathbb{Z}}$.
Consideriamo il gruppo dei quaternioni Q_4, se Q_4 si potesse scrivere come prodotto semidiretto, allora esisterebbero H e K sottogruppi di ordine 4 e 2 con $H \cap K = \{1\}$ e $H \cdot K = Q_4$. L'unico gruppo di ordine 2 è $Z(Q_4) = \{\pm 1\}$, ma nei gruppi di ordine 4 c'e' sempre -1 e quindi $H \cap K$ non potrà mai essere solo l'identità. Di conseguenza G non può essere isomorfo ad un prodotto semidiretto.

CAPITOLO 6

Anelli

1. Definizione e prime proprietà

Dopo aver studiato la struttura algebrica di *gruppo*, ne introduciamo un'altra che in qualche modo generalizza la struttura degli interi: quella di anello. Per definire una struttura di anello, proprio come per l'insieme degli interi, è necessario definire su di un insieme A due operazioni, che chiameremo addizione e moltiplicazione.

Definizione 6.1. Un **anello** è un insieme $\mathcal{A}$ su cui sono definite due operazioni (che indicheremo con $+, \cdot$) in modo tale che:

(1) $(\mathcal{A}, +)$ è un gruppo abeliano (indicheremo con 0 l'elemento neutro[1]).
(2) $\mathcal{A}$ è chiuso per l'operazione $\cdot$, ovvero per ogni $a, b \in \mathcal{A}$ si ha che $a \cdot b$ è un elemento di $\mathcal{A}$.
(3) L'operazione $\cdot$ è associativa.
(4) Valgono le leggi distributive:
   - $\forall a, b, c \in \mathcal{A} \quad a(b + c) = ab + ac$.
   - $\forall a, b, c \in \mathcal{A} \quad (a + b)c = ac + bc$.

Esempio 6.2. È facile verificare che $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ con m intero maggiore di 1, sono anelli.

Può accadere che la moltiplicazione di un anello $\mathcal{A}$ verifichi proprietà ulteriori rispetto a quelle *minimali* richieste affinchè $\mathcal{A}$ sia un anello. Introduciamo delle nuove definizioni proprio per descrivere questi casi:

Definizione 6.3. Un anello $(\mathcal{A}, +, \cdot)$ per cui $\cdot$ sia commutativa, ovvero:

$$\forall a, b \in \mathcal{A} \; a \cdot b = b \cdot a$$

si dice **anello commutativo**.

Esempio 6.4. L'anello $(\mathbb{Z}, +, \cdot)$ è ovviamente commutativo. Un esempio di anello non commutativo è quello formato dall'insieme delle matrici quadrate di ordine n a coefficienti reali con le operazioni di $+$ e $\cdot$.

Definizione 6.5. Un anello $(\mathcal{A}, +, \cdot)$ per cui esista l'elemento neutro (indicheremo tale elemento con 1) di $\cdot$, ovvero per cui $1 \cdot a = a \cdot 1 = a$, per ogni a in A, si dice **anello con unità** o **unitario**.

Esempio 6.6. L'anello $(\mathbb{Z}, +, \cdot)$ è commutativo con unità, mentre $(P, +, \cdot)$, con P insieme dei numeri interi pari, è un anello senza unità: 1 è dispari!

Esercizio 6.7. *Sia* $(\mathcal{A}, +, \cdot)$ *un anello. Dimostrare che* $\forall a \in \mathcal{A}$, $a \cdot 0 = 0$

[1] È possibile in quanto l'elemento neutro di una operazione se esiste è unico.

Svolgimento. Per ogni a in $\mathcal{A}$ si ha:

$$a \cdot 0 \underbrace{=}_{0 \ el.neutro} a \cdot (0+0) \underbrace{=}_{prop.\ dist.} a \cdot 0 + a \cdot 0$$

Addizionando per l'inverso additivo di $a \cdot 0$, si ottiene proprio $0 = a \cdot 0$.

Esempio 6.8. L'insieme $A = \{f | f : \mathbb{R} \longrightarrow \mathbb{R}\}$ con le operazioni di somma $\tilde{+}$ e prodotto $\tilde{\cdot}$ definite come segue:

$$\forall x \in \mathbb{R} \ \ (f \tilde{+} g)(x) \overset{def}{=} f(x) + g(x)$$

$$\forall x \in \mathbb{R} \ \ (f \tilde{\cdot} g)(x) \overset{def}{=} f(x) \cdot g(x)$$

è un anello commutativo con unità. La commutatività segue dal fatto che il prodotto $\tilde{\cdot}$ è definito a partire dal prodotto su $\mathbb{R}$ che è commutativo. L'unità è la funzione reale costante uguale a 1.

Siano X un insieme e $\mathcal{A}$ un anello, anche l'insieme delle funzioni da X ad $\mathcal{A}$ su cui sono definite le operazioni come sopra è un anello. In particolare sarà commutativo se $\mathcal{A}$ lo è, e avrà l'unità se $\mathcal{A}$ è con unità (in questo caso l'unità è la funzione che manda tutti gli elementi di X nell'unità di $\mathcal{A}$).

Definizione 6.9. Sia $(\mathcal{A}, +, \cdot)$ un anello commutativo. Un elemento a di $\mathcal{A}$ diverso da 0 si dice **divisore di zero** se esiste b in $\mathcal{A}$ diverso da 0 tale che: $a \cdot b = 0$. Un anello (commutativo) $\mathcal{A}$ si dice **privo di divisori di zero** se nessun x di $\mathcal{A}$ è un divisore di zero[2].

Esempio 6.10. Consideriamo $\mathbb{Z}_{10}$, l'elemento $[2]_{10}$ è un divisore di zero, infatti $[2]_{10} \cdot [5]_{10} = [0]_{10}$ e $[5]_{10} \neq [0]_{10}$. In particolare $\mathbb{Z}_{10}$ non è privo di divisori di zero.

Definizione 6.11. Sia $(\mathcal{A}, +, \cdot)$ un anello commutativo, un elemento $x \in \mathcal{A}$ diverso da 0 e per cui esiste n in $\mathbb{N}$ con $x^n = 0$, si dice **elemento nilpotente**.

Esercizio 6.12. *Dimostrare che l'insieme dei nilpotenti è un sottoinsieme dell'insieme dei divisori di zero di un anello.*

Esempio 6.13. Esistono elementi che sono divisori dello zero, ma non nilpotenti. Ad esempio consideriamo in $\mathbb{Z}/10\mathbb{Z}$ l'elemento $[2]_{10}$. È un divisore dello zero, infatti:

$$[2]_{10} \cdot [5]_{10} = [0]_{10}$$

ma nessuna potenza di 2 sarà mai un multiplo di 10 (per il teorema fondamentale dell'aritmetica). Dunque $[2]_{10}$ non è nilpotente.

Definizione 6.14. Un anello commutativo con unità privo di divisori di zero si dice un **dominio d'integrità**.

Esempio 6.15. $(\mathbb{Z}, +, \cdot)$ è un dominio d'integrità.

Esercizio 6.16. $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ *è un dominio di integrità se e solo se* m *è primo.*

[2]Avremmo potuto generalizzare la definizione anche per anelli non commutativi, differenziando tra moltiplicazione a destra e sinistra, e dunque tra divisore destro e sinistro di zero. Trattando nel seguito quasi esclusivamente anelli commutativi, preferiamo non *complicare* le cose.

Svolgimento. Dall'Esempio 6.10 dovrebbe essere chiara l'idea. Se m si può scrivere come $a \cdot b$ entrambi maggiori di 1 e minori di m (ovvero m non è primo), allora $[a]_m \cdot [b]_m = [0]_m$ e $[a]_m$, $[b]_m$ sono diversi $[0]_m$. Viceversa se m è primo, $[a]_m \cdot [b]_m = [0]_m$ (ovvero m divide $a \cdot b$) equivale, per definizione di primo, a m divide a (ovvero $[a]_m = [0]_m$) o m divide b (ovvero $[b]_m = [0]_m$).

Definizione 6.17. Sia $(\mathcal{A}, +, \cdot)$ un anello con unità. Un elemento a di $\mathcal{A}$ si dice **invertibile** se esiste b in $\mathcal{A}$ tale che $a \cdot b = b \cdot a = 1$.

Proposizione 6.18. *Sia $\mathcal{A}$ un anello commutativo con unità. L'insieme $\mathcal{A}^*$ degli elementi invertibili di $\mathcal{A}$, ovvero:*

$$\mathcal{A}^* = \{x \in \mathcal{A} | \exists y \in \mathcal{A} \quad xy = 1\}.$$

è un gruppo rispetto alla moltiplicazione.

Dimostrazione. $\mathcal{A}^*$ è non vuoto, infatti $1 \in \mathcal{A}^*$. Inoltre per ogni $x, y \in \mathcal{A}^*$ (ovvero esistono in $\mathcal{A}$, x^{-1} e y^{-1} inversi rispettivamente di x e y), mostriamo che xy^{-1} appartiene ad $\mathcal{A}^*$ esibendone un inverso in $\mathcal{A}$.

$$(xy^{-1}) \underbrace{(yx^{-1})}_{\in \mathcal{A}} \underbrace{=}_{prop.ass.} x(y^{-1}y)x^{-1} = xex^{-1} = e$$

Dal Lemma 5.39, segue la tesi. □

Dimostriamo che in un anello commutativo privo di divisori di zero vale la regola di cancellazione per la moltiplicazione.

Lemma 6.19 (Legge di cancellazione)**.** *Sia $(\mathcal{A}, +, \cdot)$ un anello commutativo privo di divisori di zero, allora per ogni $a, b, c \in \mathcal{A}$ con $a \neq 0$:*

$$ab = ac \Leftrightarrow b = c$$

Dimostrazione. Una implicazione è banale. Supponiamo dunque che $a \cdot b$ sia uguale ad $a \cdot c$, allora:

$$a \cdot b - a \cdot c = a \cdot (b - c) = 0$$

Essendo $a \neq 0$ e $\mathcal{A}$ privo di divisori di zero, deve essere $b - c = 0$, ovvero $b = c$. □

Osservazione 6.20. Per dimostrare il Lemma 6.19 non si può usare la Proposizione 5.26 che dimostra la proprietà analoga per i gruppi. $\mathcal{A}$ infatti non è un gruppo per la moltiplicazione. D'altra parte facciamo notare come le due dimostrazioni siano sostanzialmente diverse, in quanto nel caso dei gruppi usavamo l'esistenza degli inversi, qui abbiamo sfruttato la non esistenza di divisori di zero.

Definizione 6.21. Un anello $(\mathcal{A}, +, \cdot)$ i cui elementi diversi da zero formino un gruppo rispetto a $\cdot$ si dice un **corpo**. Un corpo commutativo è detto un **campo**.

Osservazione 6.22. Dalla definizione di corpo segue che l'anello $\mathcal{A}$ deve essere con unità (altrimenti non potrebbe essere un gruppo rispetto a $\cdot$, in quanto privo di elemento neutro).

Dalla definizione segue anche che un anello $\mathcal{A}$ commutativo è un campo se e solo se ogni elemento di $\mathcal{A}$ diverso da 0 è invertibile rispetto alla moltiplicazione. Infatti, se $\mathcal{A} \setminus \{0\}$ è un gruppo per la moltiplicazione, allora - per definizione di gruppo - ogni suo elemento deve essere invertibile; viceversa, se ogni elemento diverso da 0 ha inverso, allora $\mathcal{A}^* = \mathcal{A} \setminus \{0\}$, che sappiamo essere un gruppo per la Proposizione 6.18.

Esempio 6.23. L'anello $(\mathbb{Z}, +, \cdot)$ non è un campo, infatti gli unici elementi invertibili rispetto alla moltiplicazione sono 1 e -1. L'insieme $\mathbb{Q}$ dei numeri razionali con le usuali operazioni di somma e prodotto è un campo, così come l'insieme $\mathbb{R}$ dei numeri reali.

Nel caso degli $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ è un campo se e solo se m è primo.

Sia $\mathcal{A}$ un anello commutativo con unità. Il prossimo lemma mostra che l'insieme dei divisori di zero D e quello degli invertibili $\mathcal{A}^*$ di $\mathcal{A}$ sono disgiunti.

Lemma 6.24. *Sia $(\mathcal{A}, +, \cdot)$ un anello commutativo con unità, ed indichiamo con D l'insieme dei divisori di zero di $\mathcal{A}$. Allora $D \cap \mathcal{A}^* = \emptyset$*

Dimostrazione. Mostriamo che, supponendo l'esistenza di $a \in D \cap \mathcal{A}^*$, si arriva ad un assurdo. Essendo a in D, $a \neq 0$ ed esiste $y \in \mathcal{A}$ diverso da 0 tale che $a \cdot y = 0$. D'altra parte, essendo a in $\mathcal{A}^*$, esiste $z \in \mathcal{A}$ tale che $z \cdot a = 1$. Avremmo dunque:

$$y = 1 \cdot y = (z \cdot a) \cdot y \underbrace{=}_{prop.ass.} z \cdot (a \cdot y) = z \cdot 0 \underbrace{=}_{Ese\ 6.7} 0$$

Assurdo perché per ipotesi $y \neq 0$. □

Corollario 6.25. *Un campo è privo di divisori di zero.*

Osservazione 6.26. Non è vero in generale il viceversa del Corollario 6.25, ovvero che un anello commutativo con unità senza divisori di zero sia un campo. Consideriamo infatti $\mathbb{Z}$: pur privo di divisori di zero, non è un campo. In particolare questo mostra come, in un anello infinito, un elemento non nullo che non sia divisore di zero, non è detto sia invertibile. Dimostreremo invece che, se $\mathcal{A}$ è finito, allora un elemento diverso da zero di $\mathcal{A}$ o è divisore di zero o è invertibile.

Per dimostrare il risultato sugli anelli finiti, abbiamo bisogno di provare alcune proprietà di *calcolo* valide negli anelli. Abbiamo già mostrato che, in qualsiasi anello, il prodotto di qualsiasi elemento a dell'anello con 0 è l'elemento 0. Il seguente lemma dimostra altre proprietà che ricordano la regola dei segni dei numeri interi[3].

Lemma 6.27. *Sia $(\mathcal{A}, +, \cdot)$ un anello, allora, indicando con $-a$ l'opposto di a rispetto alla addizione, per ogni $a, b \in \mathcal{A}$ si ha:*

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$$
$$(-a) \cdot (-b) = a \cdot b$$

Dimostrazione. Dobbiamo mostrare che $a \cdot b + a \cdot (-b) = 0$ (ovvero che $a \cdot (-b)$ è l'opposto di $a \cdot b$). Dalla proprietà distributiva segue che:

$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$$

Analogamente si dimostra che $(-a) \cdot b = -(a \cdot b)$.

Il fatto che $(-a) \cdot (-b) = a \cdot b$ segue dall'osservazione che $-(-a) = a$ (ovvero che l'opposto di $-a$ è a) e dalla dimostrazione del punto precedente. □

Lemma 6.28. *Sia $(\mathcal{A}, +, \cdot)$ un anello finito commutativo con unità. Allora $\mathcal{A} \setminus \{0\} = \mathcal{A}^* \cup D$.*

[3] In questo caso possiamo dimostrare la regola perché segue appunto dalle proprietà di anello, nel caso di $\mathbb{Z}$ invece definivamo in quel modo la regola proprio affinché valessero in $\mathbb{Z}$ le proprietà di anello (nello specifico la proprietà distribuitiva).

DIMOSTRAZIONE. Facciamo vedere che, se x è un elemento di $\mathcal{A}$ diverso da 0 che non appartiene a D, allora x appartiene ad $\mathcal{A}^*$. Se $x \notin D$, allora la funzione φ_x da $\mathcal{A}$ in $\mathcal{A}$ che ad ogni $y \in \mathcal{A}$ associa $\varphi_x(y) = xy$ è iniettiva. Infatti, due elementi y, z hanno la stessa immagine tramite φ_x se e solo se $xy = xz$, ovvero $xy - xz = 0$, e:

$$xy - xz = 0 \underbrace{\Leftrightarrow}_{\text{prop.dis. e Lemma 6.27}} x(y-z) = 0 \underbrace{\Leftrightarrow}_{x \notin D,\ x \neq 0} y - z = 0 \Leftrightarrow y = z$$

$\varphi_x : \mathcal{A} \to \mathcal{A}$ è iniettiva tra due insiemi finiti della stessa cardinalità ($\mathcal{A}$ sia in partenza che in arrivo), dunque φ_x è bigettiva. Esiste quindi $y \in \mathcal{A}$ tale che $\underbrace{\varphi_x(y)}_{xy} = 1$, cioè $x \in \mathcal{A}^*$. □

Corollario 6.29. *Un dominio d'integrità $(\mathcal{A}, +, \cdot)$ finito è un campo.*

Esercizio 6.30. *Dimostrare che, se di $(\mathcal{A}, +, \cdot)$ sappiamo che è un anello commutativo finito privo di divisori di zero, allora possiamo concludere che $(\mathcal{A}, +, \cdot)$ è un campo.*

Svolgimento. Quello che dobbiamo dimostrare è che sotto le ipotesi date $(\mathcal{A}, +, \cdot)$ ha l'unità.

Sia x un elemento di $\mathcal{A}$ diverso da 0, allora l'applicazione φ_x definita nella dimostrazione del Lemma 6.28 è bigettiva. Esiste dunque $e \in \mathcal{A}$ tale che $\varphi_x(e) = x \cdot e = x$. Mostriamo che e è l'elemento neutro di $\mathcal{A}$, ovvero che per ogni a in $\mathcal{A}$ si ha: $e \cdot a = a$. Sempre sfruttando la bigettività di φ_x, per ogni $a \in \mathcal{A}$, esiste $b \in \mathcal{A}$ tale che $\varphi_x(b) = x \cdot b = a$. Dunque:

$$e \cdot a = e \cdot (x \cdot b) = (e \cdot x) \cdot b = x \cdot b = a$$

Come per i gruppi, anche nel caso degli anelli siamo interessati ai sottoinsiemi che mantengano le proprietà di anello:

Definizione 6.31. Un sottoinsieme B di un anello $(\mathcal{A}, +, \cdot)$ si dice un **sottoanello** di $\mathcal{A}$ se $(B, +_B, \cdot_B)$ è un anello con le operazioni $+_B$ e $\cdot_B$, restrizioni di $+$ e $\cdot$ a B. Se $\mathcal{A}$ è unitario allora anche B deve essere unitario. Un sottoanello B di $\mathcal{A}$ si dice **proprio** se è diverso da $\mathcal{A}$ e da $\{0\}$.

In pratica, per dimostrare che B è un sottoanello di $\mathcal{A}$, basta verificare che B è un sottogruppo per l'addizione ed è chiuso per il prodotto. Nel caso di $\mathcal{A}$ unitario dobbiamo provare anche che 1 appartenga a B.

Esempio 6.32. $\mathbb{Z}$ è un sottoanello di $(\mathbb{Q}, +, \cdot)$.

$m\mathbb{Z}$ con $m > 1$ non è un sottoanello di $\mathbb{Z}$, infatti pur essendo un sottogruppo e chiuso per prodotto, non contiene l'identità.

Esercizio 6.33. *L'intersezione di due o più sottoanelli di un anello $(\mathcal{A}, +, \cdot)$ è un sottoanello di $\mathcal{A}$.*

Svolgimento. Siano B e C sottoanelli di $\mathcal{A}$: sappiamo che $B \cap C$ è un sottogruppo additivo (Proposizione 5.44). Dobbiamo perciò mostrare che l'intersezione $B \cap C$ è chiusa per la moltiplicazione. Per ogni $s, t \in B \cap C$ si ha che $s \cdot t \in B$ (B è sottoanello di $\mathcal{A}$ e quindi chiuso per il prodotto) e $s \cdot t \in C$ (anche C è sottoanello di $\mathcal{A}$). Dunque $s \cdot t \in B \cap C$.

Osserviamo infine che, se $\mathcal{A}$ è con unità, allora per definizione di sottoanello sia B che C, e dunque la loro intersezione, contengono l'unità.
Chiudiamo il paragrafo introducendo il concetto centrale di omomorfismo di anelli che riprenderemo nel seguito. Infatti, come per i gruppi, anche per la struttura di anello siamo interessati a definire e studiare le proprietà di applicazioni che conservano la struttura.

Definizione 6.34. Siano $(\mathcal{A}, +_{\mathcal{A}}, \cdot_{\mathcal{A}})$ e $(B, +_B, \cdot_B)$ anelli. Un'applicazione f da A a B si dice un **omomorfismo di anelli** se per ogni x, y in $\mathcal{A}$:

(1) $f(x +_{\mathcal{A}} y) = f(x) +_B f(y)$.,
(2) $f(x \cdot_{\mathcal{A}} y) = f(x) \cdot_B f(y)$.

2. L'anello dei polinomi $\mathcal{A}[x]$

In questa sezione definiamo l'insieme $\mathcal{A}[x]$ dei polinomi a coefficienti in un anello $\mathcal{A}$ commutativo con unità (in seguito ci interesseremo al caso particolare di $\mathcal{A}$ campo), definendo su esso le operazioni di addizione e moltiplicazione e dimostrando che l'insieme così costruito è un anello commutativo con unità.

Definizione 6.35. Sia $\mathcal{A}$ un anello commutativo con unità, un **polinomio** in una variabile a coefficienti in $\mathcal{A}$, è un'espressione formale finita del tipo:

$$f(x) = a_0 + \sum_{i=1}^{n} a_i x^i \; n \in \mathbb{N} \; a_i \in \mathcal{A}$$

Gli a_i sono detti **coefficienti** del polinomio $f(x)$.

Osservazione 6.36. Con la convenzione che $x^0 = 1$, possiamo scrivere $f(x)$ in forma compatta come $\sum_{i=0}^{n} a_i x^i$.

Inoltre possiamo vedere (può far comodo nelle prime dimostrazioni formali) un polinomio $f(x)$ in $\mathcal{A}[x]$ anche come somma infinita $\sum_{i\in\mathbb{N}} a_i x^i$ con un numero finito di a_i diversi da zero.

Definizione 6.37. Il coefficiente a_0 si dice **termine noto** di $f(x)$. Un polinomio con coefficiente direttivo 1 si dice **monico**.

Esempio 6.38. $\sqrt{2}x^3 - 5x + 1$ è un esempio di polinomio a coefficienti in $\mathbb{R}$, così come 7 è un polinomio a coefficienti in $\mathbb{R}$ (con $a_i = 0$ per $i > 0$ e $a_0 = 7$), mentre non sono polinomi a coefficienti in $\mathbb{R}$ né $5x^{-2} - 3x + 1$, né $x^{\frac{3}{2}} - 5x + 1$

Definito l'insieme $\mathcal{A}[x]$ come l'insieme di tutti i polinomi a coefficienti in $\mathcal{A}$, per costruire una struttura di anello su di esso, bisogna definire l'uguaglianza tra i suoi elementi e due operazioni binarie (che chiameremo addizione e moltiplicazione, e indicheremo con $+$ e $\cdot$).

Definizione 6.39 (Uguaglianza tra polinomi)**.** Due polinomi $f(x) = \sum_{i\in\mathbb{N}} a_i x^i$ e $g(x) = \sum_{i\in\mathbb{N}} b_i x^i$ in $\mathcal{A}[x]$ si dicono **uguali** se e solo se $a_i = b_i$ per ogni $i \in \mathbb{N}$.

Definizione 6.40. Ogni polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ in $\mathcal{A}[x]$ definisce una funzione polinomiale, che indicheremo con $\tilde{f}(x)$ da $\mathcal{A}$ in $\mathcal{A}$, ottenuta associando ad ogni k di $\mathcal{A}$ la *valutazione* di $f(x)$ in k, ovvero l'elemento $\tilde{f}(k)$ di $\mathcal{A}$ dato da:

$$\sum_{i=0}^{n} a_i \cdot k^i$$

Polinomio $f(x)$ e funzione polinomiale associata $\tilde{f}(x)$ non sono la stessa cosa. Infatti due funzioni (e quindi in particolare anche quelle polinomiali) a valori in $\mathcal{A}$ si dicono uguali se ad ogni elemento di $\mathcal{A}$ associano lo stesso valore. Se consideriamo $\mathcal{A} = \mathbb{Z}_2$, i polinomi 0 e $x-1$ di $\mathbb{Z}_2[x]$, e le rispettive funzioni polinomiali da $\mathbb{Z}_2$ a $\mathbb{Z}_2$, si ha che i polinomi sono diversi (in quanto non hanno la stessa espressione formale), mentre la funzione polinomiale associata è la stessa nei due casi, infatti le valutazioni dei due polinomi in 0 e 1 (gli unici due elementi di $\mathbb{Z}_2$) sono sempre 0. Dunque la funzione polinomiale associata sia al polinomio 0 che al polinomio $x - 1$ di $\mathbb{Z}_2[x]$ è la funzione nulla.

In realtà possiamo, usando il piccolo teorema di Fermat, generalizzare l'esempio appena fatto. Infatti sappiamo che, per ogni $\mathbb{Z}_p$ (con p primo), i due distinti polinomi x e x^p di $\mathbb{Z}_p[x]$ definiscono la stessa funzione polinomiale da $\mathbb{Z}_p$ in se stesso (ovvero la funzione identità che manda ogni elemento in se stesso). Questo ci dice che l'applicazione da $\mathbb{Z}_p[x]$ all'insieme delle funzioni da $\mathbb{Z}_p$ in $\mathbb{Z}_p$, che associa ad ogni polinomio la funzione polinomiale associata, non è iniettiva.

Dimostreremo in seguito che, se $\mathcal{A}$ è un campo infinito, tale applicazione è iniettiva; in particolare se $\mathcal{A}$ è infinito, allora due polinomi sono uguali se e solo se le corrispondenti funzioni polinomiali associate coincidono.

Osservazione 6.41. Una doverosa precisazione è il fatto che, pur non avendo definito il prodotto tra un elemento di $\mathcal{A}$ e l'indeterminata x, si assume (in qualche modo in deroga alla definizione di uguaglianza tra polinomi data) che non scrivere un termine i-esimo o scriverlo con coefficiente 0 sia la stessa cosa. Ovvero il polinomio $3x^4 - 5x^3 + x$ e $3x^4 - 5x^3 + 0 \cdot x^2 + x + 0$ vengono considerati lo stesso polinomio.

Tale espediente rende molto più semplice dare la definizione di somma tra due polinomi generici $f(x)$ e $g(x)$ in quanto permette di scriverli con lo stesso numero di coefficienti, associati alle stesse potenze dell'indeterminata x. Ad esempio, dovendo trattare le operazioni tra $x^5 - 3x + 1$ e $x^2 - 3$, possiamo *pensare* i due polinomi come:

$$x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 - 3x + 1$$
$$0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + x^2 + 0 \cdot x - 3$$

Si potrebbe essere più rigorosi introducendo la relazione di equivalenza che associa due polinomi le cui espressioni formali differiscano solo per la presenza di coefficienti nulli, ma crediamo sia una inutile complicazione.

A questo punto possiamo introdurre le operazioni di addizione e moltiplicazione tra due polinomi $f(x)$ e $g(x)$ in $\mathcal{A}[x]$.

Definizione 6.42 (Addizione tra polinomi)**.** Dati $f(x) = \sum_{i=0}^{n} a_i x^i$ e[4] $g(x) = \sum_{i=0}^{n} b_i x^i$, definiamo il **polinomio somma** $f(x)+g(x)$, che indicheremo anche con $(f + g)(x)$, come il polinomio:

$$\sum_{i=0}^{n} (a_i + b_i) x^i$$

[4]Per l'osservazione precedente possiamo considerare $f(x)$ e $g(x)$ con lo stesso numero di coefficienti.

Esempio 6.43. Seguendo la definizione appena data, la addizione dei polinomi $f(x) = x^4 - x^2 + 1$ e $g(x) = x^2 + 3$ di $\mathbb{Z}[x]$ si ottiene come segue:

$$\underbrace{1x^4 + 0x^3 - 1x^2 + 0x + 1}_{f(x)} + \underbrace{0x^4 + 0x^3 + 1x^2 + 0x + 3}_{g(x)} = \underbrace{1x^4 + 0x^3 + 0x^2 + 0x + 4}_{(f+g)(x)}$$

Se scriviamo $(f + g)(x)$ omettendo i coefficienti nulli, otteniamo come risultato il polinomio somma $x^4 + 4$.

Facciamo notare come l'idea di scrivere anche i coefficienti nulli è funzionale solo alla definizione formale di addizione data sopra.

Definizione 6.44 (Moltiplicazione tra polinomi)**.** Dati $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{j=0}^{m} b_j x^j$, definiamo il **polinomio prodotto** $f(x) \cdot g(x)$, che indicheremo anche con $(f \cdot g)(x)$, come:

$$\sum_{h=0}^{n+m} (\sum_{i+j=h} a_i \cdot b_j) x^h$$

Ovvero, se indichiamo con c_r i coefficienti di $(f \cdot g)(x)$, si ha che $c_r = \sum_{i+j=r} a_i \cdot b_j$.

Esempio 6.45. Sia $f(x) = -3x^3 - x + 3$ e $g(x) = 2x^2 + 7x$ in $\mathbb{Z}[x]$, allora il polinomio prodotto $(f \cdot g)(x)$ ha i seguenti coefficienti c_r:

$$c_0 = \underbrace{3}_{a_0} \cdot \underbrace{0}_{b_0} = 0$$

$$c_1 = \underbrace{-1}_{a_1} \cdot \underbrace{0}_{b_0} + \underbrace{3}_{a_0} \cdot \underbrace{7}_{b_1} = 21$$

$$c_2 = \underbrace{0}_{a_2} \cdot \underbrace{0}_{b_0} + \underbrace{(-1)}_{a_1} \cdot \underbrace{7}_{b_1} + \underbrace{3}_{a_0} \cdot \underbrace{2}_{b_2} = -1$$

$$c_3 = \underbrace{-3}_{a_3} \cdot \underbrace{0}_{b_0} + \underbrace{0}_{a_2} \cdot \underbrace{7}_{b_1} + \underbrace{(-1)}_{a_1} \cdot \underbrace{2}_{b_2} + \underbrace{3}_{a_0} \cdot \underbrace{0}_{b_3} = -2$$

$$c_4 = \underbrace{0}_{a_4} \cdot \underbrace{0}_{b_0} + \underbrace{(-3)}_{a_3} \cdot \underbrace{7}_{b_1} + \underbrace{0}_{a_2} \cdot \underbrace{2}_{b_2} + \underbrace{(-1)}_{a_1} \cdot \underbrace{0}_{b_3} + \underbrace{3}_{a_0} \cdot \underbrace{0}_{b_4} = -21$$

$$c_5 = \underbrace{0}_{a_5} \cdot \underbrace{0}_{b_0} + \underbrace{0}_{a_4} \cdot \underbrace{7}_{b_1} + \underbrace{(-3)}_{a_3} \cdot \underbrace{2}_{b_2} + \underbrace{0}_{a_2} \cdot \underbrace{0}_{b_3} + \underbrace{(-1)}_{a_1} \cdot \underbrace{0}_{b_4} + \underbrace{3}_{a_0} \cdot \underbrace{0}_{b_5} = -6$$

Dunque $(f \cdot g)(x) = -6x^5 - 21x^4 - 2x^3 - x^2 + 21x$.

Osserviamo che l'elemento neutro di $+$ è il polinomio con tutti i coefficienti uguali a 0, detto anche **polinomio nullo** (che indicheremo, laddove non ci siano ambiguità, con 0).

Definizione 6.46. La funzione $deg : \mathcal{A}[x] \setminus \{0\} \to \mathbb{N}$ definita come segue:

$$\forall f(x) \in \mathcal{A}[x] \setminus \{0\} \;\; deg(f(x)) = max\{i \in \mathbb{N} | a_i \neq 0\}$$

è detta **funzione grado**. Il valore $deg(f(x))$ è detto **grado** del polinomio $f(x)$.

Osservazione 6.47. La funzione grado è ben definita per ogni $\mathcal{A}[x] \setminus \{0\}$ in quanto, per $f(x) = \sum_{i=0}^{n} a_i x^i$ diverso dal polinomio nullo, l'insieme $\{i \in \mathbb{N} | a_i \neq 0\}$ è non vuoto e finito, e dunque ha massimo.

Definizione 6.48. Se $f(x) = \sum_{i=0}^{n} a_i x^i$ ha grado n, a_n si dice **coefficiente direttivo** di $f(x)$.

Proposizione 6.49 (Proprietà del grado)**.** *Supponiamo $f(x)$ e $g(x)$ elementi di $\mathcal{A}[x] \setminus \{0\}$, con $\mathcal{A}$ dominio d'integrità, allora:*

(1) *Se $(f+g)(x) \neq 0$, allora $deg((f+g)(x)) \leq \max(deg(f(x)), deg(g(x)))$*
(2) *$deg((f \cdot g)(x)) = deg(f(x)) + deg(g(x))$. In particolare, il grado del prodotto tra $f(x)$ e $g(x)$ è maggiore o uguale di $\max(deg(f(x)), deg(g(x)))$.*

DIMOSTRAZIONE. Supponiamo $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{j=0}^{m} b_j x^j$ di grado m e n rispettivamente (ovvero $a_n \neq 0$ e $b_m \neq 0$).

- Consideriamo i coefficienti c_k del polinomio somma $(f+g)(x)$. Se $k > max(n, m)$, allora $a_k = b_k = 0$ e quindi $c_k = a_k + b_k = 0$. Per definizione di grado si ha quindi che $deg((f+g)(x)) \leq max(m, n)$.
- Per definizione di polinomio prodotto, il massimo indice per cui un coefficiente del polinomio prodotto può essere diverso da 0 è $m+n$, quindi per provare la tesi basta mostrare che il coefficiente di indice $m+n$ è diverso da zero. Tale coefficiente, $a_n \cdot b_m$, essendo a_n e b_m diversi da zero e $\mathcal{A}$ un dominio di integrità, è effettivamente diverso da zero.

□

Le proprietà della funzione grado permettono di approfondire il nostro percorso di caratterizzazione della struttura di $\mathcal{A}[x]$ a partire dalla conoscenza della struttura dell'anello dei coefficienti $\mathcal{A}$.

Teorema 6.50. *$\mathcal{A}$ è un dominio di integrità se e solo se $\mathcal{A}[x]$ lo è.*

DIMOSTRAZIONE. Se $\mathcal{A}[x]$ è un dominio di integrità è ovvio che anche $A \subset \mathcal{A}[x]$ sia un dominio d'integrità. Viceversa, nella dimostrazione della Proposizione 6.49 abbiamo visto che, se $\mathcal{A}$ è un dominio di integrità e $f(x)$ e $g(x)$ sono due polinomi diversi dal polinomio nullo, allora il prodotto dei loro coefficienti direttivi è diverso da 0: dunque $(f \cdot g)(x)$ non è il polinomio nullo. □

Dal teorema sul grado del polinomio prodotto segue anche la caratterizzazione degli invertibili in $\mathcal{A}[x]$.

Corollario 6.51. *I polinomi invertibili di $\mathcal{A}[x]$ sono gli invertibili di $\mathcal{A}$.*

DIMOSTRAZIONE. $f(x)$ è invertibile in $\mathcal{A}[x]$ se e solo se esiste $g(x) \in A[x]$ tale che $(f \cdot g)(x) = 1$. Dall'Esercizio 6.7 sappiamo che il polinomio nullo è sicuramente non invertibile. Supponiamo dunque $f(x)$ diverso da 0 ed invertibile (con inverso $g(x)$), allora:

$$\underbrace{deg(f(x)) + deg(g(x))}_{deg((f \cdot g)(x))} = \underbrace{0}_{deg(1)}$$

Essendo $deg(f(x))$ e $deg(g(x))$ due numeri naturali, necessariamente deve essere $deg(f(x)) = deg(g(x)) = 0$. Dunque $f(x) \in \mathcal{A}$ e deve essere un invertibile di $\mathcal{A}$ (infatti l'inverso $g(x)$ appartiene anch'esso ad $\mathcal{A}$ avendo grado 0). □

Studieremo in particolare i polinomi a coefficienti nel dominio d'integrità $\mathbb{Z}$, e ancor di più quelli a coefficienti in uno dei seguenti campi: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$. Dunque cominciamo ad analizzare le proprietà dell'anello dei polinomi $\mathbb{K}[x]$ a coefficienti in un campo (d'ora innanzi, il simbolo $\mathbb{K}$ indicherà un generico campo).

Innanzitutto osserviamo che gli invertibili in $\mathbb{K}[x]$ sono tutte e solo le costanti diverse da 0 (Corollario 6.51), dunque, se è vero che l'essere dominio d'integrità di

$\mathcal{A}$ *passa* anche ad $\mathcal{A}[x]$, lo stesso non si può dire per quanto riguarda l'essere un campo.

Proviamo ora che $\mathbb{K}[x]$ *assomiglia molto da vicino* a $\mathbb{Z}$, mostrando che possiamo fare divisioni euclidee tra elementi di $\mathbb{K}[x]$ e calcolare il massimo comun divisore, proprio come nel caso degli interi. La somiglianza che notiamo nei risultati la ritroviamo anche nelle dimostrazioni, conseguenza del fatto che le proprietà che proveremo discendono dalla struttura comune tra $\mathbb{Z}$ e $\mathbb{K}[x]$.

Teorema 6.52 (Divisione con resto o euclidea per polinomi)**.** *Siano $f(x), g(x)$ in $\mathbb{K}[x]$ con $g(x) \neq 0$, allora esistono unici $q(x)$ e $r(x)$ in $\mathbb{K}[x]$ tali che:*

(1) $f(x) = q(x) \cdot g(x) + r(x)$.
(2) $deg(r(x)) < deg(g(x))$, *oppure* $r(x) = 0$.

Dimostrazione. **Esistenza.** Se $f(x)$ è il polinomio nullo, possiamo scrivere:

$$f(x) = \underbrace{0}_{q(x)} \cdot g(x) + \underbrace{0}_{r(x)}$$

Se $f(x)$ non è il polinomio nullo, procediamo per induzione sul grado n di $f(x)$.
Passo base. $n = 0$, ovvero $f(x)$ è una costante non nulla. Se anche $deg(g(x)) = 0$, allora:

$$f(x) = \underbrace{(f(x) \cdot g^{-1}(x))}_{q(x)} g(x) + \underbrace{0}_{r(x)}$$

Se $deg(g(x)) > 0$, si può scrivere:

$$f(x) = \underbrace{0}_{q(x)} \cdot g(x) + \underbrace{f(x)}_{r(x)}$$

In tutti e due i casi è rispettata la condizione richiesta sul grado (nel primo caso $r(x) = 0$, in questo secondo caso $deg(r(x)) = 0 < deg(g(x))$.
Passo induttivo. Supponiamo di aver dimostrato l'esistenza di $q(x)$ e $r(x)$ con le caratteristiche volute per ogni polinomio $f(x)$ in $\mathbb{K}[x]$ di grado minore di n, e dimostriamo l'esistenza di $q(x)$ e $r(x)$ con le medesime proprietà nel caso di $deg(f(x)) = n$.

Siano $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_n \neq 0$ e $g = \sum_{j=0}^{m} b_j x^j$ con $b_m \neq 0$. Anche in questo caso distinguiamo due casi. Se $m > n$, allora possiamo scrivere:

$$f(x) = \underbrace{0}_{q(x)} \cdot g(x) + \underbrace{f(x)}_{r(x)}$$

Se $n \geq m$, allora:

$$\frac{a_n x^n}{b_m x^m} = a_n \cdot b_m^{-1} \cdot x^{n-m}$$

Da questo segue che il polinomio $h(x) = -(a_n {b_m}^{-1} x^{n-m}) \cdot g(x)$ ha come termine di grado massimo $-a_n x^n$. Dunque, il polinomio somma $f_1(x) = f(x) + h(x)$ ha grado strettamente minore di n. Applichiamo l'ipotesi induttiva per trovare $q_1(x)$ e $r_1(x)$ tali che:

$$f_1(x) = q_1(x)g(x) + r_1(x) \quad deg(r_1(x)) < deg(g(x)) \text{ oppure } r_1(x) = 0$$

Quindi:

$$f(x) = \underbrace{(a_n b_m^{-1} x^{n-m} + q_1(x))}_{q(x)} \cdot g(x) + \underbrace{r_1(x)}_{r(x)}$$

Abbiamo trovato i due polinomi con le proprietà richieste, infatti $deg(r(x)) = deg(r_1(x)) < deg(g(x))$.
Unicità. Supponiamo $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$ con $r_i(x) = 0$ oppure $deg(r_i(x)) < deg(g(x))$ $(i \in \{1, 2\})$. Allora si ha:

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x) \tag{2.1}$$

Se $q_1(x) \neq q_2(x)$, essendo $\mathbb{K}[x]$ un dominio di integrità (Teorema 6.50) e $g(x) \neq 0$, anche $r_2(x) \neq r_1(x)$ e dunque possiamo determinare il grado dei polinomi presenti ai due membri dell'equazione 2.1:

$$deg[(q_1(x) - q_2(x))g(x)] = \underbrace{deg(q_1(x) - q_2(x))}_{\geq 0} + \underbrace{deg(g(x))}_{=m} \geq m$$
$$deg(r_2(x) - r_1(x)) \leq \max(\underbrace{deg(r_1)}_{<m}, \underbrace{deg(r_2)}_{<m}) < m$$

Dunque l'equazione 2.1 è soddisfatta se e solo se $q_1(x) = q_2(x)$, da cui segue $r_1(x) = r_2(x)$. □

Osservazione 6.53. È sempre istruttivo chiedersi dove sono state usate determinate ipotesi in un teorema. Ad esempio, per quanto riguarda il Teorema di divisione euclidea 6.52, ci chiediamo se l'ipotesi di avere un campo $\mathbb{K}$ come insieme dei coefficienti sia stata usata oppure no[5]. La risposta è sì: nel dimostrare l'esistenza di q, abbiamo usato il fatto che i coefficienti direttivi di $f(x)$ e $g(x)$, essendo elementi non nulli di un campo, hanno l'inverso.

Esercizio 6.54. *In $\mathbb{Q}[x]$, trovare quoziente e resto della divisione tra $p(x) = 2x^4 + x^3 + -x^2 + 1$ e $s(x) = 3x^2 + 1$.*

Svolgimento. Calcoliamo $q(x)$ e $r(x)$ per passi successivi, seguendo il metodo di dimostrazione del Teorema 6.52. Il punto di partenza è confrontare i termini di grado maggiore, indicando con a, b i coefficienti direttivi di $p(x)$ e $s(x)$ si ha:

$$p_1(x) = p(x) - (\tfrac{a}{b}x^{deg(p(x))-deg(s(x))}) \cdot s(x) =$$
$$= 2x^4 + x^3 + -x^2 + 1 - \tfrac{2}{3}x^2(3x^2 + 1) = x^3 - \tfrac{5}{3}x^2 + 1$$

Ripetiamo il procedimento con $p_1(x)$ al posto di $p(x)$:

$$p_2(x) = p_1(x) - \frac{1}{3}x(3x^2 + 1) = -\frac{5}{3}x^2 - \frac{1}{3}x + 1$$

Ripetiamo una terza volta il procedimento con $p_2(x)$ al posto di $p(x)$:

$$p_3(x) = p_2(x) + \frac{5}{9}(3x^2 + 1) = -\frac{1}{3}x + \frac{14}{9}$$

Essendo $p_3(x)$ di grado minore a $s(x)$ non possiamo più iterare il procedimento di divisione e $p_3(x)$ è il polinomio resto $r(x)$ che cercavamo, e abbiamo:

$$p(x) = p_1(x) + \left(\tfrac{2}{3}x^2\right) \cdot s(x) = p_2(x) + \left(\tfrac{1}{3}x + \tfrac{2}{3}x^2\right) \cdot s(x) =$$
$$= p_3(x) + \left(-\tfrac{5}{9} + \tfrac{1}{3}x + \tfrac{2}{3}x^2\right) \cdot s(x)$$

[5]Questo in generale non significa che l'ipotesi sia necessaria, potrebbero esistere delle dimostrazioni diverse che non usano tale ipotesi. Ad esempio, nei corsi di analisi usualmente si dimostra l'archimedeità di $\mathbb{R}$ usando l'assioma di continuità (è una immediata conseguenza), ma noi sappiamo (abbiamo dimostrato che $\mathbb{N}$ è archimedeo) che l'assioma di continuità non è condizione necessaria per l'archimedeità.

Riassumendo, abbiamo calcolato

$$p(x) = \left(-\frac{5}{9} + \frac{1}{3}x + \frac{2}{3}x^2\right)(3x^2+1) + \left(-\frac{1}{3}x + \frac{14}{9}\right)$$

Mostriamo ora come, con una forma grafica che ricorda quella della divisione in colonna tra numeri interi, l'algoritmo di divisione tra polinomi non nasconda particolari insidie.

Esempio 6.55. Supponiamo di voler calcolare quoziente e resto della divisione tra i due polinomi $x^6 - 1$ e $x^4 + x^3 + x^2 - 4x + 1$ in $\mathbb{Q}[x]$.

Come abbiamo visto nell'Esempio 6.54, bisogna confrontare i termini dei due polinomi di grado maggiore: tra $f(x) = x^6 - 1$ e $g(x) = x^4 + x^3 + x^2 - 4x + 1$ i termini di grado maggiore sono rispettivamente x^6 e x^4. Ci chiediamo per cosa dobbiamo moltiplicare x^4 per arrivare ad x^6, la risposta è ovviamente x^2. Allora moltiplichiamo $g(x)$ per x^2 e sottraiamo il risultato da $f(x)$. Quello che otteniamo è un polinomio di grado minore di 6 perché nella sottrazione $f(x) - x^2 \cdot g(x)$ si cancella il termine x^6. Continuiamo fino a che non otteniamo 0 o un polinomio di grado minore a $g(x)$ (cioè fino a che non otteniamo il resto della divisione tra $f(x)$ e $g(x)$). Questo è quello che abbiamo fatto nell'Esempio 6.54. Vediamo come aiutarci con una forma grafica che ricorda la divisione tra interi:

$$\begin{array}{cccccc|l} x^6 & & & & & -1 & \mid\ x^4+x^3+x^2-4x+1 \\ x^6 & +x^5 & +x^4 & -4x^3 & +x^2 & & \mid\ x^2 \\ & -x^5 & -x^4 & +4x^3 & -x^2 & -1 & \end{array}$$

A questo punto dobbiamo *confrontare* x^4 (il termine principale di $g(x)$) con $-x^5$ (il termine principale del polinomio ottenuto). Il secondo passaggio sarà quindi quello di moltiplicare $g(x)$ per $-x$:

$$\begin{array}{cccccc|l} x^6 & & & & & -1 & \mid\ x^4+x^3+x^2-4x+1 \\ x^6 & +x^5 & +x^4 & -4x^3 & +x^2 & & \mid\ x^2-x \\ & -x^5 & -x^4 & +4x^3 & -x^2 & -1 & \\ & -x^5 & -x^4 & -x^3 & +4x^2 & -x & \\ & & & 5x^3 & -5x^2 & +x & -1 \end{array}$$

Il polinomio ottenuto è di grado minore di $g(x)$, quindi abbiamo terminato l'algoritmo di divisione tra $f(x)$ e $g(x)$:

$$f(x) = g(x) \cdot \underbrace{(x^2 - x)}_{q(x)} + \underbrace{(5x^3 - 5x^2 + x - 1)}_{r(x)}$$

Come vedremo nel seguito, tra i domini di integrità possiamo fare ulteriori classificazioni considerando anelli con proprietà particolari. Anticipiamo qui la definizione di anello euclideo, soddisfatta da $\mathbb{K}[x]$ e $\mathbb{Z}$, per mostrare le proprietà di $\mathbb{K}[x]$ e $\mathbb{Z}$ che discendono esclusivamente dal loro essere anelli euclidei, ovvero quelle che possiamo chiamare proprietà strutturali degli anelli euclidei.

Definizione 6.56. Un dominio di integrità $\mathcal{A}$ si dice **anello euclideo** se esiste una funzione $d : \mathcal{A} \setminus \{0\} \longrightarrow \mathbb{N}$ (detta anche **funzione grado**) tale che:

(1) $\forall x, y \in \mathcal{A} \setminus \{0\}$ si ha $d(xy) \geq d(x)$.

(2) $\forall x \in \mathcal{A}$ e $\forall y \in A \setminus \{0\}$ esistono $q, r \in \mathcal{A}$ tali che:

$$x = qy + r \quad \text{con} \quad d(r) < d(y) \quad \text{oppure} \quad r = 0.$$

Esercizio 6.57. *Abbiamo dimostrato che $\mathbb{K}[x]$ è un anello euclideo con d data dalla funzione grado del polinomio. Dimostrare che anche l'anello $\mathbb{Z}$ è euclideo, con d data dalla funzione valore assoluto.*

L'importanza di aver *osservato* l'analogia strutturale tra $\mathbb{Z}$ e $\mathbb{K}[x]$ come anelli euclidei, sarà da subito abbastanza evidente. Daremo infatti delle definizioni molto simili a quelle già date per $\mathbb{Z}$ (per esempio di divisore, massimo comun divisore, etc.), in cui l'unica differenza sarà appunto il riferirsi a $\mathbb{K}[x]$ in luogo di $\mathbb{Z}$: tali definizioni potrebbero essere date per qualsiasi anello euclideo. Proprio per questo, potremo sfruttare molti dei risultati già provati in $\mathbb{Z}$ (tutti quelli che dipendono unicamente dalle proprietà di anello euclideo) senza la necessità di dimostrarli nuovamente.

Definizione 6.58. Dati $f(x)$ e $g(x)$ in $\mathbb{K}[x]$ si dice che $f(x)$ **divide** $g(x)$ (o equivalentemente $g(x)$ è un **multiplo** di $f(x)$) se e solo se esiste $h(x)$ in $\mathbb{K}[x]$ tale che $g(x) = f(x)h(x)$.

Corollario 6.59. *Siano $f(x)$ e $g(x)$ in $\mathbb{K}[x]$, $f(x)$ diverso da 0* **divide** *$g(x)$ se e solo se il resto della divisione euclidea di $g(x)$ con $f(x)$ è 0.*

Esercizio 6.60. *Dimostrare, sfruttando le proprietà del grado, che se $f(x)$ e $g(x)$ sono polinomi in $\mathbb{K}[x]$ diversi da 0, $f(x)$ divide $g(x)$ e $g(x)$ divide $f(x)$ allora esiste $k \in \mathbb{K}$ diverso da 0, tale che $g(x) = k \cdot f(x)$.*

Osservazione 6.61. Il suggerimento contenuto nel testo dell'Esercizio 6.60 segnala come la proprietà dimostrata sia strutturale degli anelli euclidei. In pratica dimostra che in un anello euclideo la divisibilità non è antisimmetrica, ma se due elementi diversi da 0 si dividono reciprocamente, allora si ottengono l'uno dall'altro per moltiplicazione per un invertibile (era quello che succede anche in $\mathbb{Z}$, dove gli invertibili sono 1 e -1).

Un concetto importante che lega i divisori di grado uno di un polinomio $f(x)$ alla funzione polinomiale $\tilde{f}(x)$ associata a $f(x)$ è quello di radice di $f(x)$.

Definizione 6.62. Un elemento a di $\mathbb{K}$ si dice **radice** in $\mathbb{K}$ del polinomio $f(x)$ se la funzione polinomiale $\tilde{f}(x)$ associata a $f(x)$ valutata in a è uguale a 0.

In pratica le radici di un polinomio $f(x)$ sono gli zeri della funzione polinomiale:

$$\tilde{f}(x) : \mathbb{K} \to \mathbb{K}$$

Esempio 6.63. 5 è una radice razionale del polinomio $f(x) = x^3 - 3x^2 - 50$ in quanto:

$$\tilde{f}(5) = 5^3 - 3 \cdot 5^2 - 50 = 125 - 75 - 50 = 0$$

Mentre 3 non è radice dello stesso polinomio infatti:

$$\tilde{f}(3) = 3^3 - 3 \cdot 3^2 - 50 = 27 - 27 - 50 = -50 \neq 0$$

Il Corollario 6.59, analogo del Corollario 4.20 per $\mathbb{Z}$, permette di dimostrare un semplice, ma importante (e solitamente molto conosciuto anche a livello di scuola secondaria superiore) risultato[6] che lega l'aver radici in $\mathbb{K}$ all'avere un divisore di grado 1 in $\mathbb{K}[x]$

[6] Lo abbiamo già usato, senza averlo ancora provato, nel Teorema 5.71 per dimostrare la ciclicità di $\mathbb{Z}/p\mathbb{Z}^*$.

Teorema 6.64 (Teorema di Ruffini)**.** *$a \in \mathbb{K}$ è una radice del polinomio $f(x) \in \mathbb{K}[x]$ se e solo se il polinomio $x - a$ divide $f(x)$.*

Dimostrazione. Il teorema di divisione per polinomi ci dice che esistono unici $q(x)$ e $r(x)$ in $\mathbb{K}[x]$, quoziente e resto della divisione di $f(x)$ per $x - a$. Essendo $r(x) = 0$ o $deg(r(x)) < deg(x - a) = 1$, si ha che il polinomio $r(x)$ è una costante, quindi possiamo indicarlo con r.

$$f(x) = q(x) \cdot (x - a) + r$$

Se $(x - a)$ divide $f(x)$, ovvero $r = 0$, allora $f(a) = q(a) \cdot (a - a) = 0$. Viceversa se a è una radice di $f(x)$, ovvero $f(a) = 0$, allora $0 = q(a) \cdot (a - a) + r = r$. □

Prima di proseguire con l'analogia strutturale tra $\mathbb{K}[x]$ e $\mathbb{Z}$, vogliamo mostrare alcune importanti conseguenze del Teorema di Ruffini relative al numero massimo di radici di un polinomio, ed a criteri per provare l'uguaglianza tra polinomi.

Corollario 6.65. *Un polinomio $f(x) \in \mathbb{K}[x] \setminus \{0\}$ di grado n, ha al più n radici distinte in $\mathbb{K}$.*

Dimostrazione. Procediamo per induzione sul grado n di $f(x)$.
Passo base. Se $n = 0$, allora $f(x)$ è una costante diversa da zero e quindi non ha radici.
Passo induttivo. Supponiamo il teorema vero per i polinomi di grado minore di n e sia $deg(f(x)) = n$. Se $f(x)$ non ha radici in $\mathbb{K}$, non c'è niente da dimostrare perché $n \geq 0$. Se $f(x)$ ha almeno una radice $a \in \mathbb{K}$, per il teorema di Ruffini si ha che esiste $q(x) \in \mathbb{K}[x]$ tale che $f(x) = q(x) \cdot (x - a)$. Per le proprietà della funzione grado sul prodotto di polinomi $deg(q(x)) = n - 1$. Dunque, per ipotesi induttiva, $q(x)$ ha al più $n - 1$ radici distinte in $\mathbb{K}$. Per concludere mostriamo che ogni radice b in $\mathbb{K}$ di $f(x)$, diversa da a, è radice di $q(x)$. Avremo dunque che le radici di $f(x)$ diverse da a sono tutte tra le al più $n - 1$ radici di $q(x)$, e dunque $f(x)$ ha al più n radici.

Se $b \neq a$ è radice di $f(x)$, allora $0 = f(b) = q(b) \cdot (a - b)$. Essendo $b \neq a$, $a - b$ è diverso da zero e dunque deve essere ($\mathbb{K}$ è un campo, ed in particolare quindi un dominio d'integrità) $q(b) = 0$. □

Il Corollario 6.65 ci permette di enunciare il risultato noto come principio d'identità dei polinomi. Tale risultato, per $\mathbb{K}$ infinito, identifica i polinomi in $\mathbb{K}[x]$ e le funzioni polinomiali associate.

Teorema 6.66 (Principio d'identità dei polinomi)**.** *Sia $\mathbb{K}$ un campo infinito e $f(x)$ e $g(x)$ polinomi in $\mathbb{K}[x]$. Le funzioni polinomiali:*

$$\widetilde{f} : a \longrightarrow f(a) \quad e \quad \widetilde{g} : a \longrightarrow g(a)$$

sono uguali se e solo se $f(x) = g(x)$ (cioè la funzione che associa al polinomio la funzione polinomiale è iniettiva).

Dimostrazione. Se i due polinomi $f(x)$ e $g(x)$ sono uguali, cioè per definizione hanno la stessa espressione formale, allora è evidente che la funzione polinomiale associata è la stessa.

Viceversa se $\widetilde{f}(x) = \widetilde{g}(x)$ per qualunque x in $\mathbb{K}$, allora la funzione polinomiale $\widetilde{f}(x) - \widetilde{g}(x)$ è la funzione identicamente nulla, che associa ad ogni elemento di $\mathbb{K}$ lo zero: cioè tutti gli elementi di $\mathbb{K}$ sono radici del polinomio $(f - g)(x)$. Ma dal

corollario 6.65 segue che se $(f-g)(x)$ non è nullo, può avere al più n radici. Deve dunque essere $(f-g)(x)=0$, cioè tutti i coefficienti di $(f-g)(x)$ sono nulli, ovvero $f(x)$ e $g(x)$ hanno gli stessi coefficienti. □

Abbiamo già osservato che in generale, ovvero senza l'ipotesi che $\mathbb{K}$ sia infinito, l'enunciato del principio d'identità di polinomi è falso: due polinomi diversi possono definire la stessa funzione su $\mathbb{K}$ ($x^p - x$ e il polinomio nullo definiscono la stessa funzione in $\mathbb{Z}/p\mathbb{Z}[x]$). Effettivamente nella dimostrazione del principio d'identità abbiamo usato l'infinità di $\mathbb{K}$: se il polinomio $(f-g)(x)$ ha infinite radici, il numero delle radici è maggiore di qualsiasi n finito.

Dal corollario 6.65 segue però un criterio per l'uguaglianza tra polinomi valido per polinomi a coefficienti in un campo $\mathbb{K}$, a prescindere dal fatto che sia finito o infinito.

Corollario 6.67. *Siano $f(x), g(x) \in \mathbb{K}[x]$ con $m \geq max(deg(g(x)), deg(f(x)))$. Se esistono $m+1$ elementi distinti k_i di $\mathbb{K}$ tali che $f(k_i) = g(k_i)$, allora i polinomi $f(x)$ e $g(x)$ sono uguali.*

Dimostrazione. Consideriamo il polinomio $h(x) = f(x) - g(x)$. Dalle proprietà del grado abbiamo che $h(x) = 0$ oppure $deg(h(x)) \leq m$. Mostriamo che $h(x)$ necessariamente è il polinomio nullo.

Se $h(x)$ non fosse il polinomio nullo, potrebbe avere al più m radici distinte in $\mathbb{K}$, ma per ipotesi $h(x)$ ha almeno $m+1$ radici, infatti $h(k_i) = 0$ per ogni k_i. Perciò il polinomio $h(x)$ deve necessariamente essere il polinomio nullo. □

Proseguiamo il parallelo tra $\mathbb{K}[x]$ e $\mathbb{Z}$ definendo, dati due polinomi non entrambi nulli $f(x)$ e $g(x)$ di $\mathbb{K}[x]$, il massimo comun divisore $(f(x), g(x))$, e conseguentemente la coprimalità tra due polinomi.

Definizione 6.68. Siano $f(x)$ e $g(x)$ in $\mathbb{K}[x]$ non entrambi nulli, $d(x)$ in $\mathbb{K}[x]$ si dice **un massimo comun divisore** di $f(x)$ e $g(x)$, e si indica con $(f(x), g(x))$, se:

- $d(x)$ divide sia $f(x)$ che $g(x)$.
- Per ogni $c(x)$ in $\mathbb{K}[x]$ che divide sia $f(x)$ che $g(x)$, si ha che $c(x)$ divide $d(x)$.

Si dimostrano, analogamente a $\mathbb{Z}$, tutti i risultati relativi al massimo comun divisore (stessa cosa per il minimo comun multiplo tra due polinomi). Ad esempio, dall'Esercizio 6.60 abbiamo, come per $\mathbb{Z}$, che il massimo comun divisore in $\mathbb{K}[x]$ è unico a meno di moltiplicazione per invertibile (ovvero costante diversa da zero). Possiamo dunque stabilire per convenzione che, tra tutti i polinomi che sono massimi comun divisori di $f(x)$ e $g(x)$ secondo la Definizione 6.68, chiamiamo **il** massimo comun divisore di $f(x)$ e $g(x)$ l'unico polinomio monico[7].

Definizione 6.69. Due polinomi $f(x)$ e $g(x)$ non entrambi nulli si dicono **relativamente primi** o anche **coprimi** se $(f(x), g(x)) = 1$.

Teorema 6.70. *Dati $f(x), g(x)$ non entrambi nulli in $\mathbb{K}[x]$, esiste il massimo comun divisore tra $f(x)$ e $g(x)$.*

[7]Che ce ne sia uno solo è evidente: moltiplicando per una costante diversa da 0 si cambia il coefficiente direttivo.

Teorema 6.71 (Lemma di Bézout per polinomi)**.** *Dati $f(x)$ e $g(x)$ di $\mathbb{K}[x]$ non entrambi nulli, esistono $a(x), b(x) \in \mathbb{K}[x]$ tali che:*

$$a(x) \cdot f(x) + b(x) \cdot g(x) = (f(x), g(x))$$

Citiamo infine l'analogo del teorema sulle funzioni diofantee tra numeri interi:

Proposizione 6.72. *Dati $f(x), g(x) \in \mathbb{K}[x]$ non entrambi nulli e $h(x) \in \mathbb{K}[x]$, esistono $t(x), s(x) \in \mathbb{K}[x]$ tali che:*

$$f(x) \cdot t(x) + g(x) \cdot s(x) = h(x)$$

se e solo se il massimo comun divisore tra $f(x)$ e $g(x)$ divide $h(x)$.

Esercizio 6.73. *Provare a dimostrare l'esistenza del massimo comun divisore tra due polinomi non entrambi nulli, il lemma di Bézout, e il teorema di esistenza di soluzioni di equazioni diofantee, ripercorrendo quanto fatto in $\mathbb{Z}$.*

Per quanto riguarda l'analogia degli algoritmi utilizzati in $\mathbb{Z}$, basta osservare che la dimostrazione del Teorema di divisione euclidea 6.52, ricalcando quella in $\mathbb{Z}$, fornisce la stessa procedura (algoritmo euclideo) per calcolare il massimo comun divisore tra due polinomi, e anche le stesse giustificazioni al fatto che l'algoritmo termini e restituisca proprio il massimo comun divisore.

Infatti, quel che faremo dati $f(x)$ e $g(x)$ in $\mathbb{K}[x]$ di cui vogliamo calcolare il massimo comun divisore $(f(x), g(x))$, è effettuare una serie di divisioni successive. La prima divisione è quella tra il polinomio di grado maggiore, se c'è, e quello di grado minore (se i due polinomi hanno lo stesso grado la scelta di quale sia il divisore è ininfluente).

$$f(x) = q_1(x) \cdot g(x) + r_1(x)$$

Se $r_1(x) = 0$ allora il massimo comun divisore tra $f(x)$ e $g(x)$ è $g(x)$, altrimenti procediamo con il secondo passo dividendo $g(x)$ per $r_1(x)$. Se $r_2(x) = 0$, allora $(f(x), g(x)) = r_1(x)$, altrimenti iteriamo il procedimento dividendo $r_i(x)$ per $r_{i+1}(x)$, finché non si trova $r_j(x) = 0$. In tal caso $(f(x), g(x)) = r_{j-1}(x)$.

Che tale procedimento termini sempre restituendo proprio $(f(x), g(x))$, è conseguenza del fatto che $\mathbb{K}[x]$ è un anello euclideo (ripercorrere le giustificazioni di questi fatti nel caso dell'anello $\mathbb{Z}$ e osservare che gli stessi passaggi logici possono essere fatti nel caso $\mathbb{K}[x]$, e, più in generale, in qualsiasi anello euclideo con una determinata funzione grado).

Analogamente, per calcolare i polinomi dell'algoritmo di Bézout, *risaliremo* l'algoritmo euclideo.

Esempio 6.74. Supponiamo di voler calcolare il massimo comun divisore in $\mathbb{Q}[x]$ tra $g(x) = x^9 - 1$ e $f(x) = x^{11} - 1$.

Effettuiamo dunque la divisione tra $f(x)$ e $g(x)$, trovando $q_1(x)$ e $r_1(x)$ tali che:

$$\begin{array}{llll} x^{11} & & -1 & \mid \; x^9 - 1 \\ x^{11} & -x^2 & & \mid \; x^2 \\ & x^2 & -1 & \end{array}$$

Dunque il primo passo dell'algoritmo di Euclide è:

$$f(x) = g(x) \cdot \underbrace{x^2}_{q_1(x)} + \underbrace{(x^2 - 1)}_{r_1(x)}$$

A questo punto dividiamo $g(x)$ per $r_1(x)$:

$$\begin{array}{cccccc|l}
x^9 & & & & & -1 & x^2-1 \\
x^9 & -x^7 & & & & & x^7+x^5+x^3+x \\
 & x^7 & & & & -1 & \\
 & x^7 & -x^5 & & & & \\
 & & x^5 & & & -1 & \\
 & & x^5 & -x^3 & & & \\
 & & & x^3 & & -1 & \\
 & & & x^3 & -x & & \\
 & & & & x & -1 &
\end{array}$$

Il secondo passo dell'algoritmo di Euclide è dunque dato da:

$$g(x) = r_1(x) \cdot \underbrace{(x^7+x^5+x^3+x)}_{q_2(x)} + \underbrace{x-1}_{r_2(x)}$$

L'algorimo continua dividendo $r_1(x)$ per $r_2(x)$ ed è evidente (prodotto notevole), senza fare la divisione, che il terzo passo dell'algoritmo di Euclide sarà:

$$\underbrace{(x^2-1)}_{r_1(x)} = \underbrace{(x-1)}_{r_2(x)} \cdot \underbrace{(x+1)}_{q_2(x)} + \underbrace{0}_{r_3(x)}$$

Perciò l'algoritmo è terminato e un massimo comun divisore tra $f(x)$ e $g(x)$ è l'ultimo resto non zero, ovvero $r_2(x) = x-1$.
Abbiamo trovato il massimo comun divisore (monico) tra $f(x)$ e $g(x)$, vogliamo ora determinare due polinomi $t(x)$ e $h(x)$ in $\mathbb{Q}[x]$ tali che:

$$f(x) \cdot t(x) + g(x) \cdot h(x) = x-1$$

e poi un[8] minimo comun multiplo tra $f(x)$ e $g(x)$, ovvero un polinomio $m(x)$ che è multiplo sia di $f(x)$ che di $g(x)$ e tale che ogni polinomio che è multiplo comune di $f(x)$ e $g(x)$ ha grado maggiore o uguale di $m(x)$.

Per trovare $t(x)$ e $h(x)$ possiamo utilizzare l'algoritmo di Euclide esteso, oppure, come faremo in questo caso, scrivere i tre passi che son stati necessari dell'algoritmo di Euclide e *risalirli*.

(1) $f(x) = g(x) \cdot \underbrace{x^2}_{q_1(x)} + \underbrace{(x^2-1)}_{r_1(x)}$

(2) $g(x) = r_1(x) \cdot \underbrace{(x^7+x^5+x^3+x)}_{q_2(x)} + \underbrace{x-1}_{r_2(x)}$

(3) $\underbrace{(x^2-1)}_{r_1(x)} = \underbrace{(x-1)}_{r_2(x)} \cdot \underbrace{(x+1)}_{q_2(x)} + \underbrace{0}_{r_3(x)}$

Dal primo passo si trova che:

$$f(x) - g(x) \cdot q_1(x) = r_1(x)$$

E dal secondo passo si trova che:

$$r_2(x) = g(x) - r_1(x) \cdot q_2(x)$$

[8] L'uso dell'articolo indeterminativo ha la stessa spiegazione di quello usato per il massimo comun divisore. È facile provare che se $m(x)$ è un minimo comun multiplo tra $f(x)$ e $g(x)$, allora anche ogni altro polinomio ottenuto dalla moltiplicazione di $m(x)$ per una costante diversa da zero lo è. Anche in questo caso diremo **il** minimo comun multiplo per indicare quello monico.

Sostituendo $r_1(x)$ in questa seconda uguaglianza si trova che:

$$r_2(x) = g(x) - (f(x) - g(x) \cdot q_1(x)) \cdot q_2(x)$$

ovvero:

$$r_2(x) = g(x) \cdot \underbrace{(1 + q_1(x) \cdot q_2(x))}_{t(x)} + f(x) \cdot \underbrace{(-q_2(x))}_{h(x)}$$

Per trovare un minimo comun multiplo tra $f(x)$ e $g(x)$, si procede come con i numeri interi, ovvero si fattorizzano $f(x)$ e $g(x)$ a partire dalla divisione per il massimo comun divisore. Otteniamo:

$$g(x) = (x-1) \cdot \underbrace{(x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)}_{s(x)}$$

e

$$f(x) = (x-1) \cdot \underbrace{(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)}_{w(x)}$$

Sappiamo inoltre che in $\mathbb{Q}[x]$ i due fattori $s(x)$ e $w(x)$ sono primi tra loro (altrimenti $(x-1)$ non sarebbe il massimo comun divisore tra $f(x)$ e $g(x)$ perché esisterebbe un fattore comune di grado maggiore). Perciò un minimo comun multiplo tra $f(x)$ e $g(x)$ è $(x-1) \cdot s(x) \cdot w(x)$.

Chiudiamo il paragrafo, introducendo il concetto di molteplicità di radice di un polinomio.

Definizione 6.75. Una radice α si dice di **molteplicità** m se

$$(x-\alpha)^m | f(x) \quad \text{e} \quad (x-\alpha)^{m+1} \text{ non divide } f(x)$$

Una radice si dice **semplice** se è di molteplicità 1, altrimenti si dice **multipla**.

Indichiamo con $f'(x)$ il polinomio che ha come funzione associata la derivata di $f(x)$: per esempio se $f(x) = x^4 - 3x + 1$ abbiamo che il polinomio $f'(x)$ è $4x^3 - 3$. Una volta individuata una radice α di un polinomio $f(x) \in \mathbb{K}[x]$, valutando $f'(x)$ in α abbiamo un criterio per stabilire se α è radice multipla o semplice di $f(x)$.

Proposizione 6.76. *Sia $f(x) \in \mathbb{K}[x]$ non nullo e α una radice di $f(x)$. α è una radice multipla se e solo se, indicato con $f'(x)$ il polinomio derivata di $f(x)$, si ha $f(\alpha) = f'(\alpha) = 0$.*

Dimostrazione. Supponiamo che α sia una radice di $f(x)$ di molteplicità m. Allora possiamo scrivere $f(x) = (x-\alpha)^m g(x)$, con $g(\alpha) \neq 0$ altrimenti α avrebbe molteplicità maggiore di m.

- Se $m = 1$, cioè α è radice semplice, $f'(x) = (x-\alpha)g'(x) + g(x)$ da cui:
$$f'(\alpha) = g(\alpha) \neq 0$$
- Se $m > 1$, cioè α è radice multipla, si ha:
$$f'(x) = m(x-\alpha)^{m-1} g(x) + g'(x)(x-\alpha)^m$$
Dunque il polinomio $f'(x)$ valutato in α è:
$$f'(\alpha) = m(\alpha-\alpha)^{m-1} g(\alpha) + g'(\alpha)(\alpha-\alpha)^m = 0$$

□

La dimostrazione precedente ci fornisce anche lo spunto per un'osservazione. Indichiamo con $h(x)$ il massimo comun divisore tra un polinomio $f(x)$ e la sua derivata $f'(x)$. Se α è una radice di $f(x)$ di molteplicità m, allora α è una radice di $h(x)$ di molteplicità $m-1$. Perciò il polinomio $\dfrac{f(x)}{h(x)}$ ha le stesse radici di $f(x)$, tutte con molteplicità 1.

Definizione 6.77. Un polinomio $f(x)$ senza radici multiple si dice **libero da quadrati**.

È abbastanza facile dimostrare che il limite delle n radici per un polinomio $f(x) \in \mathbb{K}[x]$ di grado n, provato nel Corollario 6.65, sussiste anche nel caso di contare le radici con la loro molteplicità (cioè se 2 è una radice di molteplicità 3 di $f(x)$ la contiamo 3 volte).

Esercizio 6.78. *Dimostrare che se $f(x) \in \mathbb{K} \setminus \{0\}$ di grado n, allora il numero di radici di $f(x)$ in $\mathbb{K}$, contate con la loro molteplicità, è al più n.*

3. Fattorizzazione in $\mathbb{K}[x]$

Per parlare di fattorizzazione definiamo, come in $\mathbb{Z}$, elemento primo e invertibile nel caso dell'anello $\mathbb{K}[x]$.

Definizione 6.79. Un polinomio $f(x)$ in $\mathbb{K}[x]$ di grado maggiore di zero si dice **irriducibile** se $f(x) = g(x) \cdot h(x)$ implica che $g(x)$ o $h(x)$ è una costante.

Osservazione 6.80. Si potrebbe qui pensare che il parallelo con $\mathbb{Z}$ *vacilli* dato che definiamo l'irriducibilità escludendo le costanti. In realtà osserviamo che l'insieme delle costanti non è altro che l'insieme degli elementi invertibili di $\mathbb{K}[x]$ con *aggiunto* l'elemento 0. La stessa esclusione l'avevamo fatta in $\mathbb{Z}$, dove non consideravamo 0 e ± 1 (che sono appunto gli invertibili di $\mathbb{Z}$).

Esercizio 6.81. *Dimostrare che l'insieme $Irr_{\mathbb{K}[x]}$ dei polinomi irriducibili di $\mathbb{K}[x]$ è chiuso per moltiplicazione per costanti diverse da zero. Ovvero che se $f(x) \in Irr_{\mathbb{K}[x]}$, allora $k \cdot f(x) \in Irr_{\mathbb{K}[x]}$ per ogni $k \in \mathbb{K}$.*

Definizione 6.82. Un polinomio $f(x)$ in $\mathbb{K}[x]$ di grado maggiore di zero si dice **primo** se $f(x)$ divide $g(x) \cdot h(x)$ implica che $f(x)$ divide $g(x)$ o $f(x)$ divide $h(x)$.

La struttura di anello euclideo di $\mathbb{K}[x]$ ci permette di avere, con la stessa struttura di dimostrazione usata in $\mathbb{Z}$ (e che quindi non ripeteremo), i seguenti due importanti teoremi.

Teorema 6.83. *Un polinomio $f(x) \in \mathbb{K}[x]$ è primo se e solo se è irriducibile.*

Teorema 6.84. *Ogni polinomio $f(x) \in \mathbb{K}[x]$ di grado maggiore di zero si scrive in maniera unica (a meno dell'ordine e di moltiplicazione per invertibili) come prodotto di elementi irriducibili.*

Osservazione 6.85. Una conseguenza del teorema sul grado del prodotto di due polinomi è che i polinomi di grado uno sono irriducibili in $\mathbb{K}[x]$. Infatti, se $f(x)$ è di grado uno ed è uguale al prodotto di $g(x)$ per $h(x)$, allora:

$$1 = deg(f(x)) = deg(g(x) \cdot h(x)) = deg(g(x)) + deg(h(x))$$

Ne segue che uno tra $g(x)$ e $h(x)$ deve avere grado zero e dunque essere una costante.

Osservazione 6.86. Nel teorema di fattorizzazione abbiamo parlato di unicità meno dell'ordine e di moltiplicazione per invertibile. Ad esempio le fattorizzazioni in irriducibili (siamo sicuri che lo siano per l'Osservazione 6.85) $x(x+3)$ ed $\frac{1}{2}x(2x+6)$ del polinomio x^2+3x di $\mathbb{R}[x]$, sono considerate non distinte. Osserviamo che anche in questo caso vale il parallelo con $\mathbb{Z}$. In quel caso avevamo risolto il problema considerando fattorizzazioni in $\mathbb{N}$ (in $\mathbb{Z}$ gli invertibili sono 1 e -1).

Spesso si equivoca l'enunciato del Teorema di Ruffini 6.64, identificando il non aver radici con l'essere irriducibile. In realtà il teorema mostra l'equivalenza tra il non aver radici e non avere fattori di grado 1, ma un polinomio senza radici potrebbe essere prodotto di fattori irriducibili di grado maggiore di 1, e dunque riducibile.

Il polinomio $f(x) = x^4 - 4$ in $\mathbb{Q}(x)$ non ha radici (nessun numero razionale elevato alla quarta è uguale a 4), ma si può scrivere come il prodotto di (x^2-2) e (x^2+2). Tra l'altro, in questo caso, il teorema di Ruffini ci dice che $(x^2-2)\cdot(x^2+2)$ è proprio la fattorizzazione in irriducibili di $f(x)$ in $\mathbb{Q}[x]$, in quanto i due polinomi di secondo grado non si possono ulteriormente ridurre non avendo $f(x)$ radici (e dunque fattori di grado 1).

Possiamo generalizzare quest'ultima osservazione e, dalle proprietà del grado del prodotto tra polinomi, identificare dei casi in cui il non aver radici e l'essere irriducibile coincide.

Corollario 6.87. *Se $f(x) \in \mathbb{K}[x]$ ha grado 2 o 3, allora è irriducibile se e solo se non ha radici in $\mathbb{K}$.*

Dimostrazione. $\Rightarrow$) Se $f(x)$ ha una radice in $\mathbb{K}$, dal teorema di Ruffini segue che ha un fattore di grado 1 e quindi è riducibile.

$\Leftarrow$) Se $f(x) = g(x) \cdot h(x)$ con $g(x)$ e $h(x)$ di grado m e n entrambi maggiori di 0, allora il grado di $f(x)$ è uguale a $m+n$. Per avere $m+n = 2$ o $m+n = 3$ con m, n numeri naturali positivi, uno tra m e n deve essere uguale a 1. Ovvero $f(x)$ ha, per il teorema di Ruffini, una radice. □

Discutiamo adesso la fattorizzazione in irriducibili in $\mathbb{K}[x]$ al variare di $\mathbb{K}$ nei campi $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$.

Cominciamo enunciando, per ora senza dimostrarlo, quello che viene chiamato teorema fondamentale dell'algebra, riguardante le radici complesse di un polinomio in $\mathbb{C}[x]$.

Teorema 6.88 (Teorema fondamentale dell'algebra)**.** *Ogni polinomio $f(x)$ a coefficienti in $\mathbb{C}$ di grado maggiore di zero ammette almeno una radice in $\mathbb{C}$.*

Una prima conseguenza del teorema fondamentale dell'algebra è la generalizzazione del risultato che abbiamo trovato nell'Esempio 6.74 facendo *i conti a mano*.

Esercizio 6.89. *Dimostrare che, dati $m, n \in \mathbb{N}^+$, e indicando (m, n) con d, si ha in $\mathbb{Q}[x]$:*

$$(x^n - 1, x^m - 1) = x^d - 1$$

Svolgimento. Indichiamo $(x^m - 1, x^n - 1)$ con $g(x)$, e osserviamo che:

$$\begin{array}{l} d|m \\ d|n \end{array} \rightarrow \begin{array}{l} m = dm_1 \\ n = dn_1 \end{array} \rightarrow \begin{array}{l} x^m - 1 = (x^d)^{m_1} - 1 = (x^d - 1)(\sum_{j=0}^{m_1-1} x^{j\cdot d}) \\ x^n - 1 = (x^d)^{n_1} - 1 = (x^d - 1)(\sum_{j=0}^{n_1-1} x^{j\cdot d}) \end{array}$$

Cioè $x^d - 1$ è un divisore comune di $x^m - 1$ e $x^n - 1$, quindi $x^d - 1 | g(x)$.

Sia $\alpha \in \mathbb{C}$ una radice di $g(x)$, allora $(x-\alpha)|g(x)$, e inoltre:

$$\begin{array}{l} \alpha^m - 1 = 0 \\ \alpha^n - 1 = 0 \end{array} \quad \rightarrow \quad \begin{array}{l} \alpha^m = 1 \\ \alpha^n = 1 \end{array}$$

Quindi l'ordine dell'elemento α nel gruppo moltiplicativo $(\Xi, \cdot)$ (Esempio 5.12) divide sia m che n, e in particolare divide d. Di conseguenza $\alpha^d - 1 = 0$, cioè $x - \alpha$ divide $x^d - 1$. Osserviamo inoltre che:

$$(x^m - 1)' = mx^{m-1} \quad \text{e} \quad (x^n - 1)' = nx^{n-1}$$

Dunque i due polinomi non hanno fattori multipli. Allora anche $g(x)$ non ha fattori multipli. Concludendo:

- tutte le radici complesse di $g(x)$ sono radici anche di $x^d - 1$.
- $g(x)$ non ha fattori multipli.

Allora $g(x)|(x^d - 1)$. Dunque $g(x) = x^d - 1$.

Dal teorema fondamentale dell'algebra segue la caratterizzazione degli irriducibili in $\mathbb{C}[x]$ e delle fattorizzazioni in irriducibili.

Corollario 6.90. *Un polinomio $f(x)$ in $\mathbb{C}[x]$ è irriducibile se e solo se è di grado 1.*

Dimostrazione. Una implicazione sappiamo già che è vera in qualsiasi $\mathbb{K}[x]$ (Osservazione 6.85), e dunque in particolare in $\mathbb{C}[x]$. Per il viceversa, se $f(x)$ irriducibile fosse di grado n maggiore di 1, allora esisterebbe, per il Teorema 6.88, una radice α in $\mathbb{C}$ di $f(x)$. Ovvero per il teorema di Ruffini e le proprietà del grado, esisterebbe $g(x)$ di grado $n-1$:

$$f(x) = (x - \alpha)g(x)$$

Assurdo, perché essendo $n - 1 > 0$ questa sarebbe una fattorizzazione di $f(x)$ con due polinomi non costanti. □

Corollario 6.91. *Ogni polinomio $f(x) \in \mathbb{C}[x]$ di grado $n > 0$ è il prodotto di n fattori di primo grado in $\mathbb{C}[x]$.*

Il teorema fondamentale dell'algebra e le sue conseguenze ci dicono anche che possiamo, per polinomi $f(x)$ in $\mathbb{C}[x]$, precisare la stima sul numero di radici contate con la loro molteplicità in $\mathbb{C}$ (dal corollario 6.65, sappiamo essere nel caso generale minori o uguali di n).

Corollario 6.92. *Le radici di un polinomio $f(x) \in \mathbb{C}[x]$, con $deg(f) = n$, contate con la loro molteplicità sono esattamente n.*

La discussione riguardo alla fattorizzazione in $\mathbb{R}[x]$ è legata in qualche modo al teorema fondamentale dell'algebra. In particolare è utile conoscere la funzione coniugio da $\mathbb{C}$ in $\mathbb{C}$, in quanto vedremo che le radici complesse di un polinomio sono *legate* da questa funzione (e d'altra parte osserviamo come un polinomio in $\mathbb{R}[x]$ può essere sempre visto come polinomio in $\mathbb{C}[x]$, dato che $\mathbb{R} \subset \mathbb{C}$).

Definizione 6.93. Chiamiamo funzione **coniugio**, la funzione da $\mathbb{C}$ in $\mathbb{C}$ che al numero complesso $a + ib$ associa $\overline{a + ib} = a - ib$.

Mostriamo alcune delle proprietà della funzione coniugio

(1) I punti fissi della funzione, cioè gli $\alpha \in \mathbb{C}$ tali che $\overline{\alpha} = \alpha$, sono i numeri reali. Infatti, se $\alpha = a + ib$ allora

$$\overline{\alpha} = \alpha \leftrightarrow a + ib = a - ib \leftrightarrow 2ib = 0 \leftrightarrow b = 0 \leftrightarrow \alpha \in \mathbb{R}$$

(2) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$. Infatti, se $\beta = c + id$ allora:

$$\overline{(a + ib) + (c + id)} = \overline{(a + c) + i(b + d)} = a + c - i(b + d) = a - ib + c - id$$

cioè

$$\overline{(a + ib) + (c + id)} = \overline{a + ib} + \overline{c + id}$$

(3) $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$. Infatti:

$$\overline{\alpha \cdot \beta} = \overline{(ac - bd) + i(bc + ad)} = (ac - bd) - i(bc + ad)$$

e

$$\overline{a + ib} \cdot \overline{c + id} = (a - ib) \cdot (c - id) = (ac - bd) - i(bc + ad)$$

Proposizione 6.94. *Sia $f(x) \in \mathbb{R}[x] \subset \mathbb{C}[x]$ e sia $\alpha \in \mathbb{C}$ una radice di f. Allora anche $\overline{\alpha}$ è una radice di f.*

Dimostrazione. Sia $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in \mathbb{R}$. Per ipotesi:

$$0 = f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$$

quindi:

$$\overline{0} = \overline{\sum_{i=0}^{n} a_i \alpha^i} = \sum_{i=0}^{n} \overline{a_i \alpha^i} = \sum_{i=0}^{n} a_i \overline{\alpha^i} = \sum_{i=0}^{n} a_i \overline{\alpha}^i$$

Cioè $f(\overline{\alpha}) = \overline{0} = 0$. □

La Proposizione 6.94 permette la caratterizzazione degli irriducibili e delle fattorizzazioni in irriducibili in $\mathbb{R}[x]$.

Consideriamo $f(x) \in \mathbb{R}[x]$ di grado n e, pensandolo come polinomio in $\mathbb{C}[x]$, fattorizziamolo in irriducibili in $\mathbb{C}[x]$. Sappiamo che in $\mathbb{C}[x]$ tutti i fattori irriducibili sono di grado uno (Corollario 6.90), perciò:

$$f(x) = c_n \prod_{i=1}^{n} (x - \alpha_i) \quad c_n, \alpha_i \in \mathbb{C}$$

Distinguiamo le radici α_i di $f(x)$ tra quelle che sono reali, che indicheremo con γ_i, e quelle che stanno in $\mathbb{C} \setminus \mathbb{R}$, che indicheremo con β_j. Dalla Proposizione 6.94 segue che le radici β_j sono in numero pari, diciamo $2k$ (dove k al limite può essere 0, così come 0 può essere il numero di radici reali se $2k = n$). Riscriviamo quindi $f(x)$ come:

$$f(x) = c_n \prod_{i=1}^{n-2k} (x - \gamma_i) \prod_{j=1}^{k} \underbrace{(x - \beta_j)(x - \overline{\beta}_j)}_{x^2 - 2Re(\beta_j)x + |\beta_i|^2 \in \mathbb{R}[x]}$$

Questa riscrittura di $f(x)$ ci dice che $f(x)$ è fattorizzabile in $\mathbb{R}[x]$ come prodotto di fattori di grado uno (come osservato un fattore di grado uno è sempre irriducibile) e di grado due anch'essi irriducibili in quanto non hanno radici reali. Per quanto appena detto, conoscendo le radici complesse di $f(x)$ riusciamo a scriverne una fattorizzazione anche in $\mathbb{R}[x]$.

Dato un polinomio $f(x) = ax^2 + bx + c$ in $\mathbb{R}[x]$ di grado 2, sappiamo dalle scuole superiori che $f(x)$ ha radici in $\mathbb{R}$ se e solo se $\Delta_f = \sqrt{b^2 - 4ac}$ è maggiore o uguale a 0. Abbiamo dunque, come per $\mathbb{C}[x]$, una caratterizzazione degli irriducibili e delle fattorizzazioni in irriducibili in $\mathbb{R}[x]$.

Proposizione 6.95. *Un polinomio $f(x) \in \mathbb{R}[x]$ è irriducibile se e solo se $deg(f(x)) = 1$ oppure $deg(f(x)) = 2$ e $\Delta_f < 0$.*

Siamo riusciti a caratterizzare gli irriducibili in $\mathbb{R}[x]$ e $\mathbb{C}[x]$ in base al grado del polinomio, la stessa cosa non è possibile in $\mathbb{Q}[x]$ in quanto, per ogni $n \in \mathbb{N}$, si trovano elementi irriducibili di grado n.

Proposizione 6.96. *Per ogni $n \in \mathbb{N}$, esiste un polinomio $f(x) \in \mathbb{Q}[x]$ di grado n irriducibile.*

Dimostrazione. Consideriamo il polinomio $f(x) = x^n - 2$, vogliamo mostrare che, per ogni n, tale polinomio è irriducibile in $\mathbb{Q}[x]$. Considerato come polinomio in $\mathbb{C}[x]$, $f(x)$ è fattorizzabile nel modo seguente:

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

dove gli α_i hanno modulo uguale a $\sqrt[n]{2}$ e argomenti $\theta_i = \frac{2\pi i}{n}$.

Avendo in mente questa fattorizzazione, supponiamo che $f(x)$ in $\mathbb{Q}[x]$ sia uguale a $g(x) \cdot h(x)$ con $deg(g(x)) = l$, $deg(h(x)) = m$ e $m + l = n$.

Distinguiamo, usando indici diversi, le radici complesse di $f(x)$ che sono radici di $g(x)$ da quelle che sono radici di $h(x)$:

$$\{\alpha_1, \ldots, \alpha_n\} = \{\alpha_{i_1}, \ldots, \alpha_{i_l}, \alpha_{t_1}, \ldots, \alpha_{t_m}\}$$

Potrebbe anche essere che l'insieme delle radici complesse di $g(x)$ (o di $h(x)$) sia vuoto, ovvero che $g(x)$ ($h(x)$) sia di grado 0. Quello che vogliamo dimostrare è proprio che questo è l'unico caso possibile. Si ha dunque che la fattorizzazione in $\mathbb{C}[x]$ di $g(x)$ e $h(x)$ è:

$$g(x) = \prod_{j=1}^{l} (x - \alpha_{i_j}) \quad h(x) = \prod_{j=1}^{m} (x - \alpha_{t_j})$$

Quindi il termine noto dei due polinomi è rispettivamente:

$$(-1)^l \prod_{j=1}^{l} \alpha_{i_j} \quad \text{e} \quad (-1)^m \prod_{j=1}^{m} \alpha_{t_j}$$

Ora basta osservare che se m e l fossero minori di n (ovvero tutti e due maggiori di 0 e quindi $f(x)$ riducibile) si avrebbe:

$$|(-1)^l \prod_{j=1}^{l} \alpha_{i_j}| = (\sqrt[n]{2})^l \notin \mathbb{Q} \quad \text{e} \quad |(-1)^m \prod_{j=1}^{m} \alpha_{t_j}| = (\sqrt[n]{2})^m \notin \mathbb{Q}$$

E quindi né $g(x)$, né $h(x)$ sarebbero polinomi a coefficienti in $\mathbb{Q}$. Quindi $f(x)$ si può scrivere come prodotto di $g(x)$ e $h(x)$ solo se uno dei due è una costante, ovvero $f(x)$ è irriducibile in $\mathbb{K}[x]$. □

Cerchiamo di trovare criteri su $\mathbb{Q}[x]$ per studiare l'irriducibilità o meno di un polinomio. Cominciamo cercando di sfruttare il fatto che per studiare la riducibilità di un polinomio in $\mathbb{Q}[x]$ possiamo ricondurci a polinomi con coefficienti interi.

Esempio 6.97. Sia $f(x)$ il polinomio a coefficienti razionali:

$$f(x) = \frac{-3}{8}x^3 + \frac{9}{20}$$

Calcoliamoci il minimo comun multiplo s dei denominatori dei coefficienti del polinomio $f(x)$, $s = 40$. Sia $g(x)$ il polinomio $g(x) = s \cdot f(x)$:

$$g(x) = -15x^3 + 18$$

Consideriamo adesso il polinomio $h(x)$ ottenuto dalla divisione di $g(x)$ per il massimo comun divisore d dei suoi coefficienti (ovvero 3):

$$h(x) = \frac{g(x)}{d} = -5x^3 + 6$$

$h(x)$ così ottenuto è un polinomio a coefficienti interi con il massimo comun divisore tra i coefficienti uguale ad 1.

Definizione 6.98. Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{A}[x]$ con $\mathcal{A}$ anello euclideo. Si dice **contenuto** di f, e si indica con $c(f)$ il massimo comun divisore $(a_n, \ldots, a_1, a_0)$ dei coefficienti del polinomio.

Definizione 6.99. Un polinomio $f \in \mathcal{A}[x]$ si dice **primitivo** se $c(f) = 1$.

Esercizio 6.100. *Sia $f(x)$ in $\mathbb{Z}[x]$ primitivo, se $r \in \mathbb{Q}$ è tale che $rf(x)$ è ancora un polinomio a coefficienti interi primitivo, allora $r = \pm 1$.*

Quanto fatto nell'Esempio 6.97 può facilmente essere generalizzato per qualsiasi polinomio a coefficienti razionali. Infatti, se $f(x) = \sum_{i=0}^{n} a_i x^i$ è in $\mathbb{Q}[x]$ e s è il minimo comun multiplo s dei denominatori degli a_i, allora il polinomio $g(x) = s \cdot f(x)$ è a coefficienti interi. Inoltre, indicando con d il massimo comun divisore dei coefficienti interi di $g(x)$, il polinomio $h(x) = \dfrac{g(x)}{d}$ è un polinomio (a coefficienti interi) primitivo.

Il risultato dell'Esercizio 6.81 ci dice che $h(x) = \dfrac{s}{d} \cdot f(x)$ è irriducibile in $\mathbb{Q}[x]$ se e solo se $f(x)$ lo è in $\mathbb{Q}[x]$. Quindi, per discutere l'irriducibilità di un polinomio $f(x) \in \mathbb{Q}[x]$, possiamo ridurci sempre al caso di un polinomio $h(x) \in \mathbb{Z}$ primitivo. Questo sarà molto importante nell'ottica della fattorizzazione in $\mathbb{Q}[x]$, perché, in un certo senso, ci ridurremo a "fattorizzare" in $\mathbb{Z}[x]$.

Abbiamo scritto tra virgolette *fattorizzare*, in quanto abbiamo definito cosa sia un irriducibile solo in $\mathbb{K}[x]$ con $\mathbb{K}$ campo. Estendiamo dunque la definizione al caso specifico di $\mathbb{Z}[x]$.

Definizione 6.101. Un polinomio $f(x)$ in $\mathbb{Z}[x] \setminus \{-1, 0, 1\}$ si dice **irriducibile** se $f(x) = g(x) \cdot h(x)$ implica che $g(x)$ o $h(x)$ è una costante.

Osservazione 6.102. Osserviamo che in questo caso non abbiamo escluso le costanti diverse da 0 nella definizione, in quanto in $\mathbb{Z}[x]$ non sono invertibili. In particolare non vale più il fatto che un polinomio di grado 1 è sempre irriducibile (Osservazione 6.85): ad esempio il polinomio $2x$ è, in $\mathbb{Z}[x]$, il prodotto dei polinomi

irriducibili 2 e x. Possiamo però osservare che un polinomio di primo grado primitivo è irriducibile (non possiamo raccogliere nessun fattore costante maggiore di 1 che in $\mathbb{Z}[x]$ è irriducibile).

Il prossimo risultato ci dice che se il polinomio $h(x) \in \mathbb{Z}[x]$ è fattorizzabile come prodotto di irriducibili in $\mathbb{Q}[x]$, allora è fattorizzabile come prodotto di irriducibili in $\mathbb{Z}[x]$. Il viceversa non è in generale vero proprio per l'Osservazione 6.102 (il polinomio $2x$ è irriducibile in $\mathbb{Q}[x]$), lo è se il polinomio è primitivo.

Lemma 6.103 (Lemma di Gauss)**.** *Sia $f(x) \in \mathbb{Z}[x]$, e sia $f(x) = a(x)b(x)$ una fattorizzazione di $f(x)$ in $\mathbb{Q}[x]$. Allora esiste q in $\mathbb{Q}$ tale che $a_1(x) = qa(x)$ e $b_1(x) = q^{-1}b(x)$ sono polinomi in $\mathbb{Z}[x]$, e dunque*

$$f(x) = a_1(x)b_1(x)$$

è una fattorizzazione di $f(x)$ in $\mathbb{Z}[x]$.

Dimostrazione. Abbiamo già osservato che possiamo supporre $f(x)$ primitivo (dividendo per $c(f)$), e che esistano due razionali s, t tali che $sa(x)$ e $tb(x)$ sono in $\mathbb{Z}[x]$ e primitivi. Per concludere dobbiamo mostrare che $s = t^{-1}$.

Il passo essenziale è dimostrare che se due polinomi $h(x)$, $g(x)$ in $\mathbb{Z}[x]$ sono primitivi, allora $h(x)g(x) \in \mathbb{Z}[x]$ è ancora primitivo. Per ipotesi non esistono primi p che dividono tutti i coefficienti di $h(x)$, né che dividono tutti i coefficienti di $g(x)$, ovvero $h(x)$ e $g(x)$ non sono congrui a 0 modulo p. Da questo segue che anche il loro prodotto $h(x)g(x)$ non è congruo a 0 modulo p, ovvero nessun primo p divide tutti i coefficienti di $h(x)g(x)$.

Tornando alla nostra dimostrazione, quello che abbiamo appena dimostrato implica che $sa(x)tb(x) = stf(x)$ è ancora un polinomio primitivo. Dall'Esercizio 6.100 segue che $st = 1$. □

Corollario 6.104. *Un polinomio $f(x) \in \mathbb{Z}[x]$ primitivo è irriducibile in $\mathbb{Q}[x]$ se e solo se è irriducibile in $\mathbb{Z}[x]$.*

Continuiamo ad esplorare la riducibilità in $\mathbb{Q}[x]$, partendo dalla ricerca di fattori di grado uno che, per il teorema di Ruffini, equivale all'esistenza di radici razionali.

La prima osservazione da fare è che $f(x) \in \mathbb{Q}[x]$ e $g(x) \in \mathbb{Z}[x]$, ottenuto moltiplicando $f(x)$ per il minimo comun multiplo s dei denominatori dei suoi coefficienti, hanno le stesse radici. Quindi anche per cercare le radici di un polinomio $f(x)$ in $\mathbb{Q}[x]$ non è restrittivo supporre che $f(x)$ abbia coefficienti interi.

Il seguente risultato caratterizza l'insieme R delle possibili radici razionali di un polinomio a coefficienti interi. In particolare, tale insieme è finito, e dunque abbiamo un algoritmo finito per capire se $f(x) \in \mathbb{Z}[x]$ ha radici razionali: valutare $f(x)$ per tutti gli elementi di R.

Teorema 6.105. *Se $f(x) \in \mathbb{Z}[x]$ e $q = \dfrac{r}{s} \in \mathbb{Q}$ è una radice razionale di $f(x)$, ovvero $f(q) = 0$, allora r divide il termine noto e s divide il coefficiente direttivo di $f(x)$.*

Dimostrazione. Sia $f(x) = \sum_{j=0}^{m} b_j x^j$ un polinomio a coefficienti interi e supponiamo $\alpha = \dfrac{r}{s}$ sia una radice razionale di $f(x)$ ridotta ai minimi termini, cioè

$(r, s) = 1$. Il fatto che α sia radice significa che:

$$\sum_{i=0}^{m} b_i \cdot \frac{r^i}{s^i} = 0$$

Moltiplicando tutto per s^m otteniamo l'equazione equivalente:

$$b_0 \cdot s^m + (\sum_{i=1}^{m-1} b_i \cdot r^i \cdot s^{m-i}) + b_m \cdot r^m = 0 \tag{3.1}$$

Da cui:

$$b_m \cdot r^m = -(b_0 \cdot s^m + \sum_{i=1}^{m-1} b_i \cdot r^i \cdot s^{m-i})$$

Osserviamo che il secondo membro di questa uguaglianza è un multiplo di s, perciò s divide $b_n r^n$. Essendo $(s, r) = 1$, questo implica che s divide b_n, ovvero il coefficiente direttivo del polinomio $f(x)$.

Osserviamo che l'equazione 3.1 può essere riscritta anche come:

$$b_0 \cdot s^m = -\sum_{i=1}^{m} b_i \cdot r^i \cdot s^{m-i}$$

Come prima, il secondo membro è un multiplo di r, dunque r divide $b_0 \cdot s^m$, inoltre $(r, s) = 1$ dunque r deve dividere b_0, ovvero il termine noto del polinomio $f(x)$. □

Esempio 6.106 (Irrazionalità di $\sqrt{2}$)**.** Consideriamo il polinomio $f(x) = x^2 - 2$. Dal Teorema 6.105 sappiamo che le uniche radici razionali possibili sono da ricercarsi nell'insieme $A = \{\pm 1, \pm 2\}$. Valutando $f(x)$, per ogni elemento di A, non si ottiene 0. Dunque $f(x)$ non ha radici razionali e di conseguenza (Corollario 6.87) è irriducibile in $\mathbb{Q}[x]$). Abbiamo in particolare dimostrato che l'equazione $x^2 = 2$ non ha soluzioni in $\mathbb{Q}$, ovvero $\sqrt{2}$ è irrazionale.

Esempio 6.107. Mostriamo, con un altro esempio, come il Teorema 6.105 e il Corollario 6.104 possono essere usati insieme per discutere la riducibilità di un polinomio a coefficienti razionali di quarto grado.

Consideriamo il polinomio razionale $f(x) = \frac{1}{2}x^4 + \frac{1}{4}$. Discutere la riducibilità di $f(x)$ è equivalente a discutere quella di $g(x) = 4 \cdot f(x) = 2x^4 + 1$ (inoltre trovando una fattorizzazione di $g(x)$ basterà moltiplicare per $\frac{1}{4}$ per avere una fattorizzazione di $f(x)$).

Dal Teorema 6.105 appena dimostrato, segue che le possibili radici razionali di $g(x)$ sono da ricercare nell'insieme:

$$A = \left\{\frac{1}{2}, -\frac{1}{2}, 1, -1\right\}$$

Andiamo a valutare dunque il polinomio $g(x)$ negli elementi di A:

$$g(1) = g(-1) = 3 \quad g(\tfrac{1}{2}) = g(-\tfrac{1}{2}) = \tfrac{9}{8}$$

Dunque $g(x)$ non ha radici razionali e quindi non ha fattori di grado 1. Se $g(x)$ è riducibile in $\mathbb{Q}[x]$, allora è prodotto di due polinomi razionali di grado 2.

Il Corollario 6.104 ci dice che se $g(x)$ è riducibile, allora è prodotto di due polinomi a coefficienti interi. Questo ci permette di verificare il fatto che $g(x)$ sia riducibile o meno attraverso il cosiddetto metodo della forza bruta.

In cosa consiste tale metodo? Supponiamo $g(x) = h(x) \cdot t(x)$ con $h(x)$ e $t(x)$ due polinomi di grado 2 a coefficienti interi, cioè:

$$h(x) = h_2 \cdot x^2 + h_1 \cdot x + h_0 \quad h_i \in \mathbb{Z} \quad h_2 \neq 0$$

$$t(x) = t_2 \cdot x^2 + t_1 \cdot x + t_0 \quad t_i \in \mathbb{Z} \quad t_2 \neq 0$$

Svolgiamo il prodotto tra $h(x)$ e $t(x)$ e imponiamo che coefficiente per coefficiente sia uguale a $g(x)$. Ne risulta il seguente sistema a coefficienti interi la cui risolubilità implica l'esistenza di una fattorizzazione di $g(x)$ e viceversa la cui non risolubilità implica l'irriducibilità di $g(x)$:

$$\begin{cases} h_2 \cdot t_2 = 2 \\ h_1 \cdot t_2 + h_2 \cdot t_1 = 0 \\ h_0 \cdot t_2 + h_1 \cdot t_1 + h_2 \cdot t_0 = 0 \\ h_0 \cdot t_1 + h_1 \cdot t_0 = 0 \\ h_0 \cdot t_0 = 1 \end{cases} \tag{3.2}$$

Innanzitutto non è restrittivo supporre che il coefficiente direttivo di $h(x)$ e $t(x)$ sia positivo: il loro prodotto deve essere positivo, quindi se fossero entrambi negativi basterebbe considerare $-h(x)$ e $-t(x)$ il cui prodotto è sempre $h(x) \cdot t(x)$. Perciò abbiamo che $h_2 = 1$ e $t_2 = 2$, visto che il ruolo di $h(x)$ e $t(x)$ è simmetrico, possiamo scegliere liberamente quale è uguale a 1 e quale è uguale a 2. Inoltre h_0 e t_0 sono uguali e sono entrambi 1 o entrambi -1: avendo già fissato il coefficiente direttivo positivo non possiamo a priori fare lo stesso con il termine noto. Portiamo avanti dunque due sistemi distinti, il primo con $h_0 = t_0 = 1$ e il secondo con $h_0 = t_0 = -1$:

$$\begin{cases} 2h_1 + t_1 = 0 \\ 2 + h_1 \cdot t_1 + 1 = 0 \\ t_1 + h_1 = 0 \end{cases} \qquad \begin{cases} 2h_1 + t_1 = 0 \\ -2 + h_1 \cdot t_1 - 1 = 0 \\ -t_1 - h_1 = 0 \end{cases}$$

È facile osservare che dalla prima e dalla terza equazione si ricava in entrambi i sistemi $h_1 = 0$ che sostituito nella seconda equazione restituisce in un caso $3 = 0$ e nell'altro $-3 = 0$. Ovvero il sistema 3.2 non ha soluzione e quindi $g(x)$, e di conseguenza $f(x)$ non è riducibile in $\mathbb{Q}[x]$.

È evidente che all'aumentare del grado del polinomio da fattorizzare, il metodo della forza bruta diventa praticamente inutilizzabile. Esistono algoritmi per il calcolo della fattorizzazione in irriducibili di un polinomio in $\mathbb{Z}[x]$ (e quindi come osservato in $\mathbb{Q}[x]$), ma non li descriveremo in questa trattazione. Ci limitiamo dunque a dare alcuni criteri di irriducibilità, che sono conseguenza di un importante risultato generale per anelli $\mathbb{K}[x]$.

Teorema 6.108. *Sia $\varphi : \mathbb{K}[x] \to \mathbb{K}[x]$ un omomorfismo di anelli tale che, per ogni $q(x) \in \mathbb{K}[x]$ di grado maggiore di zero, $\varphi(q(x))$ abbia grado maggiore di zero. Per ogni $g(x)$ in $\mathbb{K}[x]$, se $g(x)$ è riducibile allora anche $\varphi(g(x))$ lo è.*

Dimostrazione. Se $g(x)$ è riducibile in $\mathbb{K}[x]$, allora esistono due polinomi $a(x)$ e $b(x)$ di grado maggiore di zero in $\mathbb{K}[x]$ tali che $g(x) = a(x) \cdot b(x)$. Essendo φ un omomorfismo di anelli, si ha che:

$$\varphi(g(x)) = \varphi(a(x)) \cdot \varphi(b(x))$$

Per le ipotesi su φ, questa è una fattorizzazione non banale di $\varphi(g(x))$ (entrambi i polinomi $\varphi(a(x))$ e $\varphi(b(x))$ hanno grado maggiore di zero). □

Osservazione 6.109 (Criterio di irriducibilità)**.** Dalla dimostrazione del Teorema 6.108 segue che, se $g(x)$ è un polinomio di grado maggiore di 0 e φ è un omomorfismo di anelli con $\varphi(g(x))$ di grado maggiore di 0, allora $g(x)$ riducibile implica $\varphi(g(x))$ riducibile (insomma il teorema vale per qualsiasi sottoinsieme di $\mathbb{K}[x]$ per cui φ abbia la proprietà sul grado voluta).

In particolare se $g(x)$ in $\mathbb{K}[x]$ ha grado maggiore di 0, ed esiste un omomorfismo di anelli per cui $\varphi(g(x))$ ha grado maggiore di 0 ed è irriducibile in $\mathbb{K}[x]$, allora $g(x)$ è irriducibile in $\mathbb{K}[x]$.

Corollario 6.110. *Se $f(x)$ è riducibile in $\mathbb{K}[x]$, allora $f(x^k)$ è riducibile in $\mathbb{K}[x]$ per ogni $k \in \mathbb{N}^+$,.*

Dimostrazione. Basta osservare che l'omomorfismo di anelli φ che lascia fisse le costanti di $\mathbb{K}[x]$ e manda x in x^k, verifica la proprietà sul grado del Teorema 6.108. □

Osservazione 6.111. Osserviamo che il viceversa del Corollario 6.110 è ovviamente falso: il polinomio $f(x) = x$ è irriducibile in $\mathbb{K}[x]$ (è di grado 1), ma per qualsiasi $k > 1$ non lo è $f(x^k) = x^k$ (è il prodotto di k fattori irriducibili tutti uguali a x).

Corollario 6.112. *$f(x)$ in $\mathbb{K}[x]$ è irriducibile se e solo se, per ogni $a, b \in \mathbb{K}$ con $a \neq 0$, $f(ax + b)$ è irriducibile in $\mathbb{K}[x]$.*

Dimostrazione. Basta considerare i due omomorfismi di anelli φ e σ che lasciano fisse le costanti e mandano x rispettivamente in $ax + b$ ed in $\dfrac{x - b}{a}$, e mostrare che verificano la proprietà sul grado del Teorema 6.108. □

Esercizio 6.113. *Sia $f(x) \in \mathbb{K}[x]$ di grado n. Il polinomio $q(x)$ di $\mathbb{K}[x]$ definito da:*

$$q(x) = x^n \cdot f\left(\frac{1}{x}\right)$$

è detto **polinomio reciproco** *di $f(x)$. Dimostrare che se $f(x) \neq a_n x^n$, allora $f(x)$ è irriducibile in $\mathbb{K}[x]$ se e solo se $q(x)$ lo è.*

A questo punto cerchiamo di sfruttare il Teorema 6.108 nel caso specifico di polinomi a coefficienti interi per trovare criteri di irriducibilità in $\mathbb{Q}[x]$.

Proposizione 6.114 (Criterio della riduzione modulo p)**.** *Sia $f(x) \in \mathbb{Z}[x]$, se il primo p non divide il coefficiente direttivo di $f(x)$, allora $f_p[x]$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$ (dove $f_p[x]$ è il polinomio i cui coefficienti sono le classi di equivalenza modulo p dei coefficienti di $f(x)$) implica $f(x)$ è irriducibile in $\mathbb{Q}[x]$.*

Dimostrazione. Pur non essendo in partenza su un $\mathbb{K}[x]$ (essendo i polinomi a coefficienti interi), possiamo ripercorrere esattamente la dimostrazione del Teorema 6.109, nel caso specifico dell'applicazione che associa ad ogni $f(x)$ in $\mathbb{Z}[x]$, il polinomio $f_p[x]$ in $\mathbb{Z}/p\mathbb{Z}[x]$. □

Osservazione 6.115. Il viceversa della Proposizione 6.114 non è, in generale, vero: il polinomio $f(x) = x^2 - 3$ è irriducibile in $\mathbb{Q}[x]$ (non ha radici in $\mathbb{Q}$ e Corollario 6.87), mentre il polinomio $f_3(x) = x^2$ è riducibile in $\mathbb{Z}_3[x]$, nonostante 3 non divida il coefficiente direttivo di $f(x)$ che è 1.

Esempio 6.116. Il polinomio $f(x) = x^3 + 4x^2 + 3x + 1$ è irriducibile in $\mathbb{Q}[x]$, infatti $f_2(x) = x^3 + [1]_p x + [1]_p$ non ha radici, e dunque è irriducibile (Corollario 6.87), in $\mathbb{Z}_2[x]$.

Teorema 6.117 (Criterio di irriducibilità di Eisenstein)**.** *Dato un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, se esiste un numero primo p tale che:*

(1) *p non divide a_n.*
(2) *$p | a_i$ per ogni $0 \leq i < n$.*
(3) *p^2 non divide a_0.*

allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e quindi in $\mathbb{Q}[x]$.

Dimostrazione. Supponiamo $f(x)$ riducibile in $\mathbb{Z}[x]$, ovvero esistono $g(x)$ e $h(x)$ in $\mathbb{Z}[x]$ di grado maggiore di 0, con $f(x) = g(x)h(x)$. Dalla Proposizione 6.114, sappiamo che $f_p(x) = g_p(x)h_p(x)$ è una fattorizzazione in $\mathbb{Z}/p\mathbb{Z}[x]$. Per le prime due ipotesi si ha che $f_p = a_n x^n$ e, per la definizione di prodotto tra polinomi, si ha che i termini noti b_0 e c_0, rispettivamente di $g(x)$ e $h(x)$, devono essere congrui a 0 modulo p. Questo è assurdo perché sarebbe $a_0 = b_0 c_0$ multiplo di p^2, contro la terza ipotesi del teorema. □

Esempio 6.118. Il polinomio $f(x) = 3x^4 + 12x^3 + 6x^2 + 2$ è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein, infatti $p = 2$ non divide il coefficiente direttivo 3 di $f(x)$, divide tutti gli altri coefficienti di $f(x)$, e $2^2 = 4$ non divide il termine noto 2 di $f(x)$.

Osservazione 6.119. Usando il criterio di Eisenstein si può dare un'altra dimostrazione del fatto che per ogni n intero positivo esiste un polinomio irriducibile di grado n in $\mathbb{Q}[x]$. Infatti i polinomi $x^n - 2$, considerati nella prima dimostrazione che abbiamo dato, rispettano le ipotesi del criterio con $p = 2$.

Con lo stesso ragionamento possiamo dimostrare che, per ogni n intero positivo, ci sono infiniti polinomi di grado n irriducibili in $\mathbb{Q}[x]$, basta considerare tutti i polinomi della forma $x^n - p$ al variare di p tra i numeri primi (che sappiamo appunto essere infiniti).

Corollario 6.120. *Se p è un numero primo, allora il polinomio $f(x) = \sum_{i=0}^{p-1} x^i$ è irriducibile in $\mathbb{Z}[x]$.*

Dimostrazione. Indichiamo con $f(x)$ il polinomio $\sum_{i=0}^{p-1} x^i$, allora:

$$f(x) = \frac{x^p - 1}{x - 1}.$$

Consideriamo l'omomorfismo $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[y]$ che manda x in $y + 1$:

$$\varphi(f) = \frac{(y+1)^p - 1}{y + 1 - 1} = \frac{(\sum_{k=0}^{p} \binom{p}{k} y^k) - 1}{y} = \sum_{k=0}^{p-1} \binom{p}{k} y^{p-1-k}$$

Osserviamo innanzitutto che φ conserva la riducibilità o meno di $f(x)$, in quanto ne conserva sia il grado che il fatto di essere primitivo. Usiamo il criterio di Eisenstein per dimostrare che $\varphi(f)$ è irriducibile:

- Sicuramente p non divide il coefficiente del termine di grado maggiore, che è 1.

- p divide tutti gli altri coefficienti che sono del tipo $\binom{p}{k}$ con k che varia tra 1 e $p-1$.
- Infine p^2 non divide $\binom{p}{p-1} = p$.

□

Esercizio 6.121. *Dimostrare che $f(x) \in \mathbb{K}[x]$. $f(x)$ ha fattori di grado maggiore di 0 multipli se e solo se il grado di $(f(x), f'(x))$ è maggiore di 0.*

Esercizio 6.122. *Trovare una fattorizzazione in irriducibili su $\mathbb{Z}_3[x]$ del polinomio $g = x^6 + x^5 - x + 1$.*

Svolgimento. $g(x)$ non ha radici in $\mathbb{Z}_3$ infatti:

$$g(0) = 1 \quad g(1) = 2 \quad g(2) = 2$$

Cerchiamo di vedere se ha fattori multipli. Il polinomio derivata è $g'(x) = 2x^4 - 1$. Calcoliamo il massimo comun divisore tra $g(x)$ e $g'(x)$:

$$g(x) = g'(x) \cdot \underbrace{2x^2 + 2x}_{q_1(x)} + \underbrace{2x^2 + x + 1}_{r_1(x)}$$

$$g'(x) = r_1(x) \cdot (x^2 + x - 1)$$

Dunque $r_1(x) = (g(x), g'(x)) = 2x^2 + x + 1$ è un fattore multiplo di $g(x)$. A questo punto abbiamo due casi possibili visto il grado di $g(x)$:

- $g(x) = r_1^3(x)$.
- $g(x) = r_1^2(x) \cdot h(x)$ con $(r_1(x), h(x)) = 1$.

In ogni caso $x^4 + x^3 + 2x^2 + 2x + 1 = (2x^2 + x + 1)^2$ divide $g(x)$. Possiamo perciò eseguire la divisione e vedere se il fattore che rimane è $r_1(x)$ stesso o un fattore primo con $r_1(x)$:

$$g(x) = r_1^2(x) \cdot (x^2 - 2)$$

Dunque la fattorizzazione in irriducibili di $g(x)$ in $\mathbb{Z}_3[x]$ è:

$$g(x) = (2x^2 + x + 1)^2 \cdot (x^2 + 1)$$

Esercizio 6.123. *Discutere la fattorizzazione in irriducibili in $\mathbb{Q}[x]$ dei seguenti polinomi a coefficienti interi:*

(1) $f(x) = 3x^5 + 6x^3 + 9x + 2$.
(2) $g(x) = x^6 + 3x^3 - 2$.
(3) $h(x) = x^4 - 3x^2 + 2$.

Svolgimento. Consideriamo un polinomio alla volta. Mostreremo che $f(x)$ è irriducibile in $\mathbb{Q}[x]$ mentre $g(x)$ e $h(x)$ sono riducibili.

(1) Non possiamo usare il criterio di Eisenstein per il polinomio $f(x)$, in quanto $6, 9, 2$ hanno come divisore comune solo 1 e quindi non esiste nessun primo che li divide tutti e non divide il coefficiente direttivo 3.

Se invece calcoliamo il polinomio reciproco $q(x)$ di $f(x)$, si ha:

$$q(x) = 2y^5 + 9y^4 + 6y^2 + 3$$

che verifica le ipotesi del criterio di Eisenstein con $p = 3$. Quindi $q(x)$ è irriducibile in $\mathbb{Q}[x]$, e di conseguenza (Esercizio 6.113) anche $f(x)$.

(2) Per trovare una fattorizzazione di $g(x)$, consideriamo il cambiamento di variabile descritto dall'omomorfismo ψ tra $\mathbb{K}[t]$ e $\mathbb{K}[x]$ che manda t in x^3. Si ha che:

$$w(t) = \psi^{-1}(g(x)) = t^2 + 3t + 2$$

Il polinomio $w(t)$ si fattorizza su $\mathbb{Q}[t]$ come $(t+1)(t+2)$, la cui immagine tramite il cambiamento di variabile fornisce la fattorizzazione $(x^3+1)(x^3+2)$ di $g(x)$ (che dunque non è irriducibile).

Per trovare la fattorizzazione di $g(x)$ in irriducibili, basta osservare che x^3+1 è una somma di cubi e quindi si fattorizza come $(x+1)(x^2-x+1)$, mentre x^3+2 è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein.

Concludendo, la fattorizzazione in irriducibili in $\mathbb{Q}[x]$ di $g(x)$ è:

$$(x+1)(x^2-x+1)(x^3+2)$$

(3) Anche per $h(x)$ procediamo con un cambio di variabile ponendo $\psi(t) = x^2$. Si ha che:

$$k(t) = \psi^{-1}(h(x)) = t^2 - 3t + 2$$

$k(t)$ si fattorizza come $(t-1)\cdot(t-2)$ e dunque $g(x) = \psi(k(t))$ si fattorizza come:

$$g(x) = \psi(k(t)) \underbrace{=}_{\psi \text{ é omo.}} \psi(t-1)\cdot\psi(t-2) = (x^2-1)\cdot(x^2-2)$$

In $\mathbb{Q}[x]$ x^2-1 si fattorizza come $(x-1)(x+1)$ mentre x^2-2 è irriducibile per Eisenstein. Concludendo la fattorizzazione in irriducibili di $h(x)$ è:

$$(x^2-2)\cdot(x-1)\cdot(x+1)$$

Esercizio 6.124. *Fattorizzare in* $\mathbb{Q}[x]$ *i polinomi* x^6+3x^3-2 *e* x^4-3x^2+2.

Svolgimento. Consideriamo il cambiamento di variabile, dato dall'omomorfismo $\mathcal{S}$ tra $\mathbb{K}[t]$ e $\mathbb{K}[x]$ che manda t in x^3: $\mathcal{S}(t^2+3t+2) = x^6+3x^3+2$.

Il polinomio t^2+3t+2 si fattorizza su $\mathbb{Q}[t]$ come $(t+1)(t+2)$ la cui immagine, tramite $\mathcal{S}$, fornisce la fattorizzazione $(x^3+1)(x^3+2)$ di x^6+3x^3+2. (x^3+1) è una somma di cubi e quindi si fattorizza come $(x+1)(x^2-x+1)$, mentre (x^3+2) è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein. Quindi la fattorizzazione in irriducibili in $\mathbb{Q}[x]$ di x^6+3x^3+2 è:

$$(x+1)(x^2-x+1)(x^3+2).$$

Anche per x^4-3x^2+2 facciamo un cambio di variabile e poniamo $\mathcal{S}(t) = x^2$, ottenendo il polinomio t^2-3t+2 di $\mathbb{K}[t]$, che si fattorizza in $(t-1)(t-2)$. Questa fattorizzazione corrisponde alla fattorizzazione $(x^2-1)(x^2-2)$ di x^4-3x^2+2. È semplice osservare che in $\mathbb{Q}[x]$, x^2-1 si fattorizza come $(x-1)(x+1)$, mentre x^2-2 è irriducibile. Perciò la fattorizzazione in irriducibili di x^4-3x^2+2 è:

$$(x^2-2)(x-1)(x+1)$$

Abbiamo discusso la fattorizzazione in $\mathbb{K}[x]$ con $\mathbb{K}$ uguale a $\mathbb{C}$, $\mathbb{R}$ e $\mathbb{Q}$. Ci rimarrebbe da trattare solo il caso della fattorizzazione in $\mathbb{Z}/p\mathbb{Z}[x]$. Ci limitiamo a due osservazioni:

- Il problema di determinare se un elemento $f(x)$ di $\mathbb{Z}/m\mathbb{Z}[x]$ di grado k qualsiasi sia irriducibile (e in caso negativo trovarne una fattorizzazione in irriducibili) è deterministico in quanto i polinomi di grado fissato in $\mathbb{Z}/m\mathbb{Z}[x]$ sono finiti.

Esercizio 6.125. *Contare, in funzione di m e k, quanti sono i polinomi distinti di grado k in $\mathbb{Z}/m\mathbb{Z}[x]$.*

Inoltre, se $f(x) = g(x) \cdot h(x)$ è una fattorizzazione non banale di $f(x)$ e r e s sono il grado rispettivamente di $g(x)$ e $h(x)$ allora $1 \leq r < k$, $1 \leq s < k$ e (per le proprietà della funzione grado) $s + r = k$. Da questo segue che uno tra s e r è minore o uguale di $N =$ parte intera di $\frac{k}{2}$. Dunque per affermare che $f(x)$ è irriducibile in $\mathbb{Z}/m\mathbb{Z}[x]$ (o trovarne suoi fattori non banali) *basta* provare la divisione di $f(x)$ con tutti i polinomi in $\mathbb{Z}/m\mathbb{Z}[x]$ di grado maggiore di 0 e minore di N.

- Se $f(x) \in \mathbb{Z}[x]$ si fattorizza come $g(x) \cdot h(x)$ e m non divide il coefficiente direttivo di $f(x)$, allora l'omomorfismo $\varphi_m(f(x))$, che associa ad $f(x)$ il polinomio $\overline{f(x)}$ di $\mathbb{Z}/m\mathbb{Z}[x]$ i cui i coefficienti sono le classi di resto modulo m, conserva il grado di $f(x)$. Dunque una fattorizzazione in $\mathbb{Z}/m\mathbb{Z}[x]$ di $\overline{f(x)}$ è data da $\overline{g(x)} \cdot \overline{h(x)}$.

  Cioè se $f(x)$ è fattorizzabile in $\mathbb{Z}[x]$ allora lo è anche $\varphi_m(f(x))$ per ogni m che non divide il coefficiente direttivo di $f(x)$. Questo ci fornisce un ulteriore criterio di irriducibilità in $\mathbb{Q}[x]$, infatti abbiamo che:

  Proposizione 6.126. *Sia $f(x) \in \mathbb{Z}[x]$ con coefficiente direttivo a. Se $\varphi_m(f(x))$ è irriducibile in $\mathbb{Z}/m\mathbb{Z}[x]$ per un m che non divide a, allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$.*

4. Una dimostrazione del teorema fondamentale dell'algebra

In questo paragrafo, per completezza, riportiamo una dimostrazione del teorema fondamentale dell'algebra che ci è servito per caratterizzare la fattorizzazione dei polinomi in $\mathbb{C}[x]$ e anche in $\mathbb{R}[x]$. Faremo uso di qualche risultato tipicamente affrontato nei corsi di Analisi in particolare il fatto che, dato $f(x) \in \mathbb{C}[x]$, la funzione polinomiale ad esso associata che fa corrispondere ad $\alpha \in \mathbb{C}$ il complesso $f(\alpha)$ è continua. Ci servirà inoltre il risultato noto come teorema di Weierstrass, ovvero che se f è una funzione continua da un insieme compatto X a $\mathbb{R}$, allora f assume in X valore massimo e minimo.

Teorema 6.127. *Ogni polinomio $f(x)$ a coefficienti in $\mathbb{C}$ di grado maggiore di zero ammette almeno una radice in $\mathbb{C}$.*

Definizione 6.128. Un campo $\mathbb{K}$ si dice **algebricamente chiuso** se ogni polinomio in $\mathbb{K}[x]$ di grado maggiore di zero ha una radice in $\mathbb{K}$.

Alla luce della definizione di campo algebricamente chiuso (che useremo anche nel seguito), possiamo formulare il teorema fondamentale dell'algebra anche come segue:

Teorema 6.129. *Il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso.*

Dimostrazione. Sia $f(z) = \sum_{i=0}^{n} a_i z^i \in \mathbb{C}[x]$ con $a_n \neq 0$, cioè di grado maggiore di zero. Dobbiamo mostrare che esiste $\alpha \in C$ tale che $f(\alpha) = 0$. Consideriamo la funzione polinomiale $F : \mathbb{C} \longrightarrow \mathbb{C}$ associata al polinomio $f(x)$ e componiamola con la funzione $\beta : \mathbb{C} \longrightarrow \mathbb{R}_+$ che associa ad un complesso il suo modulo:

$$z \in \mathbb{C} \xrightarrow{F} f(z) \in \mathbb{C} \xrightarrow{\beta} |f(z)| \in \mathbb{R}_+$$

Indichiamo con φ la composizione di F con β e osserviamo che è una funzione continua, perché composizione di due funzioni continue ($|z| = 0$ se e solo se $z = 0$). Osserviamo che (a meno di dividere per a_n che è un coefficiente diverso da zero) possiamo supporre il polinomio $f(z)$ monico.

$$\varphi(f(z)) = |f(z)| \geq |z^n| - |\sum_{i=0}^{n-1} a_i z^i| \geq |z|^n - A\sum_{i=0}^{n-1} |z|^i$$

dove con A abbiamo indicato il massimo dei valori assoluti dei coefficienti a_i. Vogliamo determinare c in modo tale che se $|z| > c$ allora $|f(z)| \geq \frac{|z^n|}{2}$. Scegliendo $c > 1$ si ha che:

$$\forall i \leq n-1 \quad |z|^i A \leq |z|^{n-1} A$$

quindi

$$|f(z)| \geq |z|^n - A\sum_{i=0}^{n-1} |z|^i \geq |z|^n - nA|z|^{n-1}$$

Allora basta scegliere c tale che se $|z| > c$ allora:

$$|z|^n - nA|z|^{n-1} \geq \frac{|z|^n}{2} \leftrightarrow \frac{|z|^n}{2} \geq nA|z|^{n-1} \leftrightarrow |z| \geq 2nA.$$

Conclusione: Per c abbastanza grande, $|z| > c$ implica

$$|f(z)| \geq \frac{|z|^n}{2} \geq \frac{c^n}{2}$$

cioè al di fuori del cerchio di raggio c la funzione φ assume valori abbastanza grandi.

Osserviamo che $\varphi(0) = |f(0)| = a_0$ e che $\frac{c^n}{2} = \frac{(2nA)^n}{2} \geq |a_0|$, quindi il valore della funzione φ nello zero è più piccolo di qualsiasi valore della funzione fuori dal cerchio di raggio c. Questo ci assicura che φ ha un minimo assoluto, infatti possiamo considerare $\varphi|_X$, la funzione ristretta al cerchio di raggio c. X è un compatto, φ è continua e quindi esiste z_0 minimo della funzione su φ. Basta osservare che:

$$\forall |z| \geq c \quad \varphi(z_0) \leq \varphi(0) \leq \varphi(z).$$

Vogliamo dimostrare che questo minimo è zero. Supponiamo per assurdo che il minimo sia $\varphi(z_0) = a > 0$, possiamo supporre che:

- Il minimo sia nel punto zero, considerando la traslazione, che non cambia il grado di $f(z)$: $\tau : f(z) \longrightarrow f(z - z_0)$.
- Il valore del minimo sia 1 considerando la moltiplicazione per il fattore $\frac{1}{a}$: $f(z) \longrightarrow \frac{1}{a} f(z)$, che come la precedente traslazione non cambia il grado di $f(z)$.

Fatte queste due ipotesi, che abbiamo visto non essere ristrettive, abbiamo che: $f(z) = \sum_{i=0}^{n} a_i z^i$ con $a_0 = 1$. Sia a_k il primo coefficiente diverso da zero in $f(z)$ con $k > 0$. Analogamente a quanto fatto in precedenza si dimostra che si può scegliere ϵ (abbastanza vicino allo 0) tale che per $|z| \leq \epsilon$ si abbia:

$$|\sum_{i=k+1}^{n} a_i z^i| \leq \frac{|a_k z^k|}{2}$$

Possiamo risolvere in $\mathbb{C}$ l'espressione binomiale $1 + a_k z^k = 0$, e sia λ una soluzione. Allora se $z = t\lambda$ con $t \geq 0$ si ha:

$$a_k(t\lambda)^k = -t^k$$

e per t piccolo (in modo che $t\lambda$ sia minore o uguale di ϵ):

$$|f(z)| = |1 - t^k + \sum_{i=k+1}^{n} a_i z^i| \leq |1 - t^k| + |\sum_{i=k+1}^{n} a_i z^i| \leq 1 - t^k + \frac{1}{2}t^k = 1 - \frac{1}{2}t^k < 1$$

e questo è assurdo perché avevamo supposto che il minimo della funzione φ fosse 1. Quindi il minimo della funzione $|f(z)|$ è zero, cioè esiste z_0 tale che $|f(z_0)| = 0$ se e solo se $f(z_0) = 0$. □

5. Omomorfismi di anelli, ideali e anelli quoziente

Da qui in avanti, se non specificato diversamente, quando parleremo di *anello*, intenderemo *anello commutativo con unità*.
Abbiamo già introdotto (Definizione 6.34) il concetto di omomorfismo di anelli, come una funzione che rispetta la struttura di anello, ovvero che *commuta* con le due operazioni definite su di un anello. Similmente al caso dei gruppi possiamo introdurre il concetto di isomorfismo, e ripercorrere lo studio delle caratteristiche strutturali, fatta con i gruppi, nel caso degli anelli.

Definizione 6.130. Un omomorfismo di anelli iniettivo e surgettivo si dice un **isomorfismo di anelli**. Due anelli $(\mathcal{A}, +_\mathcal{A}, \cdot_\mathcal{A})$ e $(B, +_B, \cdot_B)$ si dicono **isomorfi** se esiste un isomorfismo da $\mathcal{A}$ in B (se $\mathcal{A}$ e B sono isomorfi useremo la stessa notazione dei gruppi ovvero $\mathcal{A} \cong B$).

Osservazione 6.131. Un omomorfismo di anelli f da $(A, +_A, \cdot_A)$ a $(B, +_B, \cdot_B)$ è in particolare un omomorfismo di gruppi additivi, dunque se $(A, +_A)$ è un gruppo ciclico basta definire f sul generatore del gruppo.

Esempio 6.132. Quali sono i possibili omomorfismi di anello da $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ad un anello $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$? Innanzitutto $f([1]_m) = [a]_n$ deve avere ordine che divide m: questa è la condizione necessaria e sufficiente affinché f sia omomorfismo di gruppi additivi. Se f è un omomorfismo di anelli allora necessariamente:

$$[a]_n = f([1]_m) = f([1]_m \cdot [1]_m) \underbrace{=}_{omo.anelli} f([1]_m) \cdot f([1]_m) = [a]_n \cdot [a]_n$$

Viceversa, se $[a]_n$ immagine di $[1]_m$ tramite f è tale che $[a^2]_n = [a]_n$, allora per ogni $[s]_m$ e $[t]_m$ in $\mathbb{Z}/m\mathbb{Z}$ si ha:

$$f([s]_m \cdot [t]_m) = [s \cdot t \cdot a]_n = [s \cdot t \cdot a^2]_n = ([s \cdot a]_n) \cdot ([t \cdot a]_n) = f([s]_m) \cdot f([t]_m)$$

Quindi condizione necessaria e sufficiente affinché f sia omomorfismo di anelli è che l'ordine di $[a]_n$ divida m e che $[a^2]_n = [a]_n$ in $\mathbb{Z}/n\mathbb{Z}$.

Osservazione 6.133. Se $f : (\mathcal{A}, +_\mathcal{A}, \cdot_\mathcal{A}) \to (B, +_B, \cdot_B)$ è un omomorfismo di anelli, in particolare f è un omomorfismo tra gruppi additivi, dunque $f(0_\mathcal{A}) = 0_B$ e $f(-a) = -f(a)$. Nel caso di $\mathcal{A}$ e B anelli unitari, ci chiediamo se necessariamente deve essere che $f(1_\mathcal{A}) = 1_B$ (se questo fosse vero avremmo che, per ogni a di $\mathcal{A}^*$, $f(a^{-1}) = (f(a))^{-1}$).

La risposta è no, infatti l'applicazione nulla, che manda tutti gli elementi di $\mathcal{A}$ in 0_B, è sempre un omomorfismo di anelli ma evidentemente $f(1_\mathcal{A}) = 0_B \neq 1_B$. E se f non è l'omomorfismo nullo? Per ogni $a \in \mathcal{A}$ si ha che:

$$\begin{cases} f(a) = f(1_\mathcal{A} \cdot a) = f(1_\mathcal{A}) \cdot f(a) \\ f(a) = 1_B \cdot f(a) \end{cases}$$

Da cui segue che per ogni $a \in \mathcal{A}$:

$$(f(1_\mathcal{A}) - 1_B) \cdot f(a) = 0$$

Essendo f diverso dall'omomorfismo nullo, esiste $a \in \mathcal{A}$ tale che $f(a) \neq 0$, d'altra parte se B è un dominio di integrità la precedente relazione implica $f(1_\mathcal{A}) - 1_B = 0$, ovvero $f(1_\mathcal{A}) = 1_B$. In questo caso si parla di **omomorfismo di anelli con unità**.

Esempio 6.134. Consideriamo $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ definito da $f(x) = 3x$. f è un omomorfismo di anelli, infatti è un omomorfismo di gruppi $(o([3]_6)|o([1]_6))$ e inoltre per ogni coppia $x, y \in \mathbb{Z}_6$:

$$f(x \cdot y) = 3(x \cdot y) \underbrace{=}_{3 \equiv 9 \ (6)} 9(x \cdot y) = (3x) \cdot (3y) = f(x) \cdot f(y)$$

Ma f pur non essendo l'omomorfismo nullo non è un omomorfismo di anelli con unità in quanto manda 1 in 3. Esistono dunque, tra anelli con unità, omomorfismi di anelli che non sono nulli e che non conservano l'unità.

Definito l'omomorfismo di anelli introduciamo il concetto di nucleo:

Definizione 6.135. Dato $f : (\mathcal{A}, +_\mathcal{A}, \cdot_\mathcal{A}) \to (B, +_B, \cdot_B)$ omomorfismo di anelli, si chiama **nucleo** di f, e si indica con $Ker\ f$, l'insieme degli $a \in \mathcal{A}$ tali che $f(a) = 0_B$.

Osservazione 6.136. Ci chiediamo se $Ker\ f$ è un sottoanello di $\mathcal{A}$. Sicuramente è un sottogruppo additivo ed è chiuso per prodotto, anzi $Ker\ f$ ha una proprietà più forte della semplice chiusura per prodotto. Infatti è facile provare che per ogni $a \in \mathcal{A}$ si ha che:

$$a \cdot Ker\ f \underbrace{=}_{def.} \{a \cdot k | k \in Ker\ f\} = Ker\ f$$

Cioè $Ker\ f$ è chiuso per il prodotto dei suoi elementi per un qualsiasi elemento dell'anello $\mathcal{A}$. Infatti per ogni $a \in \mathcal{A}$ e $x \in Ker\ f$:

$$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0 = 0$$

Osserviamo che, se $\mathcal{A}$ è con unità, non è detto che sia $1_\mathcal{A} \in Ker\ f$ (basta considerare un qualsiasi isomorfismo di anelli con identità: per esempio l'identità da $\mathcal{A}$ in $\mathcal{A}$). Quindi $Ker\ f$ è sicuramente un sottoanello di $\mathcal{A}$ se $\mathcal{A}$ non ha unità, mentre in generale non è detto lo sia se $\mathcal{A}$ è con identità.

A questo punto vogliamo capire se è possibile definire un oggetto che possa essere quello che i sottogruppi normali sono per i gruppi, ovvero che corrisponda a tutti e soli i nuclei di omomorfismi di anelli e che permetta di definire una struttura di anello quoziente proprio come fatto nei gruppi. Partendo dall'osservazione 6.136 consideriamo la seguente definizione:

Definizione 6.137. Un sottoinsieme I di un anello $(\mathcal{A}, +, \cdot)$ si dice un **ideale** se:

(1) I è un sottogruppo di $\mathcal{A}$ rispetto all'addizione.
(2) $\forall a \in \mathcal{A}\ \forall x \in I$ si ha che $a \cdot x \in I$.

Esempio 6.138. Consideriamo l'anello dei numeri interi $\mathbb{Z}$. Se ci sono ideali in $\mathbb{Z}$, devono essere dei gruppi per la somma e quindi della forma $m\mathbb{Z}$. Inoltre, per ogni $z \in \mathbb{Z}$ e per ogni $x \in m\mathbb{Z}$, si deve avere che $z \cdot x$ è elemento di $m\mathbb{Z}$. Questo è sempre vero qualsiasi sia m: un multiplo di m moltiplicato per qualsiasi intero, continua ad essere un multiplo di m. Quindi, in questo caso, gli ideali di $\mathbb{Z}$ corrispondono ai sottogruppi, ma non sempre è così: $\mathbb{Z}$ è un sottoanello (e quindi un sottogruppo) di $\mathbb{Q}$ ma non è un ideale, infatti ad esempio:

$$\underbrace{1}_{\in\mathbb{Z}} \cdot \underbrace{\frac{1}{2}}_{\in\mathbb{Q}} = \frac{1}{2} \notin \mathbb{Z}$$

Definizione 6.139. Un ideale I di $\mathcal{A}$ si dice **proprio** se $I \neq \mathcal{A}$.

Esercizio 6.140. *Dimostrare che se $I_1, \ldots, I_n$ sono ideali di un anello $\mathcal{A}$, allora la loro intersezione è un ideale di $\mathcal{A}$.*

Definizione 6.141. Dati un anello $\mathcal{A}$ e due suoi ideali I, J, si dice **ideale somma** di I e J l'insieme:

$$I + J = \{x + y | x \in I, y \in J\}$$

Esercizio 6.142. *Dimostrare che effettivamente, dati due ideali I e J di un anello $\mathcal{A}$, l'insieme $I + J$ definito in 6.141 è un ideale di $\mathcal{A}$.*

Proposizione 6.143. *L'ideale somma $I + J$ è il più piccolo ideale contenente sia I che J.*

Dimostrazione. Per mostrare che $I + J$ contiene I (analogamente per J) basta osservare che gli elementi della forma $i + 0$ con $i \in I$ appartengono ad $I + J$.

Se X è un ideale che contiene sia I che J, essendo in particolare un sottogruppo additivo, deve contenere anche la somma tra gli elementi di I e di J e perciò deve contenere $I + J$. □

Sia S un sottoinsieme di $\mathcal{A}$, cerchiamo di descrivere, se esiste, il più piccolo ideale di $\mathcal{A}$ contenente S, che chiameremo **ideale generato** da S ed indicheremo con (S). Osserviamo innanzitutto che l'insieme degli ideali che contengono S è sicuramente non vuoto, in quanto $\mathcal{A}$ vi appartiene.

Come nel caso dei sottogruppi generati da un insieme, analizziamo dei casi distinti per la numerosità di S.

Il caso più semplice è quello di $S = \{x\}$. Un ideale che contenga x deve necessariamente contenere l'insieme $(x) = \mathcal{A} \cdot x = \{ax | a \in \mathcal{A}\}$. È facile mostrare che (x) siffatto è un ideale (esercizio), inoltre (x) contiene x (in quanto $1 \in \mathcal{A}$ e quindi $x = 1 \cdot x$). Dunque (x) è il più piccolo ideale contenente x.

Definizione 6.144. Un ideale I di un anello $\mathcal{A}$ generato da un elemento x di $\mathcal{A}$ (ovvero $I = (x)$) si dice **principale**.

Analizziamo adesso il caso di S finito di cardinalità $n > 1$: $S = \{x_1, \ldots, x_n\}$. Generalizzando quanto visto nel caso precedente si ha che:

$$(x_1, \ldots, x_n) = \mathcal{A}x_1 + \ldots + \mathcal{A}x_n = \{a_1x_1 + \ldots + a_nx_n | a_i \in \mathcal{A}\}$$

La dimostrazione che $(x_1, \ldots, x_n)$ è un ideale e che contiene S è del tutto analoga alla precedente. Ci resta da mostrare che $(x_1, \ldots, x_n)$, come definito, è il più piccolo ideale contenente S. (S) deve contenere $\mathcal{A}x_1, \ldots, \mathcal{A}x_n$. Il più piccolo contenente $\mathcal{A}x_1$ e $\mathcal{A}x_2$ è per la Proposizione 6.143 l'ideale $\mathcal{A}x_1 + \mathcal{A}x_2$. Procedendo per induzione si dimostra che effettivamente $(S) = \mathcal{A}x_1 + \ldots + \mathcal{A}x_n$.

Supponiamo infine $S = \{x_i\}_{i \in I}$ con I infinito. Si dimostra che:

$$(S) = \{a_{i_1}x_{i_1} + \ldots + a_{i_n}x_{i_n} | n \geq 1,\ i_1, \ldots, i_n \in I,\ a_{i_j} \in \mathcal{A}\}.$$

Esempio 6.145. Sia $A = \mathbb{Z}$ e $I = m\mathbb{Z} = (m)$, $J = n\mathbb{Z} = (n)$ allora:

- $I \cap J = (m) \cap (n) = ([m, n])$. Cioè gli elementi in comune ai multipli di m e di n, sono i multipli del loro minimo comun multiplo.
- $I + J = (m) + (n) = ((m, n))$, infatti $I + J$ è un ideale di $\mathbb{Z}$, quindi del tipo (d) per un certo $d \in \mathbb{Z}$. Inoltre la condizione necessaria e sufficiente affinchè (d) contenga sia (m) che (n) è che::

  $$(d) \supseteq (m) \leftrightarrow m \in (d) \leftrightarrow m = dt$$
  $$(d) \supseteq (n) \leftrightarrow n \in (d) \leftrightarrow n = dh$$

  Tra tutti i d divisori comuni di m e n, dobbiamo quindi scegliere quello più grande per avere il più piccolo ideale contenente (m) e (n).

Proposizione 6.146. *Un ideale I di $\mathcal{A}$ è proprio se e solo se $1 \notin I$.*

Dimostrazione. Se $1 \notin I$, allora $I \neq \mathcal{A}$ (ricordiamo che stiamo considerando anelli commutativi con unità).

Viceversa se $1 \in I$, allora I contiene $(1) = \mathcal{A}$, quindi $I = \mathcal{A}$ non sarebbe proprio. □

Esercizio 6.147. *Un ideale I è proprio se e solo se $I \cap \mathcal{A}^* = \emptyset$.*

Svolgimento. Se $I \cap \mathcal{A}^* = \emptyset$, allora, essendo $1 \in \mathcal{A}^*$, $I \neq \mathcal{A}$.

Viceversa supponiamo che esista $x \in I \cap \mathcal{A}^*$, allora esiste in $\mathcal{A}$ l'inverso x^{-1} di x. Perciò $1 = x \cdot x^{-1} \in I$ e per la Proposizione 6.146, I non sarebbe proprio.

Osservazione 6.148. Dall'Esercizio 6.147 segue che, nel caso di ideali I generati da un elemento x ($I = (x)$), x è invertibile se e solo se $(x) = \mathcal{A}$.

Proposizione 6.149. *Gli unici ideali di un anello $\mathcal{A}$ (commutativo con unità), sono $\{0\}$ e $\mathcal{A}$ se e solo se $\mathcal{A}$ è un campo.*

Dimostrazione. $\Leftarrow$) Supponiamo che $\mathcal{A}$ sia un campo, allora un ideale I di $\mathcal{A}$ o è l'ideale banale $I = \{0\}$, oppure contiene un elemento invertibile di $\mathcal{A}$ e quindi $I = \mathcal{A}$ (Esercizio 6.147).
$\Rightarrow$) Supponiamo che $\mathcal{A}$ abbia come unici ideali $\mathcal{A}$ e $\{0\}$. Se esistesse in $\mathcal{A}$ un elemento x tale che $x \neq 0$ e $x \notin \mathcal{A}^*$, l'ideale $I = (x)$ sarebbe proprio ($1 \notin I$) e diverso da $\{0\}$ ($x \in I$). □

Definizione 6.150. Siano I, J due ideali di un anello $\mathcal{A}$, definiamo **l'ideale prodotto** tra I e J (notazione IJ) l'ideale generato dai prodotti tra gli elementi di I e J. Abbiamo:

$$IJ = \{x_1y_1 + ... + x_ny_n | x_i \in I,\ y_i \in J,\ n > 0\}.$$

Esercizio 6.151. *Dati I, J ideali di un anello $\mathcal{A}$, dimostrare che l'insieme IJ, definito in 6.150 è effettivamente un ideale di $\mathcal{A}$ e che $IJ \subset I \cap J$.*

Svolgimento. Mostriamo che effettivamente IJ appena definito è un ideale di A.

IJ è un sottogruppo additivo, infatti non è vuoto ($0 \in I$ e $0 \in J$, dunque $0 \cdot 0 = 0 \in IJ$). Inoltre dati v, w in IJ, ovvero:

$$v = \sum_{i=1}^{n} x_i y_i, \quad w = \sum_{j=1}^{m} x'_j y'_i$$

si ha:

$$-(v+w) = -(\sum_{i=1}^{n} x_i y_i + \sum_{j=1}^{m} x'_j y'_j)$$

E dunque $-(v+w)$ appartiene ad IJ in quanto uguale a:

$$(-x_1)y_1 + \ldots (-x_n)y_n + (-x'_1)y'_1 + \ldots (-x'_m)y'_m$$

Infine IJ verifica la proprietà moltiplicativa di un ideale, infatti per ogni $a \in \mathcal{A}$ e per ogni $v \in IJ$ ($v = \sum_{i=1}^{n} x_i y_i$), si ha che:

$$a \sum_{i=1}^{n} x_i y_i = \sum_{i=1}^{n} \underbrace{(ax_i)}_{\in I} \underbrace{y_i}_{\in J} \in IJ$$

$IJ \subseteq I \cap J$. Basta osservare che $I \cap J$ contiene i generatori xy al variare di x in I e y in J:

$$\begin{matrix} \underbrace{x}_{\in I} \cdot \underbrace{y}_{\in A} \in I \\ \underbrace{x}_{\in A} \cdot \underbrace{y}_{\in J} \in J \end{matrix} \Rightarrow x \cdot y \in I \cap J$$

Proposizione 6.152. *Siano I e J due ideali di un anello A tali che $I + J = A$ allora:*

$$I \cap J = I \cdot J.$$

Dimostrazione. Sappiamo che in generale vale: $I \cdot J \subseteq I \cap J$, dobbiamo mostrare che con l'ipotesi fatta vale anche il contenimento inverso, cioè $I \cap J \subseteq I \cdot J$. Per ipotesi esistono $i \in I$ e $j \in J$ tali che: $i + j = 1$. Allora per ogni x di A si ha: $x \cdot i + x \cdot j = x$. Se $x \in I \cap J$ allora $x \cdot i \in I \cdot J$ e $x \cdot j \in I \cdot J$ e quindi anche la loro somma, cioè x sta in $I \cdot J$. □

Studiate alcune delle proprietà degli ideali, per proseguire con il parallelo tra gruppi e anelli, mostriamo che, dati $(\mathcal{A}, +, \cdot)$ anello e un suo ideale I, è possibile dare una struttura di anello ad $\mathcal{A}/I$ l'insieme delle classi laterali di I (che è un sottogruppo normale del gruppo commutativo $(\mathcal{A}, +)$).

Teorema 6.153. *Dato un anello $(\mathcal{A}, +, \cdot)$ e un ideale I di $\mathcal{A}$ consideriamo l'insieme $\mathcal{A}/I$ su cui sono definite somma e prodotto come segue:*

$$(x + I) + (y + I) \overset{def}{=} (x + y) + I$$

$$(x + I) \cdot (y + I) \overset{def}{=} (x \cdot y) + I$$

Allora $(\mathcal{A}/I, +, \cdot)$ è un anello detto **anello quoziente** *di $\mathcal{A}$.*

DIMOSTRAZIONE. Sappiamo che $\mathcal{A}/I$ è un gruppo per l'addizione in quanto, come notato, I è un sottogruppo normale additivo. Dobbiamo mostrare che la definizione di prodotto è una buona definizione (ovvero che non dipende dalla scelta dei rappresentanti) e che con questo prodotto $\mathcal{A}/I$ è un anello. Lasciamo per esercizio la verifica delle proprietà di anello e mostriamo che il prodotto è ben definito. Siano $x' \in x + I$ e $y' \in y + I$. Ovvero esistono $\alpha, \beta \in I$ tali che $x' = x + \alpha$ e $y' = y + \beta$. Mostriamo che $(x + I) \cdot (y + I) = (x' + I) \cdot (y' + I)$:

$$x' \cdot y' = (x + \alpha) \cdot (y + \beta) = x \cdot y + \underbrace{\alpha \cdot y + x \cdot \beta + \alpha \cdot \beta}_{\in I} \in x \cdot y + I$$

□

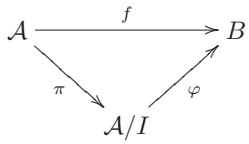
Esempio 6.154. $\mathbb{Z}/m\mathbb{Z}$ è un esempio di anello ottenuto come quoziente di $\mathbb{Z}$ con l'ideale $m\mathbb{Z}$.

Esercizio 6.155. *Dato un anello $(\mathcal{A}, +, \cdot)$ e un ideale I di $\mathcal{A}$ dimostrare che la proiezione $\pi_I : \mathcal{A} \longrightarrow \mathcal{A}/I$ definita da: $\pi(x) = x + I$ è un omomorfismo di anelli.*

Teorema 6.156. *Gli ideali sono tutti e soli i nuclei degli omomorfismi di anelli.*

DIMOSTRAZIONE. Abbiamo già visto che il nucleo di un omomorfismo di anelli è un ideale. Viceversa sia I un ideale di un anello $(\mathcal{A}, +, \cdot)$, allora I è nucleo dell'omomorfismo $\pi_I : \mathcal{A} \longrightarrow \mathcal{A}/I$. □

Teorema 6.157 (Teorema di omomorfismo per anelli)**.** *Sia $f : \mathcal{A} \longrightarrow B$ un omomorfismo di anelli e indichiamo con I il nucleo di f. Allora esiste uno e un solo omomorfismo di anelli iniettivo $\varphi : \mathcal{A}/I \longrightarrow B$ tale che il diagramma seguente sia commutativo:*



Inoltre φ è surgettivo se e solo se f è surgettivo.

DIMOSTRAZIONE. Per il teorema di omomorfismo per gruppi ci basta dimostrare che φ è un omomorfismo di anelli:

$$\varphi((x + I) \cdot (y + I)) = \varphi((x \cdot y) + I) = f(x \cdot y) = f(x) \cdot f(y) = \varphi(x + I) \cdot \varphi(y + I)$$

□

Corollario 6.158. *Sia $f : \mathcal{A} \longrightarrow B$ un omomorfismo di anelli surgettivo, allora c'è corrispondenza biunivoca tra ideali di $\mathcal{A}$ contenenti il nucleo di f e ideali di B.*

DIMOSTRAZIONE. Sappiamo già che i sottogruppi di $\mathcal{A}$ che contengono $I = Ker\ f$ sono in corrispondenza biunivoca con i sottogruppi di B. Bisogna mostrare che se J è un ideale di $\mathcal{A}$ che contiene I allora $f(J)$ è un ideale di B e viceversa se J' è un ideale di B allora esiste J ideale di $\mathcal{A}$ che contiene I con $f(J) = J'$.

- Sia J un ideale di $\mathcal{A}$. Per ogni $b \in B$ esiste $a \in \mathcal{A}$ tale che $f(a) = b$ in quanto f è surgettivo e per ogni $y \in f(J)$ per definizione esiste $x \in J$ tale che $f(x) = y$. Dobbiamo mostrare che by e yb appartengono a $f(J)$:
$$\begin{cases} by = f(a)f(x) = f(\underbrace{ax}_{\in J}) \in f(J) \\ yb = f(x)f(a) = f(\underbrace{xa}_{\in J}) \in f(J) \end{cases}$$
- Viceversa sia J la controimmagine in $\mathcal{A}$ di J', dobbiamo mostrare che J è un ideale di $\mathcal{A}$. Cioè per ogni $a \in \mathcal{A}$ e per ogni $x \in J$ ax e xa devono appartenere ad $\mathcal{A}$. Questo segue dal fatto che $f(ax) = f(a)f(x)$ e $f(xa) = f(x)f(a)$ appartengono a J'.

□

Esempio 6.159. Consideriamo l'omomorfismo surgettivo di anelli $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$. C'è corrispondenza biunivoca tra gli ideali di $\mathbb{Z}$ che contengono $m\mathbb{Z}$ ($k\mathbb{Z}$ con $k|m$) e gli ideali di $\mathbb{Z}/m\mathbb{Z}$ ($k\mathbb{Z}/m\mathbb{Z} = \pi(k\mathbb{Z})$).

Definizione 6.160. Si dice **caratteristica** di un anello $\mathcal{A}$ (useremo la notazione $char(\mathcal{A})$) il più piccolo intero positivo m (se esiste) per cui $\forall x \in \mathcal{A}$ si ha $mx = 0$. Se un tale intero positivo non esiste si definisce la caratteristica di $\mathcal{A}$ uguale a 0.

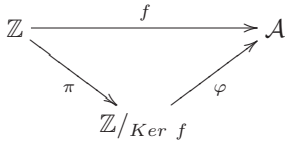
Proposizione 6.161. *$char(\mathcal{A}) = o(1)$ (dove con $ord(1)$ abbiamo indicato l'ordine di 1 per l'operazione di somma).*

Dimostrazione. Se $ord(1) = m < \infty$, per definizione m divide $char(\mathcal{A})$, inoltre, per ogni x in $\mathcal{A}$
$$mx = \underbrace{x + \ldots + x}_{m \text{ volte}} = 1 \cdot x + \ldots + 1 \cdot x = (\underbrace{1 + \ldots + 1}_{m \text{ volte}})x = 0 \cdot x = 0$$
Se $ord(1) = \infty$, allora non esiste $z > 0$ in $\mathbb{Z}$, tale che $zx = 0$ per ogni $x \in \mathcal{A}$ e quindi per definizione $char(\mathcal{A}) = 0$. □

Esempio 6.162. Un esempio di anello con caratteristica finita che conosciamo è $\mathbb{Z}/m\mathbb{Z}$, che ha caratteristica m. Un esempio di anello con caratteristica 0 è $\mathbb{Z}$. La seguente proposizione afferma che questi esempi sono dei rappresentanti degli anelli con caratteristica rispettivamente finita e zero.

Proposizione 6.163. *Sia $\mathcal{A}$ un anello se $char(\mathcal{A}) = m$ ($char(\mathcal{A}) = 0$) allora $\mathcal{A}$ contiene un anello isomorfo a $\mathbb{Z}/m\mathbb{Z}$ ($\mathbb{Z}$). Il sottoanello di $\mathcal{A}$ isomorfo a $\mathbb{Z}/m\mathbb{Z}$ o a $\mathbb{Z}$ si chiama* **sottoanello fondamentale** *di $\mathcal{A}$.*

Dimostrazione. Consideriamo la seguente applicazione tra $\mathbb{Z}$ e $\mathcal{A}$:
$$f(n) = n \cdot 1 = \underbrace{1_{\mathcal{A}} + \ldots + 1_{\mathcal{A}}}_{n \text{ volte}}$$
f è un omomorfismo di anelli, dunque dal seguente diagramma:



si ha che, se $char(\mathcal{A}) = m$ allora $Ker\ f = m\mathbb{Z}$ (l'insieme dei numeri che moltiplicati per 1 fanno zero), ovvero $\mathcal{A} \supset \mathbb{Z}/m\mathbb{Z}$. Se $char(\mathcal{A}) = 0$ allora $Ker\ f = \{0\}$ e quindi $\mathcal{A} \supset \mathbb{Z}$. □

Definizione 6.164. Un ideale proprio P di un anello $\mathcal{A}$ si dice **primo** se:

$$xy \in P \Rightarrow \quad x \in P \quad \text{oppure} \quad y \in P.$$

Proposizione 6.165. *Un ideale P di $\mathcal{A}$ è primo se e solo se $\mathcal{A}/P$ è un dominio di integrità.*

DIMOSTRAZIONE. La condizione: xP, yP in $\mathcal{A}/P$ diversi dalla classe laterale P (lo 0 di $\mathcal{A}/P$) implica xyP (ovvero $xP \cdot yP$) diversa da P, equivale alla condizione: se x e y non appartengono a P allora xy non appartiene a P. □

Definizione 6.166. Un ideale proprio M di un anello $\mathcal{A}$ si dice **massimale** se, dato I ideale di $\mathcal{A}$ si ha che:

$$M \subseteq I \subseteq \mathcal{A} \ \Rightarrow \ I = M \quad \text{oppure} \quad I = \mathcal{A}$$

Teorema 6.167. *M ideale di $\mathcal{A}$ è massimale se e solo se $\mathcal{A}/M$ è un campo.*

DIMOSTRAZIONE. Considerando la proiezione $\pi : \mathcal{A} \to \mathcal{A}/M$, abbiamo una corrispondenza biunivoca tra ideali I contenenti M e ideali $\overline{I}$ di $\mathcal{A}/M$ (Corollario 6.158).

Se M è massimale, per definizione, gli unici ideali contenenti M in $\mathcal{A}$ sono M ed $\mathcal{A}$. Perciò gli unici ideali di $\mathcal{A}/M$ sono $\pi(M) = \{\overline{0}\}$ e $\pi(\mathcal{A}) = \mathcal{A}/M$. □

Osservazione 6.168. Ogni ideale massimale è primo. Infatti se M è massimale allora A/M è un campo, in particolare è un dominio di integrità.

Esempio 6.169. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti in $\mathbb{Z}$ e sia P l'ideale generato da x: $P = (x)$. Consideriamo l'omomorfismo:

$$\varphi : A \longrightarrow \mathbb{Z} \quad \text{definito da} \quad \varphi(f(x)) = f(0)$$

φ è surgettivo, infatti l'intero z ha come controimmagine qualsiasi polinomio con termine noto z. Il nucleo di φ sono i polinomi che hanno termine noto uguale a 0, cioè sono i polinomi divisibili per x, ovvero $Ker\ \varphi = P$. Dal Teorema di omomorfismo per anelli 6.157 sappiamo che $A/P \cong \mathbb{Z}$. Dunque A/P è un dominio di integrità, ma non è un campo.

In particolare, non è, in generale, vero che un ideale primo sia anche massimale. Altro esempio di questo è l'ideale (0) dell'anello degli interi $\mathbb{Z}$, che è primo ma non massimale.

Esercizio 6.170. *Sia $\mathcal{A}$ un anello con unità tale che, per ogni $x \in \mathcal{A}$, $x^2 = x$. Dimostrare che $\mathcal{A}$ è commutativo e che se $\mathcal{A}/I$ ha 2 elementi allora I è un ideale primo.*

Svolgimento. Osserviamo che per ogni $x \in \mathcal{A}$ si ha:

$$\begin{cases} (x+x)^2 = x + x \\ (x+x)^2 = x^2 + x^2 + 2x = x + x + 2x \end{cases} \Rightarrow 2x = 0$$

In particolare per ogni $x \in \mathcal{A}$ vale $x = -x$. Per ogni coppia di elementi x, y in $\mathcal{A}$, si ha:

$$x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$

ovvero $xy = -yx$, ma per ciò che abbiamo appena osservato, $-yx = yx$ e dunque $xy = yx$.

Infine, supponiamo che $\mathcal{A}/I$ abbia 2 elementi distinti: $\bar{e}$ (la classe laterale I) e $\bar{x}$. Sia $z \cdot y \in I$, dobbiamo dimostrare che $z \in I$ oppure $y \in I$. Se così non fosse, indicando con π la proiezione da $\mathcal{A}$ in $\mathcal{A}/I$, avremmo $\pi(z) = \pi(y) = \bar{x}$. Conseguentemente, sfruttando il fatto che la proiezione π è un omomorfismo:

$$\bar{e} = \pi(z \cdot y) = \pi(z) \cdot \pi(y) = \bar{x} \cdot \bar{x} = \pi(x) \cdot \pi(x) = \pi(x^2) = \pi(x) = \bar{x}$$

E questo è assurdo, in quanto avevamo supposto $\bar{e} \neq \bar{x}$.

Se x è un elemento non invertibile di un anello $\mathcal{A}$, sappiamo che l'insieme degli ideali propri di $\mathcal{A}$ contenenti x è non vuoto (Esercizio 6.147). Vogliamo mostrare che esiste un ideale massimale M di $\mathcal{A}$ contenente x. Per far questo avremo bisogno del Lemma di Zorn, che enunciamo senza dimostrazione.

Sia X un insieme ordinato, si dice che un sottoinsieme C di X è **una catena** se è totalmente ordinato, cioè:

$$\forall c_1, c_2 \in C \quad c_1 \leq c_2 \text{ oppure } c_2 \leq c_1.$$

Lemma 6.171 (Lemma di Zorn)**.** *Sia X un insieme ordinato tale che ogni catena $C \subseteq X$ possiede un estremo superiore. Allora per ogni $x \in X$ esiste un elemento massimale $m \in X$ tale che $m \geq x$.*

Proposizione 6.172. *Sia $\mathcal{A}$ un anello e x un elemento di $\mathcal{A}$ non invertibile. Allora esiste un ideale massimale M di $\mathcal{A}$ contenente x.*

Dimostrazione. Consideriamo l'insieme X degli ideali propri di $\mathcal{A}$ contenenti l'elemento x. Come osservato $X \neq \emptyset$ in quanto $(x) \in X$. Per poter applicare il lemma di Zorn, dobbiamo definire una relazione d'ordine su X. Dati $I, J \in X$ diremo che:

$$I \leq J \overset{def}{\Leftrightarrow} I \subseteq J$$

La condizione per poter applicare il lemma di Zorn è che ogni catena ascendente di X (secondo l'ordine appena definito) ammetta un maggiorante. Consideriamo dunque una catena ascendente C di elementi di X e l'ideale $J = \cup_{I \in C} I$. Mostriamo che J è un ideale proprio di X (il fatto che sia un maggiorante di questa catena è un'ovvia conseguenza della definizione della relazione d'ordine su X, in quanto J contiene ogni I in C.)

(1) 0 appartiene ad ogni $I \in C$, quindi $0 \in J$.
(2) Se $x, y \in J$, allora esistono I, T in C tali che $x \in I$ e $y \in T$. Supponiamo $I \subset T$ (il caso opposto è del tutto analogo), allora $x \in T$. Essendo T un ideale $x + y \in T$ e dunque $x + y \in J$.
(3) Se $x \in J$ allora esiste I in C tale che $x \in I$. Essendo I un ideale da questo segue che $-x \in I$ e dunque $-x \in J$.
(4) Se $a \in \mathcal{A}$ e $x \in J$, allora esiste I in C per cui $x \in I$, da cui $ax \in I$ e quindi $ax \in J$.
(5) Se 1 appartenesse a J, allora esisterebbe I in C per cui $1 \in I$. Questo non può essere perché C è una catena di ideali propri di $\mathcal{A}$.

Applicando il lemma di Zorn esiste M massimale in X. Per come abbiamo definito la relazione d'ordine su X, il massimale coincide con la definizione di ideale massimale. Infatti sia I un ideale che contiene M, in particolare $x \in I$, dunque se I appartiene

a X può essere solo M, se invece non appartiene ad X, significa che I non è proprio, cioè $I = \mathcal{A}$. □

Proposizione 6.173. *Se l'insieme J degli elementi non invertibili di un anello $\mathcal{A}$ è un ideale, allora è l'unico ideale massimale di $\mathcal{A}$.*

Dimostrazione. Ogni ideale proprio I di $\mathcal{A}$ non contiene invertibili (Esercizio 6.147). Dunque ogni ideale proprio I di A è contenuto in J. □

Possiamo *parafrasare* l'enunciato della Proposizione 6.173 come segue: se $\mathcal{A}$ ha un unico ideale massimale M, allora $M = A \setminus A^*$.

Definizione 6.174. Se un anello $\mathcal{A}$ ha un unico ideale massimale I, I si dice **ideale massimo**.

Esempio 6.175. Consideriamo l'anello $\mathbb{Z}/_{p^n\mathbb{Z}}$. Gli elementi non invertibili sono gli x, tali che $(x, p^n) > 1$. Ma:

$$(x, p^n) > 1 \Leftrightarrow (x, p) > 1$$

quindi sono tutti i numeri non primi con p, ovvero multipli di p. (p) è un ideale massimo (Proposizione 6.173).

Mostriamo adesso che è vero anche una sorta di viceversa della Proposizione 6.173.

Proposizione 6.176. *Se l'insieme degli elementi non invertibili di un anello $\mathcal{A}$ non è un ideale di $\mathcal{A}$, allora non esiste un ideale massimo in $\mathcal{A}$.*

Dimostrazione. Indichiamo con B l'insieme degli elementi non invertibili di $\mathcal{A}$ e sia I un ideale massimale di $\mathcal{A}$. Per ipotesi, esiste un elemento $b \in B \setminus I$ e, per la Proposizione 6.172, esiste J, ideale massimale di $\mathcal{A}$ contenente b. J ed I sono ideali massimali di $\mathcal{A}$ distinti, in quanto $b \in J \setminus I$. □

Esercizio 6.177. *Sia $f : \mathcal{A} \to B$ un omomorfismo tra anelli con unità finiti. Dimostrare che:*

(1) *f induce un omomorfismo di gruppi $f^* : \mathcal{A}^* \longrightarrow B^*$.*
(2) *$|Ker\ f^*| \leq |Ker\ f|$.*
(3) *Se $\mathcal{A}$ possiede un ideale massimo M allora $|Ker\ f^*| = |Ker\ f|$.*

Svolgimento. $f|_{\mathcal{A}^*}$ è un omomorfismo di gruppi perché è una restrizione di un omomorfismo, dobbiamo dimostrare che è a valori in B^*. Per definizione di $\mathcal{A}^*$, per ogni $x \in \mathcal{A}^*$ esiste $y \in \mathcal{A}^*$ tale che $xy = 1_{\mathcal{A}}$. Allora:

$$1_B = f(1_{\mathcal{A}}) = f(xy) = f(x)f(y) \Rightarrow f(x), f(y) \in B^*$$

Per dimostrare che $|Ker\ f^*| \leq |Ker\ f|$, osserviamo che:

$$f(x) = f(y) \Leftrightarrow x - y \in Ker\ f$$

Perciò, per ogni elemento y in $Ker\ f^*$, l'elemento $y - 1_{\mathcal{A}}$ è in $Ker\ f$. Da quanto appena osservato, si ha:

$$Ker\ f^* = (1_{\mathcal{A}} + Ker\ f) \cap \mathcal{A}^*$$

Infine, sia M un ideale massimo di $\mathcal{A}$, essendo $Ker\ f$ un ideale di $\mathcal{A}$, si ha:

$$Ker\ f \subseteq M \Rightarrow (1_{\mathcal{A}} + Ker\ f) \subseteq (1_{\mathcal{A}} + M)$$

Gli elementi del tipo $1_{\mathcal{A}} + M$ non possono stare in M, altrimenti $1_{\mathcal{A}}$ starebbe in M e M non sarebbe massimale. Gli elementi della forma $1_{\mathcal{A}} + M$ sono dunque invertibili, quindi:

$$(1_{\mathcal{A}} + Ker\ f) \subseteq (1_{\mathcal{A}} + M) \subseteq \mathcal{A}^* \Rightarrow Ker f^* = (1_{\mathcal{A}} + Ker\ f)$$

Da cui $|Ker\ f^*| = |Ker\ f|$.

Esercizio 6.178 (Radicale di un ideale)**.** *Sia $\mathcal{A}$ un anello e $I, J \subset \mathcal{A}$ ideali. Allora:*

(1) *Il* **radicale** *di I, ovvero il sottoinsieme di A:*

$$\sqrt{I} \stackrel{def}{=} \{x \in \mathcal{A} | \exists n \in \mathbb{N}, \quad x^n \in I\}$$

è un ideale.

(2) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(3) *Se $P \subset \mathcal{A}$ è un ideale primo allora per ogni $n > 0$ $\sqrt{P^n} = P$.*

(4) *Descrivere $\sqrt{m\mathbb{Z}}$.*

Svolgimento. Innanzitutto osserviamo che scegliendo $n = 1$ si ha che $\sqrt{I} \supseteq I$, quindi $0 \in \sqrt{I}$. Inoltre se $x \in \sqrt{I}$ allora esiste n per cui $x^n \in I$ allora $-x^n \in I$. Se n è dispari allora $-x^n = (-x)^n$ e quindi $-x \in \sqrt{I}$. Viceversa se n è pari, osserviamo che $x^n = (-x)^n \in I \Rightarrow -x \in \sqrt{I}$.
Ci rimane da mostrare che se $x, y \in \sqrt{I}$ allora $x + y \in \sqrt{I}$ e che se $a \in \mathcal{A}$ allora $ax \in \sqrt{I}$.
La seconda implicazione è semplice: sappiamo che esiste $n \in \mathbb{N}$ tale che $x^n \in I$ allora $a^n x^n \in I$ (perché I è un ideale e $a^n \in \mathcal{A}$) e di conseguenza $ax \in \sqrt{I}$.
Per quanto riguarda la prima, sappiamo che esistono $n, m \in \mathbb{N}$ tali che $x^n, y^m \in I$, dobbiamo dimostrare che questo implica che esiste $k \in \mathbb{N}$ tale che $(x + y)^k \in I$. Osserviamo che:

$$(x+y)^{n+m} = \sum_{i=0}^{n+m} \left(\begin{array}{c} n+m \\ i \end{array} \right) x^i y^{n+m-i}.$$

Basta mostrare che, per ogni i compreso tra 0 e $n + m$, $x^i y^{n+m-i} \in I$:
Se $i \geq n$ allora:

$$x \in I \rightarrow \underbrace{x^n}_{\in I} \underbrace{x^{i-n}}_{\in \mathcal{A}} \in I \rightarrow \underbrace{x^i}_{\in I} \underbrace{y^{n+m-i}}_{\in \mathcal{A}} \in I.$$

Se $i < n$ allora:

$$n + m - i > m \rightarrow \underbrace{x^i}_{\in \mathcal{A}} \underbrace{y^{n+m-i}}_{\in I} \in I.$$

Per il secondo punto, sappiamo che in generale $I \cap J \supseteq IJ$ dunque sicuramente $\sqrt{I \cap J} \supseteq \sqrt{IJ}$. Facciamo vedere che vale il viceversa. Sia $x \in \sqrt{I \cap J}$, allora esiste $n \in \mathbb{N}$ tale che $x^n \in I \cap J$. Allora $x^{2n} = x^n \cdot x^n \in IJ$ e dunque $x \in \sqrt{IJ}$.
Facciamo vedere ora che $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. Sia $x \in \sqrt{I \cap J}$ allora:

$$\exists n \in \mathbb{N} : \ x^n \in I \cap J \rightarrow \begin{array}{c} x^n \in I \\ x^n \in J \end{array} \rightarrow \begin{array}{c} x \in \sqrt{I} \\ x \in \sqrt{J} \end{array} \rightarrow x \in \sqrt{I} \cap \sqrt{J}.$$

Viceversa sia $x \in \sqrt{I} \cap \sqrt{J}$, allora $x \in \sqrt{I}$ e $x \in \sqrt{J}$, ovvero esistono $n, m \in \mathbb{N}$ tali che:

$$x^n \in I \text{ e } x^m \in J \rightarrow x^{m+n} \in I \cap J \rightarrow x \in \sqrt{I \cap J}.$$

Consideriamo a questo punto P ideale primo. Qualsiasi sia $n \in \mathbb{N}$: se $x \in P$ allora $x^n \in P^n$, ovvero, per definizione $x \in \sqrt{P^n}$. Viceversa se $x \in \sqrt{P^n}$ allora esiste $m \in \mathbb{N}$ tale che $x^m \in P^n$, e quindi essendo $P \supseteq P^n$, $x^m \in P$. Usando il fatto che P è un ideale primo, si ha $x \in P$.
Infine descriviamo $\sqrt{m\mathbb{Z}}$:

$$\sqrt{m\mathbb{Z}} = \{x \in \mathbb{Z} | \exists n \in \mathbb{N} \quad x^n \in m\mathbb{Z}\}$$

Vediamo un esempio numerico per farci un'idea di come possiamo caratterizzare $\sqrt{m\mathbb{Z}}$. Sia $m = 36$, $36 = 2^2 \cdot 3^3$, sia $x \in \sqrt{36\mathbb{Z}}$, osserviamo che:

$$36|x^n \Rightarrow \begin{array}{c} 2^2|x^n \\ 3^2|x^n \end{array} \Rightarrow \begin{array}{c} 2|x \\ 3|x \end{array} \Rightarrow 6|x.$$

Quindi $x \in 6\mathbb{Z}$ ovvero $\sqrt{36\mathbb{Z}} \subseteq 6\mathbb{Z}$. Viceversa sia $x \in 6\mathbb{Z}$, ovvero $x = 6n$ per qualche n intero. $x^2 = 36n^2 \in 36\mathbb{Z}$, perciò $x \in \sqrt{36\mathbb{Z}}$. Concludendo $\sqrt{36\mathbb{Z}} = 6\mathbb{Z}$.
Il procedimento in generale, ricalca quello seguito in questo caso particolare, da cui si conclude che se:

$$m = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$$

è la fattorizzazione in numeri primi di m allora:

$$\sqrt{m\mathbb{Z}} = (p_1 \cdot \ldots \cdot p_k)\mathbb{Z}.$$

Osserviamo che se consideriamo l'anello $\mathbb{Z}/m\mathbb{Z}$ allora i divisori di zero sono gli elementi dell'insieme:

$$\{[x]_m \in \mathbb{Z}/m\mathbb{Z} | (x, m) \neq 1\}$$

mentre un elemento nilpotente in $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$ deve soddisfare la condizione:

$$\exists k \in \mathbb{N} \quad x^k \equiv 0 \ (m) \leftrightarrow m|x^k \leftrightarrow \prod_{i=1}^{k} p_i | x$$

Dunque l'insieme dei nilpotenti è:

$$N = \{[x]_m \in \mathbb{Z}/m\mathbb{Z} | \prod_{i=1}^{k} p_i | x \ \text{ e } \ [x]_m \neq [0]_m\}$$

Esercizio 6.179. *Descrivere e contare i divisori di zero ed i nilpotenti dell'anello* $\mathcal{A} = \mathbb{Z}_{27} \times \mathbb{Z}_{18}$.

Svolgimento. Un elemento $(\overline{a}, \overline{b}) \in \mathbb{Z}_{27} \times \mathbb{Z}_{18}$ è un divisore di zero se esiste $(\overline{c}, \overline{d}) \in \mathcal{A} \setminus \{(\overline{0}, \overline{0})\}$ tale che:

$$(\overline{a}, \overline{b}) \cdot (\overline{c}, \overline{d}) = (\overline{0}, \overline{0}) \Leftrightarrow \begin{array}{l} ac \equiv 0 \ (27) \\ bd \equiv 0 \ (18) \end{array}$$

Questo implica che:

- Se $c = 0$ e $d \neq 0$, allora a può essere un numero qualsiasi, mentre b deve essere un divisore di zero in $\mathbb{Z}_{18}$.
- Se $d = 0$ e $c \neq 0$, analogamente a prima, b può essere un numero qualsiasi mentre a deve essere un divisore di zero in $\mathbb{Z}_{27}$.
- Se $c, d \neq 0$ allora a e b devono essere divisori di zero rispettivamente in $\mathbb{Z}_{27}$ e $\mathbb{Z}_{18}$.

Per contare i divisori di zero di $\mathcal{A}$, basta contare quanti sono gli elementi invertibili di A e toglierli dal totale degli elementi di A, ovvero $27 \cdot 18$.
Un elemento $(\overline{a}, \overline{b}) \in \mathcal{A}$ è invertibile se esiste $(\overline{c}, \overline{d}) \in \mathcal{A}$ tale che:

$$\begin{array}{l} ac \equiv 1\ (27) \\ bd \equiv 1\ (18) \end{array} \Rightarrow \begin{array}{l} a \text{ è invertibile in } \mathbb{Z}_{27} \\ b \text{ è invertibile in } \mathbb{Z}_{18} \end{array}$$

Quindi gli invertibili di A sono $\phi(27) \cdot \phi(18)$ e i nilpotenti:

$$27 \cdot 18 - \phi(27) \cdot \phi(18).$$

I nilpotenti sono, per definizione, gli elementi del tipo $(\overline{a}, \overline{b}) \in \mathcal{A}$ tali che esiste $n \in \mathbb{N}$ con:

$$(\overline{a}, \overline{b})^n = (\overline{a}^n, \overline{b}^n) = (\overline{0}, \overline{0}) \Leftrightarrow \begin{cases} a^n \equiv 0\ (27) \\ b^n \equiv 0\ (18) \end{cases}$$

Quindi sia a che b devono essere nilpotenti, rispettivamente in $\mathbb{Z}_{27}$ e in $\mathbb{Z}_{18}$:

- a nilpotente in $\mathbb{Z}_{27} \Rightarrow\ a = 3k$. Ci sono 9 classi in $\mathbb{Z}_{27}$ di questo tipo.
- b nilpotente in $\mathbb{Z}_{18} \Rightarrow\ b = 6h$. Ci sono 3 classi in $\mathbb{Z}_{18}$ di questo tipo.

Quindi in $\mathcal{A}$ ci sono $9 \cdot 3$ nilpotenti.

Esercizio 6.180. *Siano $\mathcal{A}$ un anello e $x, a \in \mathcal{A}$ due elementi con x nilpotente e a invertibile. Allora $x + a$ è invertibile.*

Svolgimento. Useremo la seguente uguaglianza valida per tutti gli anelli commutativi e per ogni s dispari:

$$a^s + b^s = (a + b) \sum_{i=0}^{s-1} (-1)^i a^{s-1-i} b^i.$$

Supponiamo $a = 1$ allora, per ipotesi, esiste $n \in \mathbb{N}$ tale che $x^n = 0$. Consideriamo k tale che $2k + 1 \geq n$ allora:

$$1 = 1 + x^{2k+1} = (1 + x) \sum_{i=0}^{2k} (-1)^i x^{2k-i}$$

cioè:

$$y = (1 + x) \sum_{i=0}^{2k} (-1)^i x^{2k-i}$$

è l'inverso di $x + 1$.
Consideriamo ora il caso generale in cui $a \in \mathcal{A}$ è invertibile, allora esiste $b \in \mathcal{A}$ tale che $ab = 1$ e dunque $x + a = abx + a = a(bx + 1)$. Abbiamo scritto $x + a$ come il prodotto di a, che è invertibile, per $(bx+1)$. Ora basta osservare che bx è nilpotente, in quanto l'insieme dei nilpotenti è un ideale e dunque per il caso particolare fatto prima, anche $bx + 1$ è invertibile.

Esercizio 6.181. *Sia $\mathcal{A}$ un anello, con $\mathcal{A}[x]$ indichiamo l'anello dei polinomi con coefficienti in $\mathcal{A}$. Sia $f = \sum_{i=0}^{n} a_i x^i \in \mathcal{A}[x]$ allora:*

(1) *f è invertibile se e solo se a_0 è invertibile e $a_1, \ldots, a_n$ sono nilpotenti.*
(2) *f è nilpotente se e solo se $a_0, a_1, \ldots, a_n$ sono nilpotenti.*
(3) *f è un divisore di zero se e solo se esiste $b \in \mathcal{A} \setminus \{0\}$ tale che $bf = 0$.*

Svolgimento. Supponiamo che a_0 sia invertibile e $a_1, \ldots, a_n$ siano nilpotenti, questo implica che $\sum_{i=1}^{n} a_i x^i$ è nilpotente, in quanto l'insieme degli elementi nilpotenti è un ideale. L'Esercizio 6.180 ci dice che $f = a_0 + (\sum_{i=1}^{n} a_i x^i)$ è invertibile.

Viceversa, sia f invertibile, allora esiste $g = \sum_{j=0}^{m} b_j x^j$ tale che:

$$f \cdot g = \sum_{k=0}^{n+m} x^k (\sum_{i+j=k} a_i b_j) = 1$$

in particolare $a_0 b_0 = 1$ cioè a_0 invertibile.
Osserviamo il coefficiente di x^{n+m} nel prodotto tra f e g è: $a_n b_m$. Perciò $a_n b_m = 0$. Analogamente il coefficiente di x^{n+m-1} deve essere uguale a 0, perciò:

$$a_n b_{m-1} + a_{n-1} b_m = 0$$

e moltiplicando per a_n si ottiene:

$$a_n^2 b_{m-1} + a_{n-1} a_n b_m = 0 \rightarrow a_n^2 b_{m-1} = 0.$$

Anche il coefficiente del termine di grado $n + m - 2$ è uguale a 0:

$$a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m = 0$$

e moltiplicando per a_n^2 si ottiene:

$$a_n^3 b_{m-2} + a_{n-1} a_n^2 b_{m-1} + a_{n-2} a_n^2 b_m = 0 \Rightarrow a_n^3 b_{m-2} = 0.$$

Procedendo per induzione su r si ottiene:

$$\forall r \leq m \quad a_n^{r+1} b_{m-r} = 0 \tag{5.1}$$

Infatti per $r = 0$ abbiamo già provato che vale la relazione 5.1. Supponiamo che sia vera per $r - 1$ e proviamola per r, tenendo in mente come abbiamo fatto nei casi $r = 1, 2$. Consideriamo il coefficiente del termine di grado $n + m - r$, che sappiamo essere uguale a 0: $\sum_{i=0}^{r} a_{n-i} b_{m-r+i} = 0$. Moltiplicando per a_n^r si ottiene:

$$a_n^{r+1} b_{m-r} + \underbrace{\sum_{i=1}^{r} a_n^r a_{n-i} b_{m-r+i}}_{= 0 \text{ per ip.ind.}} = 0.$$

Il fatto che la relazione 5.1 valga per qualunque r, ci garantisce che $a_n^{m+1} g(x) = 0$, ma noi sappiamo che $g(x)$ è invertibile, quindi non può essere un divisore di zero. Allora deve essere $a_n^{m+1} = 0$, cioè a_n nilpotente.
Per concludere si procede per induzione osservando che $f - a_n x^n$ è invertibile e ha come coefficiente di grado massimo a_{n-1}.

Se $a_0, a_1, \ldots, a_n$ sono nilpotenti allora $f(x) = \sum_{i=0}^{n} a_i x^i$ è nilpotente in quanto l'insieme dei nilpotenti è un ideale. Viceversa se f è nilpotente allora esiste $k \in \mathbb{N}$ tale che $0 = f(x)^k = a_0^k + x(g(x))^k$ (per un certo $g(x)$). Allora $a_0^k = 0$, cioè a_0 nilpotente. Osserviamo ora che:

$$1 + f(x) = \underbrace{\underbrace{(a_0 + 1)}_{\text{invertibile}} + \sum_{i=1}^{n} a_i x^i}_{\text{invertibile}}$$

quindi per il punto precedente $a_1, \ldots, a_n$ sono nilpotenti.

Passiamo al terzo e ultimo punto richiesto. Un'implicazione è ovvia per definizione di divisore di zero e osservando che $\mathcal{A} \subset \mathcal{A}[x]$. Viceversa supponiamo che f sia un divisore di zero, allora scegliamo $g(x) = \sum_{j=0}^{m} b_j x^j$ di grado minimo tale che $f \cdot g = 0$. Il termine di grado massimo di questo prodotto ha coefficiente $a_n b_m$ che deve essere uguale a 0, allora $a_n g(x)$ ha grado minore strettamente di m. Ma $g(x)$ l'abbiamo scelto di grado minimo, allora deve essere $a_n g(x) = 0$. Dimostriamo per induzione su r che $a_{n-r} g(x) = 0$. Abbiamo già verificato che la relazione vale per $r = 0$. Supponiamo di averla dimostrata per $k < r$. Osserviamo che $f(x)g(x) = 0$, cioè:

$$0 = a_0 g(x) + a_1 x g(x) + \ldots + a_{n-r} x^{n-r} g(x) + \underbrace{\ldots}_{=0 \text{ per ipo.ind.}}$$

Il polinomio $a_{n-r} g(x)$ ha grado minore di n e annulla f, dunque $a_{n-r} g(x) = 0$. Dimostrato che $a_i g(x) = 0$ per tutti gli i compresi tra 0 e n, si ha che:

$$\forall 0 \leq i \leq n \quad a_i \cdot b_m = 0 \Rightarrow b_m f(x) = 0.$$

Esercizio 6.182. *Siano $\mathcal{A}$ un anello e $P_1, \ldots, P_n$ degli ideali primi di $\mathcal{A}$. Se $I \subset \cup_{i=1}^{n} P_i$ è un ideale di $\mathcal{A}$ allora esiste $1 \leq j \leq n$ tale che $I \subset P_j$.*

Svolgimento. Procediamo per induzione su n, dimostrando che: se per ogni i, I non è contenuto in P_i, allora I non è contenuto nemmeno in $\cup_{i=1}^{n} P_i$.
Passo base. Se $n = 1$ l'implicazione è tautologica.
Passo induttivo. Supponiamo che I non sia contenuto in nessuno dei P_i, allora per ipotesi induttiva, per ogni j, non è contenuto nemmeno in $\cup_{i \neq j} P_i$. Cioè:

$$\forall j \ \exists x_j \in I \ x_j \notin P_i \ \forall i \neq j.$$

Allora $x_j \in I \setminus \cup_{i \neq j} P_i$ e quindi $x_j \in P_j$. Scelti questi x_j al variare di j tra 1 e n, consideriamo il seguente elemento di I:

$$y = \sum_{j=1}^{n} (\prod_{i \neq j} x_i)$$

Osserviamo che, per ogni i, $y \notin P_i$ infatti l'addendo di y senza x_i non sta in P_i (perché i P_i sono primi), mentre gli altri addendi sono in P_i. Ovviamente la somma di un elemento di un ideale più un elemento che non sta nell'ideale non può essere nell'ideale. Quindi per ogni i, $y \notin P_i$.

Chiudiamo il paragrafo con la versione per anelli del teorema cinese. Per far questo dobbiamo introdurre il prodotto diretto di anelli. Siano dunque $(\mathcal{A}_1, +_1, \cdot_1)$, $(\mathcal{A}_2, +_2, \cdot_2)$ anelli, vogliamo *indurre* una struttura di anello sul prodotto cartesiano $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$. Similmente al caso dei gruppi si tratta di definire le operazioni componente per componente, dunque per ogni coppia (a_1, a_2), (b_1, b_2) in $\mathcal{A}$ definiamo addizione $+$ e moltiplicazione $\cdot$ in $\mathcal{A}$ come segue:

$$(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2)$$

Esercizio 6.183. *Dimostrare che se $(\mathcal{A}_1, +_1, \cdot_1)$, $(\mathcal{A}_2, +_2, \cdot_2)$ sono anelli (commutativi con identità), allora $(\mathcal{A}, +, \cdot)$ appena definito è un anello (commutativo con identità) e vale:*

$$\mathcal{A}^* = \mathcal{A}_1^* \times \mathcal{A}_2^*$$

Definizione 6.184. Dati $(\mathcal{A}_1, +_1, \cdot_1)$, $(\mathcal{A}_2, +_2, \cdot_2)$ anelli, l'anello $(\mathcal{A}_1 \times \mathcal{A}_2, +, \cdot)$ con le operazioni indotte dalle operazioni di $\mathcal{A}_1$ e $\mathcal{A}_2$ sulle singole componenti è detto anello **prodotto diretto** degli anelli $\mathcal{A}_1$ e $\mathcal{A}_2$.

Teorema 6.185 (Teorema cinese per anelli)**.** *Siano I e J due ideali di A commutativo con unità, tali che $I + J = A$, allora:*

$$A/_{I \cap J} \cong A/I \times A/J$$

Dimostrazione. L'idea è quella di costruire un omomorfismo da A in $A/I \times A/J$ che sia surgettivo e abbia come nucleo $I \cap J$ e quindi usare il teorema di omomorfismo per anelli. Consideriamo $\varphi : A \longrightarrow A/I \times A/J$ definito da:

$$\forall x \in A \quad \varphi(x) = (x + I, x + J).$$

È facile provare che φ è un omomorfismo di anelli. Vogliamo descrivere il nucleo di φ, cioè quali sono gli $x \in A$ tali che:

$$\varphi(x) = (x + I, x + J) = (\overline{0}, \overline{0}) = (I, J)$$

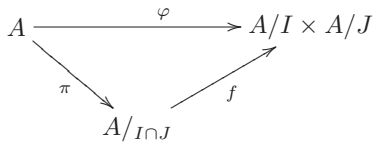
cioè $x \in Ker\ \varphi \Leftrightarrow x \in (I \cap J)$. Dimostrato che $Ker\ \varphi = I \cap J$, facciamo vedere che φ è surgettivo. L'ipotesi che $I + J = A$ equivale al fatto che $1 \in I + J$ (infatti sappiamo che la somma di ideali è un ideale e l'osservazione 6.146 ci dice che un ideale non è proprio se e solo se 1 appartiene all'ideale) cioè che esistono $i \in I$ e $j \in J$ tali che: $i + j = 1$. Allora:

$$\varphi(i) = (\overline{0}, \overline{1}) \quad \varphi(j) = (\overline{1}, \overline{0})$$

e quindi φ è surgettivo, in quanto una controimmagine di un qualsiasi elemento $(\overline{a}, \overline{b})$ di $A/I \times A/J$ è $(a \cdot j + b \cdot i)$, infatti sfruttando il fatto che φ sia un omomorfismo si ha:

$$\varphi(a \cdot j + b \cdot i) = \varphi(a) \cdot \varphi(j) + \varphi(b) \cdot \varphi(i) = (\overline{a}, \overline{0}) + (\overline{0}, \overline{b}) = (\overline{a}, \overline{b}).$$

Come detto dal teorema di omomorfismo per anelli si ha:



E f è un isomorfismo. □

Osservazione 6.186. Dal Teorema 6.185 segue che possiamo enunciare la terza forma del teorema cinese (Teorema 5.159) parlando di isomorfismo di anelli.

6. Quozienti dell'anello $\mathbb{K}[x]$

Sia $f(x)$ un polinomio di grado n in $\mathbb{K}[x]$, consideriamo l'ideale $(f(x))$ generato da $f(x)$:

$$(f(x)) = \{f(x)g(x) | g(x) \in \mathbb{K}[x]\}$$

Dal Teorema 6.153 sappiamo che $\mathbb{K}[x]/(f(x))$ è un anello commutativo con unità, formato dalle classe laterali di $(f(x))$. Vogliamo mostrare alcune proprietà di questo anello che torneranno utili nel capitolo sui campi (e che in quel capitolo dimostreremo con altri strumenti), sottolineando l'analogia con l'anello $\mathbb{Z}/n\mathbb{Z}$.

Proposizione 6.187. *Un insieme di rappresentanti per $\mathbb{K}[x]/(f(x))$ è dato dai polinomi di $\mathbb{K}[x]$ di grado minore del grado n di $f(x)$, unito il polinomio $\{0\}$.*

DIMOSTRAZIONE. Per ogni classe laterale $a(x) + (f(x))$ in $\mathbb{K}[x]/(f(x))$, consideriamo il resto $r(x)$ della divisione euclidea di $a(x)$ con $f(x)$:

$$a(x) = f(x)q(x) + r(x) \;\; r(x) = 0 \;\text{ o }\; deg(r(x)) < deg(f(x))$$

Dunque $a(x)$ appartiene alla classe laterale $r(x) + (f(x))$, ovvero:

$$a(x) + (f(x)) = r(x) + (f(x))$$

Dunque qualsiasi elemento in $\mathbb{K}[x]/(f(x))$ può essere rappresentato da $r(x)+(f(x))$, con $r(x)$ che, essendo il resto di una divisione euclidea per $f(x)$, ha le caratteristiche volute.

Mostriamo adesso che due classi del tipo $r(x)+(f(x))$ sono uguali se e solo se i *resti* rappresentanti sono lo stesso polinomio. Infatti $r_1(x)+(f(x)) = r_2(x)+(f(x))$ se e solo se $r_1(x) - r_2(x)$ appartiene a $(f(x))$. Questo equivale a dire che esiste $c(x)$ tale che:

$$r_1(x) - r_2(x) = c(x)f(x)$$

A primo membro c'è il polinomio nullo o un polinomio di grado strettamente minore di n, a secondo il polinomio nullo (se $c(x) = 0$) o un polinomio di grado maggiore o uguale a n. Dunque:

$$r_1(x) + (f(x)) = r_2(x) + (f(x)) \Leftrightarrow r_1(x) - r_2(x) = 0 \Leftrightarrow r_1(x) = r_2(x)$$

□

Osservazione 6.188. In particolare gli elementi di $\mathbb{K}[x]/(f(x))$ sono tanti quanti i polinomi di grado minore di n in $\mathbb{K}[x]$ più 1, il polinomio nullo. E dunque $\mathbb{K}[x]/(f(x))$ è finito se e solo se è finito $\mathbb{K}[x]$.

D'ora innanzi si intenderà che le classi di $\mathbb{K}[x]/(f(x))$ sono indicate attraverso il rappresentante di grado minore del grado di $f(x)$.

Corollario 6.189. *Sia $f(x) \in \mathbb{K}[x]$ un polinomio di grado n. $\mathbb{K}[x]/(f(x))$ è uno spazio vettoriale su $\mathbb{K}$ di dimensione n.*

DIMOSTRAZIONE. Le verifiche che $\mathbb{K}[x]/(f(x))$ sia uno spazio vettoriale su $\mathbb{K}$ sono lasciate per esercizio. Abbiamo appena dimostrato che $\mathbb{K}[x]/(f(x))$ ha, come insieme dei rappresentanti, l'insieme dei polinomi di grado minore di n unito all'insieme contenente il polinomio nullo; è abbastanza facile mostrare che l'insieme T delle classi delle potenze di x da 0 a $n-1$, è una base di $\mathbb{K}[x]/(f(x))$ come spazio vettoriale su $\mathbb{K}$.

Dalle loro combinazioni lineari infatti si ottengono tutte le classi dei polinomi di grado minore di n e del polinomio 0 (la classe $(f(x))$), dunque T genera $\mathbb{K}[x]/(f(x))$.

Supponiamo adesso esista una combinazione lineare degli elementi di T nulla, ovvero esistano $a_1, \ldots, a_n \in \mathbb{K}$ tali che:

$$\sum_{i=0}^{n} a_i \overline{x^i} = \overline{0}$$

Ovvero:

$$\sum_{i=0}^{n} a_i x^i \in (f(x)) \rightarrow \exists q(x) \in \mathbb{K}[x] : \sum_{i=0}^{n} a_i x^i = q(x)f(x)$$

Sempre per questioni di grado deve essere $\sum_{i=0}^{n} a_i x^i = 0$, ovvero $a_i = 0$ per ogni i. □

È abbastanza semplice caratterizzare gli elementi invertibili e i divisori di zero nell'anello $\mathbb{K}[x]/(f(x))$ e questo ci permette di dare un criterio per sapere se $\mathbb{K}[x]/(f(x))$ è un campo, criterio che per essere applicato necessita di saper trovare la fattorizzazione di $f(x)$ (e questo fa intuire il perché abbiamo dato tanta importanza alla fattorizzazione in $\mathbb{K}[x]$).

Proposizione 6.190. *Considerata la classe laterale* $g(x) + (f(x)) = \overline{g(x)}$ *in* $\mathbb{K}[x]/(f(x))$*, si ha che:*

(1) $\overline{g(x)}$ *è invertibile se e solo se* $(g(x), f(x)) = 1$.
(2) $\overline{g(x)}$ *è un divisore di* 0 *se e solo se* $(g(x), f(x)) \neq 1$.

Dimostrazione. Se $(g(x), f(x)) = 1$, dall'identità di Bézout abbiamo che esistono $t(x), s(x)$ in $\mathbb{K}[x]$ tali che:

$$g(x)t(x) + s(x)f(x) = 1$$

Tale uguaglianza, letta in $\mathbb{K}[x]/(f(x))$ ovvero tramite l'omomorfismo proiezione $\pi_{f(x)}$, è:

$$\overline{g(x)t(x)} = \overline{1}$$

Ovvero $g(x)$ è invertibile in $\mathbb{K}[x]/(f(x))$. Osserviamo come, la dimostrazione del primo punto della proposizione fornisca un metodo per trovare l'inverso della classe $\overline{g(x)}$: si tratta dell'immagine di $t(x)$ (proveniente dall'identità di Bézout) modulo $f(x)$. Ovvero della classe $\overline{r(x)}$ in $\mathbb{K}[x]/(f(x))$, dove $r(x)$ è il resto della divisione euclidea di $t(x)$ con $f(x)$.

Per il secondo punto osserviamo che, se $(g(x), f(x)) = 1$, abbiamo appena dimostrato che $\overline{g(x)}$ è invertibile, e dal Lemma 6.24 segue che $\overline{g(x)}$ non può essere un divisore dello 0. Se invece $(g(x), f(x)) = d(x) > 1$, allora esiste $s(x), t(x) \in \mathbb{K}[x]$ tali che:

$$f(x) = s(x)d(x) \quad g(x) = t(x)d(x)$$

Allora:

$$g(x)s(x) = t(x)\underbrace{d(x)s(x)}_{f(x)}t(x) \longrightarrow \overline{g(x)s(x)} = \overline{0}$$

Per concludere basta osservare che $\overline{s(x)} \neq \overline{0}$, in quanto $s(x)$ è diverso da 0 e di grado strettamente minore di $f(x)$. □

Osservazione 6.191. Sia $f(x) \in \mathbb{K}[x]$ e sia $f(x) = \prod_{i=1}^{t} q_i(x)^{\alpha_i}$ la fattorizzazione in irriducibili di $f(x)$ in $\mathbb{K}[x]$. Dimostrare che i nilpotenti in $\mathbb{K}[x]/(f(x))$ sono tutte e sole le classi $\overline{g(x)}$ tali che $g(x)$:

$$g(x) = \prod_{i=1}^{t} q_i(x)^{\beta_i} \quad 1 \leq \beta_i \leq \alpha_i$$

e con $g(x) \neq f(x)$ (cioè non tutti i β_i possono essere uguali ad α_i).

Ovvero i nilpotenti in $\mathbb{K}[x]/(f(x))$ sono tutti i divisori propri di $f(x)$ che contengono tutti i fattori irriducibili di $f(x)$. Sottolineiamo come anche questa sia una proprietà strutturale degli anelli quoziente: osservare che avevamo praticamente fatto la stessa cosa per $\mathbb{Z}/m\mathbb{Z}$ (Esercizio 6.178).

Esercizio 6.192. *Sia* $f(x) = x^4 - 2x^3 + 3x^2 - 4x + 2$*, determinare divisori di zero, nilpotenti ed invertibili nell'anello* $\mathbb{Q}[x]/(f(x))$.

Svolgimento. Abbiamo capito che per determinare nilpotenti, divisori di zero ed invertibili in $\mathbb{K}[x]/(f(x))$ è necessario trovare una fattorizzazione di $f(x)$ in $\mathbb{K}[x]$. In questo caso (esercizio), la fattorizzazione in irriducibili di $f(x)$ in $\mathbb{Q}[x]$ è data da:

$$f(x) = (x-1)^2(x^2+2)$$

Perciò abbiamo:

(1) I nilpotenti in $\mathbb{K}[x]/(f(x))$, devono contenere i fattori irriducibili di $f(x)$, dunque in questo caso sono tutte e sole le classi i cui rappresentanti sono della forma:
$$k(x-1)(x^2+2) \quad k \in \mathbb{Q}$$
(2) I divisori di zero in $\mathbb{K}[x]/(f(x))$ sono i multipli dei fattori irriducibili di $f(x)$ ovvero hanno come rappresentanti i polinomi della forma $(x-1)h(x)$ con $h(x)$ diverso da 0 e di grado minore di 3, oppure della forma $(x^2+2)g(x)$ con $g(x)$ diverso da 0 e di grado minore di 2 (non è una *classificazione disgiunta*, i polinomi $k(x^2+2)(x-1)$, al variare di k in $\mathbb{Q}$, sono divisori dello zero sia della prima forma che della seconda).
(3) Per quanto riguarda gli invertibili sappiamo che, considerato il rappresentante $g(x)$ della classe, deve essere $(g(x), f(x)) = 1$. Dunque: gli invertibili di grado 1 sono tutti i polinomi che non hanno 1 come radice (condizione necessaria e sufficiente per essere multiplo di $x-1$); gli invertibili di grado 2 sono tutti i polinomi che non hanno 1 come radice e che non sono della forma $k(x^2+2)$ con k in $\mathbb{Q}$; gli invertibili di grado 3 sono tutti e soli i polinomi che non hanno 1 come radice e che non sono della forma $h(x)(x^2+2)$ con $h(x)$ in $\mathbb{Q}[x]$ di grado 1.

Proposizione 6.193. *L'anello $\mathbb{K}[x]/(f(x))$ è un campo*[9] *se e solo se $f(x)$ è irriducibile in $\mathbb{K}[x]$.*

Dimostrazione. $\mathbb{K}[x]/(f(x))$ è un campo se e solo se tutti gli elementi non nulli di $\mathbb{K}[x]/(f(x))$ sono invertibili. Dalla Proposizione 6.190 sappiamo che ciò equivale a $f(x)$ è coprimo con tutti i polinomi di grado minore di $f(x)$. Ora basta osservare che questo equivale proprio ad essere irriducibile, infatti se $f(x) = a(x)b(x)$ allora $a(x) = k$ o $b(x) = k$, altrimenti $(f(x), a(x)) = a(x)$ avrebbe grado maggiore di 0. □

7. Campo delle frazioni di un dominio d'integrità

In questo paragrafo, vogliamo generalizzare a qualsiasi dominio d'integrità D, la costruzione del campo dei razionali $\mathbb{Q}$ a partire dall'anello $\mathbb{Z}$. Ricordiamo che l'introduzione dei razionali permette di risolvere tutte le equazioni di primo grado a coefficienti interi $ax = b$, con $a \neq 0$. Consideriamo un sottoinsieme S di D tale che:

(1) $0 \notin S$
(2) $1 \in S$
(3) S è moltiplicativamente chiuso, cioè: $s, t \in S \Rightarrow s \cdot t \in S$.

Con in mente l'esempio della costruzione dei razionali a partire dagli interi, definiamo sull'insieme $D \times S$ delle coppie (a, s), con a in $\mathcal{A}$ e s in S, la seguente relazione $\sim$:

$$(a, s) \sim (b, t) \Leftrightarrow at = bs$$

[9]Nel capitolo sui campi dimostreremo questo risultato con altri strumenti.

Esercizio 6.194. *Dimostrare che $\sim$, appena introdotta, è una relazione di equivalenza su $D \times S$.*

Consideriamo l'insieme $S^{-1}D = \{(a,s) | a \in D,\ s \in S\}/_\sim$, delle classi di equivalenza rispetto a $\sim$ in $D \times S$ e denotiamo la classe di equivalenza della coppia (a,s) con $\dfrac{a}{s}$.

Definiamo una addizione e una moltiplicazione sull'insieme $S^{-1}D$, proseguendo nel parallelo con la costruzione di $\mathbb{Q}$ a partire da $\mathbb{Z}$:

$$\frac{a}{s} + \frac{b}{t} \stackrel{def}{=} \frac{at+bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} \stackrel{def}{=} \frac{ab}{st} \tag{7.1}$$

Esercizio 6.195. *Dimostrare che le definizioni di addizione e moltiplicazione in $S^{-1}D$ (7.1), sono buone definizioni, cioè non dipendono dalla scelta dei rappresentanti delle classi di equivalenza.*

Esercizio 6.196. *Dimostrare che con le operazioni di addizione e moltiplicazione introdotte, $S^{-1}D$ è un dominio d'integrità (con elemento neutro per l'addizione dato dalla classe $\dfrac{0}{1}$, ed inverso di $\dfrac{a}{b}$ dato da $\dfrac{-a}{b}$).*

Dimostriamo adesso che $S^{-1}D$ è un ampliamento di D, in quanto ne contiene una copia isomorfa.

Proposizione 6.197. *La funzione $f : D \longrightarrow S^{-1}D$, che ad ogni a in D associa $f(a) = \dfrac{a}{1}$, è un omomorfismo iniettivo.*

Dimostrazione. Che f sia un omomorfismo di anelli segue dal fatto che:

$$f(a) + f(b) = \tfrac{a}{1} + \tfrac{b}{1} = \tfrac{a\cdot 1 + b\cdot 1}{1} = \tfrac{a+b}{1} = f(a+b)$$
$$f(a) \cdot f(b) = \tfrac{a}{1} \cdot \tfrac{b}{1} = \tfrac{ab}{1} = f(ab)$$

f è iniettivo. Infatti, in $S^{-1}D$, la classe degli elementi neutri per la addizione è costituita da tutti gli elementi della forma $\dfrac{0}{s}$, con $s \in S$. Il nucleo di f è costituito da tutti gli $a \in D$ tali che $\dfrac{a}{1} \sim \dfrac{0}{1}$, ovvero tali che $a \cdot 1 = 0 \cdot 1$. Dunque $Ker\ f = \{0\}$. □

Esercizio 6.198. *Se D è un dominio di integrità e $S = D \setminus \{0\}$, allora $S^{-1}D$ è un campo.*

Svolgimento. Che $S^{-1}D$ sia un campo segue dal fatto che per ogni suo elemento $\dfrac{a}{s}$ diverso da 0, si ha che a è diverso da zero. Dunque $\dfrac{s}{a}$ appartiene a $S^{-1}D$ ed è l'inverso di $\dfrac{s}{a}$.

Definizione 6.199. Se D è un dominio d'integrità e $S = D \setminus \{0\}$, il campo $S^{-1}D$ è detto **campo delle frazioni di** D

Esempio 6.200. $\mathbb{Q}$ è il campo delle frazioni di $\mathbb{Z}$.

Corollario 6.201. *Per ogni dominio d'integrità D, esiste un campo $\mathbb{K}$ che contiene una immagine isomorfa di D (si dice anche: ogni dominio di integrità può essere immerso in un campo).*

Dimostrazione. È una immediata conseguenza della Proposizione 6.197 e dell'Esercizio 6.198. □

Esercizio 6.202. *Sia D un dominio d'integrità e $S \subset D^*$. Dimostrare che $S^{-1}D \cong D$.*

Svolgimento. In queste ipotesi, l'omomorfismo definito nella Proposizione 6.197 è surgettivo. Infatti, per ogni $\frac{a}{s}$ in $S^{-1}D$, se consideriamo l'elemento $a \cdot s^{-1}$ (che esiste perché s per ipotesi è invertibile) di D, si ha:

$$f(a \cdot s^{-1}) = \frac{a \cdot s^{-1}}{1} = \frac{a}{s}$$

Sia I un ideale di D, definiamo il sottoinsieme $S^{-1}I$ di $S^{-1}D$:

$$S^{-1}I = \{(a, s) | a \in I,\ s \in S\}/\sim$$

Proposizione 6.203. *$S^{-1}I$ è un ideale di $S^{-1}D$.*

Dimostrazione. Dobbiamo mostrare che $S^{-1}I$ è un sottogruppo additivo, chiuso per moltiplicazione con qualsiasi elemento di $S^{-1}D$.

Sottogruppo additivo. $S^{-1}I$ non è vuoto, infatti $0 \in I$ e $1 \in S$, dunque $\frac{0}{1} \in S^{-1}I$.

Siano $\frac{a}{s}$ e $\frac{b}{t}$ due elementi di $S^{-1}I$. Per concludere che $S^{-1}I$ è un sottogruppo additivo dobbiamo mostrare che $r = \frac{a}{s} + \frac{-b}{t}$ è un elemento di $S^{-1}I$. Non possiamo a priori affermare che a e b stanno in I, ma che $\frac{a}{s}$ è la classe di equivalenza di una coppia (i, s_1) con $i \in I$ (e analogamente $\frac{b}{t}$ è equivalente ad una coppia (j, t_1) con $j \in I$). Dunque:

$$r = \frac{a}{s} + \frac{-b}{t} \underbrace{=}_{def.\ \sim} \frac{i}{s_1} + \frac{-j}{t_1} \underbrace{=}_{def.\ \sim} \frac{i \cdot t_1 - j \cdot s_1}{s_1 t_1}$$

Ed avendo a *numeratore* un elemento di I, si ha che r appartiene a $S^{-1}I$.

Chiuso per moltiplicazione per $S^{-1}D$. Supponiamo $\frac{a}{s} \in S^{-1}I$ e consideriamo, come nel caso precedente, il rappresentante equivalente $\frac{i}{s_1}$ con $i \in I$. Allora, per ogni elemento $\frac{x}{y}$ in $S^{-1}D$ si ha $\frac{x}{y} \cdot \frac{i}{s_1} = \frac{xi}{s_1 y} \in S^{-1}I$. □

Nella Proposizione 6.203 abbiamo mostrato che gli insiemi della forma $S^{-1}I$, con I ideale di D, sono ideali di $S^{-1}D$. Mostriamo adesso che essi sono tutti e soli gli ideali di $S^{-1}D$.

Proposizione 6.204. *Se J è un ideale di $S^{-1}D$, allora esiste I ideale di D tale che $J = S^{-1}I$.*

Dimostrazione. Forti della dimostrazione della Proposizione 6.203, dovremmo essere in grado di intuire quale ideale I di D cercare come *corrispondente* di un fissato ideale J di $S^{-1}D$. Consideriamo il seguente sottoinsieme di D:

$$I = \left\{ d \in D | \exists \frac{a}{b} \in J, \exists t \in S^{-1} : \frac{a}{b} = \frac{d}{t} \right\}$$

Ovvero I contiene i *numeratori* di tutte le coppie di $S^{-1} \times D$ che appartengono ad una classe di equivalenza di J.

La classe elemento neutro della addizione appartiene a J, dunque $0 \in I$ ed I non è vuoto. Inoltre, se $a, b \in I$, allora esistono $s, t \in S$ tali che $\frac{a}{s}$ e $\frac{b}{t} \in J$ e di conseguenza $\frac{-b}{t} \in J$ (J, in particolare, è un sottogruppo additivo). Essendo J un ideale, si ha:

$$\begin{array}{l} \overbrace{\frac{s}{1}}^{\in S^{-1}D} \cdot \overbrace{\frac{a}{s}}^{\in J} = \underbrace{\frac{a}{1}}_{\in J} \Rightarrow \frac{a+b}{1} \in J \Rightarrow a+b \in I \\ \underbrace{\frac{t}{1}}_{\in S^{-1}D} \cdot \underbrace{\frac{b}{t}}_{\in J} = \underbrace{\frac{b}{1}}_{\in J} \end{array}$$

Dunque I è un sottogruppo additivo di D.

Se $a \in I$ e $x \in A$, allora esiste $s \in S$ tale che $\frac{a}{s} \in J$, sfruttando il fatto che J è un ideale si ha:

$$\frac{x}{1} \cdot \frac{a}{s} = \frac{ax}{s} \in J \Rightarrow \ ax \in I.$$

Dunque I è un ideale di D.

Ci rimane da mostrare che $J = S^{-1}I$. Per definizione di I, $J \subset S^{-1}I$. Viceversa, sia $a \in I$, allora esiste $s \in S$ tale che $\frac{a}{s} \in J$ e:

$$\underbrace{\frac{s}{1}}_{\in D} \cdot \underbrace{\frac{a}{s}}_{\in J} = \underbrace{\frac{a}{1}}_{\in J}$$

Dunque, per ogni t in S:

$$\frac{1}{t} \cdot \frac{a}{1} = \frac{a}{t} \in J$$

Ovvero, se J contiene un elemento della forma $\frac{a}{s}$ con $a \in I$, allora contiene tutti gli elementi con numeratore a e denominatore che varia tra tutti gli elementi di S. Cioè $S^{-1}I \subset J$, e quindi $S^{-1}I = J$ □

Osservazione 6.205. La corrispondenza tra ideali di D e ideali di $S^{-1}D$ potrebbe sembrare biunivoca, ma così non è. Consideriamo infatti un ideale proprio I di D tale che $I \cap S \neq \emptyset$, allora esiste $x \in I \cap S$. Dunque:

$$\frac{x}{x} = \frac{1}{1} \in S^{-1}I$$

Ovvero $S^{-1}I = S^{-1}D$.

In particolare, ci sono ideali propri di A che corrispondono ad ideali banali di $S^{-1}A$.

Esercizio 6.206. *Dimostrare che* $S^{-1}I = S^{-1}D \Leftrightarrow \ I \cap S \neq \emptyset$.

Svolgimento. Un verso della doppia implicazione l'abbiamo appena dimostrato nell'Osservazione 6.205. Supponiamo ora che $I \cap S = \emptyset$ e mostriamo che $S^{-1}I$

non può essere uguale a $S^{-1}D$. Basta mostrare che $S^{-1}I$ non contiene l'identità moltiplicativa di $S^{-1}D$. Osserviamo infatti che:

$$\frac{a}{s} = \frac{1}{1} \Leftrightarrow a = s$$

Sapendo che $I \cap S \neq \emptyset$, abbiamo che $a \in I$ non potrà mai essere uguale ad $a \in S$, dunque $\frac{1}{1} \notin S^{-1}I$.

Esercizio 6.207. *Se I è un ideale primo di D ed S è un sottoinsieme di D disgiunto da I, allora $S^{-1}I$ è un ideale primo di $S^{-1}D$.*

8. Anelli *speciali*: anelli euclidei, PID, UFD

In questo paragrafo presentiamo domini d'integrità particolari[10], ovvero che verificano alcune proprietà aggiuntive rispetto a quelle richieste per essere un dominio d'integrità. Le tre classi di domini di integrità che presenteremo, e che dimostreremo essere una inclusa nell'altra nell'ordine di elencazione qui sotto, hanno nomi che *richiamano* la proprietà aggiuntiva che soddisfano, e sigle che sono legate all'acronimo in Inglese:

(1) **Anelli euclidei**, che indicheremo con EU.
(2) **Domini a ideali principali**, che indicheremo con PID.
(3) **Domini a fattorizzazione unica**, che indicheremo con UFD.

Prima di iniziare le caratteristiche degli *anelli speciali*, diamo delle definizioni e delle proprietà valide per tutti i domini d'integrità.

Definizione 6.208. Dati $a, b \in \mathcal{A}$ con $\mathcal{A}$ dominio d'integrità, si dice che a **divide** b se esiste c in $\mathcal{A}$ tale che $b = ac$.

A partire dalla Definizione 6.208, si possono introdurre, nel modo *naturale* (e già visto nei casi specifici di $\mathbb{Z}$ e $\mathbb{K}[x]$) le definizioni di divisore e multiplo di un elemento, massimo comun divisore e minimo comun multiplo tra due elementi. Si possono anche introdurre i concetti di elemento primo e irriducibile, anch'essi già visti per $\mathbb{Z}$ e $\mathbb{K}[x]$.

Definizione 6.209. Un elemento $x \in \mathcal{A} \setminus \{0\}$ non invertibile si dice **primo** se:

$$\forall a, b \in \mathcal{A} \quad x|ab \;\Rightarrow\; x|a \;\text{ o }\; x|b.$$

Definizione 6.210. Un elemento $x \in \mathcal{A} \setminus \{0\}$ non invertibile si dice **irriducibile** se:

$$\forall a, b \in \mathcal{A} \quad x = ab \;\Rightarrow\; a \text{ invertibile } \text{ o } \; b \text{ invertibile.}$$

Proposizione 6.211. *Se $x \in \mathcal{A}$ è primo allora x è irriducibile.*

Dimostrazione. Se $x = ab$, con $a, b \in \mathcal{A}$, allora in particolare x divide ab. Per ipotesi x divide a oppure x divide b. Supponiamo x divida a (il caso x divide b è del tutto analogo), allora esiste $c \in \mathcal{A}$ tale che $a = xc$, quindi $x = ab = xcb$ e usando la regola di cancellazione si ottiene $1 = cb$, cioè b è invertibile. □

Osservazione 6.212. Dire che $x \in \mathcal{A}$ è primo equivale a dire che l'ideale (x) generato da x è un ideale primo in $\mathcal{A}$. Infatti dati a, b in $\mathcal{A}$, $ab \in (x)$ se e solo se esiste $c \in \mathcal{A}$ tale che $ab = xc$, ovvero se e solo $x|ab$. Da qui la tesi.

[10]Di un tipo dei quali, gli anelli euclidei, abbiamo già anticipato la definizione e discusso alcune proprietà.

8.1. Anelli euclidei. Abbiamo già anticipato la definizione di anello euclideo nei paragrafi precedenti, ma la riportiamo nuovamente per comodità di trattazione.

Definizione 6.213. Un dominio di integrità $\mathcal{A}$ si dice **anello euclideo** se esiste una funzione $d : \mathcal{A} \setminus \{0\} \longrightarrow \mathbb{N}$ (detta anche **funzione grado**) tale che:

(1) $\forall x, y \in \mathcal{A} \setminus \{0\}$ si ha $d(xy) \geq d(x)$.
(2) $\forall x \in \mathcal{A}$ e $\forall y \in \mathcal{A} \setminus \{0\}$ esistono $q, r \in \mathcal{A}$ tali che:

$$x = qy + r \quad \text{con} \quad d(r) < d(y) \quad \text{oppure}^{11} \quad r = 0$$

Abbiamo visto che $\mathbb{Z}$ e $\mathbb{K}[x]$ sono esempi di anelli euclidei, mostriamo un esempio diverso.

Esempio 6.214 (L'anello degli interi di Gauss)**.** Si dicono **interi di Gauss** gli elementi che appartengono al seguente sottoinsieme di $\mathbb{C}$:

$$\mathbb{Z}[i] \stackrel{def}{=} \{a + bi | a, b \in \mathbb{Z}\}$$

dove i è l'unità immaginaria dei numeri complessi, tale che $i^2 = -1$.

Su $\mathbb{Z}[i]$ si possono considerare l'addizione e la moltiplicazione per come sono definite in $\mathbb{C}$:

- $+ : \quad (a + bi) + (c + di) \stackrel{def}{=} (a + c) + (b + d)i.$
- $\cdot : \quad (a + bi) \cdot (c + di) \stackrel{def}{=} (ac - bd) + (ad + cb)i.$

È una semplice verifica, mostrare che $(\mathbb{Z}[i], +, \cdot)$ è effettivamente un anello, chiamato **anello degli interi di Gauss**. Per poter affermare che $\mathbb{Z}[i]$ è un anello euclideo, dobbiamo definire una funzione grado su $\mathbb{Z}[i]$:

$$d(a + bi) \stackrel{def}{=} |a + bi|^2 = a^2 + b^2$$

Mostriamo che la funzione d considerata, effettivamente verifica le proprietà richieste per la funzione grado nella Definizione 6.213 di anello euclideo. Osserviamo che, per ogni x diverso da 0 in $\mathbb{Z}[i]$, $d(x) \geq 1$.

(1) Per ogni $x = a + bi$ e $y = c + di$ di $\mathbb{Z}[i] \setminus \{0\}$, si ha:

$$d(xy) = (ac - bd)^2 + (ad + cb)^2 = a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2acbd + c^2b^2$$

Ovvero, semplificando e raccogliendo a fattore a secondo membro:

$$d(xy) = \underbrace{\overbrace{(a^2 + b^2)}^{\geq 1}}_{d(x)} \cdot \underbrace{\overbrace{(c^2 + d^2)}^{\geq 1}}_{d(y)} \geq \begin{cases} a^2 + b^2 = d(x) \\ c^2 + d^2 = d(y) \end{cases}$$

(2) Consideriamo il piano e un riferimento cartesiano con ascisse intere e ordinate del tipo iz con $z \in \mathbb{Z}$. Siano $\alpha, \beta \in \mathbb{Z}[i]$ con $\beta \neq 0$ e consideriamo tutti i multipli di β in $\mathbb{Z}[i]$, cioè l'ideale (β). Questi individuano nel riferimento cartesiano scelto i vertici di quadrati di lato $|\beta|$. Ogni punto del piano è compreso in uno di questi quadrati, quindi anche α. La distanza di α dal vertice più vicino del quadrato che lo contiene (che ricordiamo è di lato β), è al massimo $\dfrac{|\beta|}{\sqrt{2}}$, quando α si trova al centro del quadrato (e

[11] Osserviamo infatti che la funzione d non è definita nel caso $r = 0$.

dunque non ha un vertice più vicino degli altri). Questo equivale a dire che esiste un multiplo di β, $q\beta$ con $q \in \mathbb{Z}[i]$, tale che:

$$\underbrace{|\alpha - q\beta|}_{d(\alpha - q\beta)} \leq \underbrace{\frac{|\beta|}{\sqrt{2}}}_{\frac{d(\beta)}{2}} \leq d(\beta)$$

Osservazione 6.215. Negli anelli euclidei, esattamente come fatto per $\mathbb{Z}$ e $\mathbb{K}[x]$, a partire dalle proprietà della funzione grado, si possono dimostrare: il teorema di divisione euclidea, il funzionamento dell'algoritmo euclideo per il calcolo del massimo comun divisore, il lemma di Bézout.

Osserviamo ad esempio per quanto riguarda la Proposizione 6.211, in cui si dimostra che in un dominio d'integrità un elemento primo è necessariamente irriducibile, che nei casi di $\mathbb{Z}$ e $\mathbb{K}[x]$ avevamo dimostrato l'equivalenza tra l'essere primo ed irriducibile. Andando ad analizzare la dimostrazione fatta (per esteso nel caso di $\mathbb{Z}$) si osserva che l'implicazione "irriducibile implica primo" usa proprio l'identità di Bézout, che è valida solo per anelli euclidei.

Questo non vuol dire che in altri anelli necessariamente non valga l'equivalenza tra elementi primi e irriducibili, anzi dimostreremo che proprio questa proprietà è una delle caratteristiche comuni delle tre tipologie di dominio che stiamo trattando (euclidei, PID e UFD). La dimostrazione di questo fatto negli anelli non euclidei passerà però per altre vie rispetto a quella mostrata per $\mathbb{Z}$ e che può appunto essere replicata per qualsiasi anello euclideo.

Consideriamo un anello euclideo $\mathcal{A}$, e l'insieme $Im(d) = \{d(x) | x \in \mathcal{A} \setminus \{0\}\}$ (immagine della funzione grado d). $Im(d)$ è un sottoinsieme di $\mathbb{N}$ non vuoto, dunque, per l'assioma del buon ordinamento, esiste m minimo di $Im(d)$. Caratterizzando gli elementi di grado minimo di $\mathcal{A}$, ovvero gli elementi che appartengono all'insieme:

$$M = \{x \in \mathcal{A} \setminus \{0\} | d(x) = m\}$$

si scopre una proprietà significativa degli anelli euclidei.

Proposizione 6.216. *Gli elementi di grado minimo coincidono con $\mathcal{A}^*$, cioè con gli invertibili di $\mathcal{A}$.*

Dimostrazione. Ricordiamo preliminarmente che $x \in \mathcal{A}^*$ se e solo se $(x) = \mathcal{A}$ (Osservazione 6.148).
$\Rightarrow$) Per ogni $y \in \mathcal{A}$ possiamo calcolare la divisione euclidea tra y e x, ovvero esistono $q, r \in \mathcal{A}$ tali che $y = qx + r$ con $d(r) < d(x)$ oppure $r = 0$. Per ipotesi $d(r)$ non può essere minore di $d(x)$ che sappiamo essere il minimo della funzione grado, dunque $r = 0$. Questo significa che per ogni y in $\mathcal{A}$, $y \in (x)$, ovvero $(x) = \mathcal{A}$.
$\Leftarrow$) Se $(x) = \mathcal{A}$, per ogni $y \in \mathcal{A}$ esiste $t \in \mathcal{A}$ tale che $y = xt$ e $d(y) = d(tx) \geq d(x)$, cioè $d(x)$ è il minimo tra i gradi in $\mathcal{A}$. □

Dalla Proposizione 6.216 segue una importante proprietà degli ideali di un anello euclideo.

Proposizione 6.217. *Tutti gli ideali I di un anello euclideo $\mathcal{A}$ sono principali.*

Dimostrazione. Sia I un ideale di $\mathcal{A}$, se $I = \{0\}$ non c'è niente da dimostrare: $I = (0)$. Supponiamo quindi $I \neq \{0\}$, vogliamo mostrare che I è generato da un suo elemento di grado minimo. Consideriamo dunque $m = min\{d(x) | x \in I \setminus \{0\}\}$

e sia $a \in I \setminus \{0\}$ tale che $d(a) = m$: dimostriamo che $I = (a)$. Sicuramente $(a) \subseteq I$, visto che $a \in I$.

Viceversa sia $x \in I$, allora esistono $q, r \in A$ tali che $x = qa + r$, con $d(r) < d(a)$ o $r = 0$. Osserviamo che:

$$r = \underbrace{x}_{\in I} - q \cdot \underbrace{a}_{\in I} \Rightarrow r \in I$$

Dunque $r = 0$ e $x = qa$, ovvero $x \in (a)$. □

8.2. Domini a ideali principali - PID.

Definizione 6.218. Un dominio di integrità si dice un **dominio a ideali principali** se tutti i suoi ideali sono principali.

Abbiamo osservato (Proposizione 6.217) che un anello euclideo è a ideali principali, dunque gli esempi di anelli euclidei visti sono anche esempi di domini a ideali principali. Non è vero in generale il viceversa: cioè l'insieme degli anelli euclidei è strettamente contenuto nell'insieme dei domini a ideali principali (ma non è banale mostrare, giustificando il perché, esempi di domini a ideali principali che non sono euclidei).

Il seguente esercizio dimostra che per ogni a, b in $\mathcal{A}$ dominio a ideali principali, esiste $d = (a, b)$.

Esercizio 6.219. *Dimostrare che se $\mathcal{A}$ è un dominio a ideali principali e I è l'ideale generato da due elementi a, b di $\mathcal{A}$, allora $I = (d)$ con d massimo comun divisore tra a e b.*

Svolgimento. Sappiamo che ogni ideale di $\mathcal{A}$ è principale (Proposizione 6.217), quindi esiste $d \in \mathcal{A}$, tale che $I = (d)$. Vogliamo mostrare che d è un massimo comun divisore tra (a, b).

Sappiamo che $a, b \in (d)$, quindi esistono $x, y \in \mathcal{A}$ tali che: $a = dx$ e $b = dy$, cioè d divide sia a che b. D'altra parte d è un elemento di I, ideale generato da a e b, dunque esistono $s, t \in \mathcal{A}$ tali che $d = as + bt$. Un qualsiasi divisore comune $x \in \mathcal{A}$ di a e di b, divide anche as e bt, dunque divide $as + bt = d$.

Osservazione 6.220. Anche nei domini a ideali principali si può osservare che, dati due elementi a, b, se d e d' sono due massimi comun divisori, allora esiste c invertibile tale che $d = cd'$. Dunque si può parlare "del" massimo comun divisore a meno di invertibili.

La differenza con gli anelli euclidei è che nei domini ad ideali principali non abbiamo l'algoritmo di Euclide per calcolare il massimo comun divisore. Infatti tale algoritmo basa la sua finitezza sul fatto che sia definita una funzione grado a valori in $\mathbb{N}$.

Mostriamo adesso come, anche per i domini ad ideali principali, se un elemento è irriducibile allora è primo, ovvero (Proposizione 6.211) un elemento in un PID è primo se e solo se è irriducibile.

Proposizione 6.221. *Sia $\mathcal{A}$ un dominio ad ideali principali: x è irriducibile se e solo se (x) è massimale.*

Dimostrazione. $\Rightarrow$) Supponiamo $(x) \subseteq (y) \subseteq \mathcal{A}$, allora $x \in (y)$, cioè esiste $z \in \mathcal{A}$ tale che $x = yz$. Essendo x irriducibile, si possono verificare due casi:

(1) y è invertibile, allora $(y) = \mathcal{A}$.
(2) z è invertibile, allora $y = xz^{-1}$, cioè $y \in (x)$, ovvero $(y) = (x)$.

$\Leftarrow$) Supponiamo $x = yz$, allora $(x) \subseteq (y)$. Anche qui abbiamo due casi:

(1) $(y) = \mathcal{A}$, allora y è invertibile.
(2) $(y) = (x)$, allora $y = xu$ e dunque $x = xuz$. Per la regola di cancellazione questo implica che $1 = uz$, ovvero z è invertibile.

□

Corollario 6.222. *Se $\mathcal{A}$ è un dominio a ideali principali allora x è primo se e solo se x è irriducibile.*

Dimostrazione. Sia $x \in \mathcal{A}$ irriducibile, dalla Proposizione 6.221 sappiamo che (x) è massimale in $\mathcal{A}$. Dall'Osservazione 6.168 (x) è primo. La tesi segue dall'Osservazione 6.212. □

Osservazione 6.223. Per ciò che abbiamo visto, in particolare per l'identificazione elemento primo ed elemento irriducibile, si potrebbe essere portati a pensare che nei domini a ideali principali, ideali primi e ideali massimali siano *la stessa cosa*. In realtà è quasi così, resta fuori il caso dell'ideale $I = \{0\}$, che è sempre primo, ma è massimale se e solo se il dominio è un campo (Proposizione 6.149).

Per chiudere lo studio dei PID, vogliamo mostrare che anche in queste strutture vale il teorema di fattorizzazione unica già visto nel caso di $\mathbb{Z}$ e $\mathbb{K}[x]$.

Proposizione 6.224. *Ogni catena ascendente di ideali di un dominio ad ideali principali $\mathcal{A}$ si stabilizza. Cioè se $(x_1) \subseteq (x_2) \subseteq \ldots \subseteq (x_n) \subseteq (x_{n+1}) \subseteq \ldots$ è una catena ascendente di ideali di $\mathcal{A}$, allora $\exists k \in \mathbb{N}$ tale che $\forall n \geq k$, $(x_n) = (x_k)$.*

Dimostrazione. Consideriamo $I = \bigcup_{n \in \mathbb{N} \setminus \{0\}} (x_n)$. Dalla dimostrazione della Proposizione 6.172 sappiamo che I è un ideale di $\mathcal{A}$, perciò esiste $a \in \mathcal{A}$ tale che $I = (a)$. In particolare $a \in I$, dunque esiste $k \in \mathbb{N}$ tale che $a \in (x_k)$. Allora:

$$I = (a) \subseteq (x_k) \subseteq I \Rightarrow \ \forall n \geq k : \ I = (a) \subseteq (x_k) \subseteq (x_n) \subseteq I$$

□

Teorema 6.225. *Sia $\mathcal{A}$ un dominio ad ideali principali. Ogni elemento $x \in \mathcal{A}$ diverso da zero si scrive in modo unico (a meno dell'ordine e di moltiplicazione per elementi invertibili) come prodotto di elementi irriducibili (o primi che abbiamo visto essere la stessa cosa).*

Dimostrazione. **Esistenza.** Consideriamo $x \in \mathcal{A}$, se x è irriducibile abbiamo finito è già fattorizzato in irriducibili. Se x non è irriducibile allora $x = ab$ con a, b non invertibili. Se a, b sono irriducibili allora abbiamo trovato la fattorizzazione cercata, altrimenti $a = a_1 a_2$ (analogamente se b non è irriducibile). Quindi (a) è contenuto strettamente in (a_1) e in (a_2). Continuando in questo modo troviamo una catena ascendente di ideali, che per la Proposizione 6.224, si stabilizza.

Unicità. Sia $x = \prod_{i=1}^{k} p_i = \prod_{j=1}^{h} q_j$, allora p_1 divide $\prod_{j=1}^{h} q_j$ e dunque esiste $s \in \mathbb{N}_h$ tale che p_1 divide q_s (perché, dal corollario 6.222 sappiamo che p_1 irriducibile è primo). Dunque esiste un t_s invertibile (perché anche q_s è irriducibile) in $\mathcal{A}$ tale

che $p_1 t_s = q_s$. Usando la legge di cancellazione si ha

$$\prod_{i=2}^{k} p_i = t_s \prod_{j \in N_h, j \neq s} q_j$$

Per induzione si elidono ad uno ad uno i fattori irriducibili, e troviamo dunque che $h = k$ e l'unica differenza, a parte l'ordine dei fattori, è un prodotto di elementi invertibili. □

Osservazione 6.226. È interessante confrontare la dimostrazione del Teorema 6.225 con quella del teorema fondamentale dell'aritmetica (ovvero l'analogo nel caso specifico di $\mathbb{Z}$). Emerge come le dimostrazioni siano strutturalmente identiche: in entrambi i casi l'esistenza della fattorizzazione dipende dal fatto che ogni catena ascendente di ideali si stabilizza, l'unicità della fattorizzazione dal fatto che ogni elemento irriducibile è anche primo.

Osservazione 6.227. L'unicità della fattorizzazione, come ricordato nell'enunciato del Teorema 6.225 è a meno dell'ordine dei fattori e della moltiplicazione per elementi invertibili. Consideriamo il dominio a ideali principali $\mathbb{Z}$. Il numero 6 è uguale a $2 \cdot 3$, ma anche a $3 \cdot 2$ e anche a $(-3) \cdot (-2)$. Analogamente nel caso di $\mathbb{K}[x]$, il polinomio $(x^2 - 1)$ può essere visto come $(x + 1)(x - 1)$ ma anche come $k(x + 1)\frac{1}{k}(x - 1)$ per ogni k invertibile in $\mathbb{K}[x]$.

8.3. Anelli a fattorizzazione unica.

Definizione 6.228. Un dominio di integrità $\mathcal{A}$ si dice un **dominio a fattorizzazione unica** se ogni elemento di $\mathcal{A}$ diverso da zero e non invertibile, si scrive in modo unico (a meno dell'ordine e della moltiplicazione per elementi invertibili) come prodotto di elementi irriducibili.

Abbiamo già dimostrato che $EU \subset PID \subset UFD$, e solo accennato che il contenimento tra EU e PID è stretto. Il seguente esercizio mostra che anche il contenimento tra PID e UFD è stretto.

Esercizio 6.229. *Dimostrare che $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica, ma non un dominio ad ideali principali (suggerimento per la seconda parte: considerare un ideale di $\mathbb{Z}[x]$ che contenga la x e una costante diversa da 1).*

Abbiamo sottolineato nell'Osservazione 6.226, come per dimostrare che un dominio a ideali principali è a fattorizzazione unica abbiamo utilizzato le seguenti due proprietà (valide per ogni dominio a ideali principali):

(1) **Proprietà 1:** Ogni catena ascendente di ideali (principali) si stabilizza.
(2) **Proprietà 2:** Ogni elemento irriducibile è primo.

Definizione 6.230. Un anello $\mathcal{A}$ che soddisfa la proprietà 1 (detta anche condizione della catena ascendente) si dice **noetheriano**.

Osservazione 6.231. L'anello $P = \mathcal{A}[x_1 \dots x_n \dots]$ dei polinomi su infinite variabili a coefficienti in un dominio di integrità non è noetheriano, infatti, considerando gli ideali $I_i = (x_1 \dots x_i)$ al variare di i in $\mathbb{N}^+$, si ha che per ogni $i > j$ in N^+: I_i contiene strettamente I_j. Dunque gli I_i sono una catena ascendente infinita che non si stabilizza in P.

D'altra parte, essendo $\mathcal{A}$ un dominio d'integrità, generalizzando la dimostrazione vista nel Teorema 6.50 si ha che P è un dominio. Possiamo dunque costruire il campo delle frazioni di P (Esercizio 6.198), che è banalmente noetheriano in quanto campo (ha solo due ideali: $\{0\}$ e se stesso). Questa osservazione prova che la noetherianità non si conserva in generale sui sottoanelli (P infatti è un sottoanello del suo campo delle frazioni).

Mostriamo adesso che se l'anello è a fattorizzazione unica allora valgono le proprietà 1 e 2, dunque che tali proprietà potrebbero essere usate per dare una definizione alternativa, ma equivalente, di anelli a fattorizzazione unica.

Proposizione 6.232. *Se $\mathcal{A}$ è a fattorizzazione unica allora soddisfa le proprietà 1 e 2.*

Dimostrazione. Dimostriamo separatamente che valgono le due condizioni:

(1) Consideriamo una catena ascendente di ideali principali[12] di A:

$$(x_1) \subseteq (x_2) \subseteq ... \subseteq (x_n) \subseteq ...$$

Porre $(x_1) \subseteq (x_2)$ equivale ad affermare che $x_1 \in (x_2)$, cioè che $x_2|x_1$, ovvero esiste $y \in A$ tale che: $x_1 = yx_2$. Fattorizziamo x_1 e yx_2, il numero m_1 di fattori di x_1 è maggiore o uguale al numero m_2 di fattori di x_2, in quanto ci sono anche i fattori di y. Otteniamo così una catena decrescente di numeri naturali:

$$m_1 \geq m_2 \geq \ldots \geq m_n \geq \ldots$$

che si deve stabilizzare, cioè esiste $k \in \mathbb{N}$ tale che $m_n = m_k$ per ogni $n \geq k$. Quindi per ogni $n \geq k$ si ha: $x_k = yx_n$ con y che non ha fattori primi ed è quindi invertibile, perciò $(x_n) = (x_k)$.

(2) Sia $x \in A$ irriducibile, dobbiamo mostrare che x è primo. Supponiamo che $x|ab$ allora esiste $y \in A$ tale che $ab = xy$. Scriviamo la fattorizzazione in fattori irriducibili di a, b e y:

$$ab = \underbrace{a_1 \cdot \ldots \cdot a_k}_{a} \cdot \underbrace{b_1 \cdot \ldots \cdot b_h}_{b} = x \cdot \underbrace{y_1 \cdot \ldots \cdot y_l}_{y}$$

x è irriducibile quindi è uguale ad un a_i o un b_j a meno di un fattore invertibile. Se $x = a_i$ allora $x|a$, altrimenti se $x = b_j$ allora $x|b$.

□

Esercizio 6.233. *Mostrare che $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b | a, b \in \mathbb{Z}\}$, con le operazioni indotte da $\mathbb{C}$ (che lo contiene), non è a fattorizzazione unica.*

Svolgimento. Osserviamo innanzitutto che l'anello in questione è molto simile agli interi di Gauss, che però abbiamo visto essere un anello euclideo, e dunque sicuramente a fattorizzazione unica.

Possiamo mostrare che di un numero esistono due fattorizzazioni in irriducibili, ad esempio $6 = 2 \cdot 3$ ma è anche uguale a $(1 + \sqrt{-5})(1 - \sqrt{-5})$. Questo però non basta: dovremmo mostrare che ogni fattore è irriducibile. Scegliamo dunque un'altra via: quella di mostrare che una proprietà strutturale degli UFD, ovvero che

[12] Attenzione: in F.U. non è detto che ogni ideale sia principale, se così fosse F.U. e I.P. coinciderebbero.

ogni elemento irriducibile è primo, non vale in $\mathbb{Z}[\sqrt{-5}]$, in quanto 2 è irriducibile ma non primo.

Supponiamo che 2 sia fattorizzabile $2 = (a + \sqrt{-5}b)(c + \sqrt{-5}d)$. Passando alle norme:

$$4 = (a^2 + 5b^2)(c^2 + 5d^2) \Rightarrow \begin{cases} a^2 + 5b^2 \leq 4 \\ c^2 + 5d^2 \leq 4 \end{cases} \Rightarrow \begin{cases} b = 0 \\ d = 0 \end{cases}$$

Quindi (ricordiamoci che a, b, c, d sono interi):

$$4 = a^2 \cdot c^2 \Rightarrow \begin{cases} \text{o } a^2 = 1 \text{ e } c^2 = 4 \\ \text{o } a^2 = 4 \text{ e } c^2 = 1 \end{cases}$$

Questo dimostra che 2 è irriducibile in $\mathbb{Z}[\sqrt{-5}]$.
Sappiamo che $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \in (2)$, ma si dimostra che $(1 + \sqrt{-5}) \notin (2)$ e $(1 - \sqrt{-5}) \notin (2)$. Infatti risolvendo l'equazione:

$$(1 + \sqrt{-5}) = 2(a + \sqrt{-5}b)$$

si trova come unica soluzione:

$$a = \frac{1}{2} \text{ e } b = \frac{\sqrt{-5}}{2}$$

che non sono interi e quindi non appartengono a $\mathbb{Z}[\sqrt{-5}]$. Analogamente si verifica che $(1 - \sqrt{-5}) \notin (2)$.

Se $\mathcal{A}$ è un dominio a fattorizzazione unica, consideriamo l'anello $\mathcal{A}[x]$ dei polinomi a coefficienti in $\mathcal{A}$. Si dimostra, similmente a quanto visto nel caso di $\mathbb{Z}[x]$ (e dunque riportiamo solo gli enunciati senza dimostrazione), alcuni importanti risultati.

Teorema 6.234. *Sia $\mathcal{A}$ un dominio a fattorizzazione unica allora anche l'anello $\mathcal{A}[x]$, e più in generale $\mathcal{A}[x_1, \ldots, x_n]$, sono anelli a fattorizzazione unica.*

Osservazione 6.235. Non è vero invece che se $\mathcal{A}$ è euclideo (e quindi a maggior ragione se $\mathcal{A}$ è a ideali principali) $\mathcal{A}[x]$ sia ad ideali principali. Costruiamo un esempio: consideriamo $\mathcal{A} = \mathbb{Q}[x]$ che sappiamo essere un anello euclideo. Facciamo vedere che $\mathbb{Q}[x][y] = \mathbb{Q}[x, y]$ non è a ideali principali. È facile provare che $(x, y) = \{xa(x, y) + yb(x, y) | a(x, y), b(x, y) \in \mathbb{Q}[x, y]\}$ è un ideale di $\mathbb{Q}[x, y]$. Supponiamo esista $h(x, y) \in \mathbb{Q}[x, y]$ tale che $(x, y) = (h(x, y))$, in particolare $x, y \in (x, y)$, quindi:

$$h(x, y)|x \text{ e } h(x, y)|y \rightarrow deg_y h(x, y) \leq deg_y x = 0 \text{ e } deg_x h(x, y) \leq deg_x y = 0$$

cioè $h(x, y)$ è una costante. Ma in questo caso h sarebbe invertibile (perchè un elemento del campo $\mathbb{Q}$) e quindi $(h) = \mathbb{Q}[x, y]$, mentre (x, y) è strettamente contenuto in $\mathbb{Q}[x, y]$, perchè le costanti non appartengono a (x, y).

Teorema 6.236. *Sia $\mathcal{A}$ un dominio a fattorizzazione unica e $f \in \mathcal{A}[x]$.*

1. *Se $deg(f) = 0$, $f \in \mathcal{A}$, allora f è irriducibile in $\mathcal{A}[x]$ se e solo se f è irriducibile in $\mathcal{A}$.*
2. *Se $deg(f) > 0$, f è irriducibile in $\mathcal{A}[x]$ se e solo se f è primitivo ed è irriducibile in $\mathbb{K}[x]$, dove $\mathbb{K}$ è il campo dei quozienti di $\mathcal{A}$.*

CAPITOLO 7

Campi

1. Elementi algebrici e trascendenti su $\mathbb{K}$

Nel capitolo sugli anelli abbiamo introdotto il concetto di campo, ovvero di anello in cui tutti gli elementi diversi da zero sono invertibili rispetto alla moltiplicazione. Abbiamo fatto alcuni esempi di campi e studiato la fattorizzazione di polinomi a coefficienti in un campo. In questo capitolo approfondiremo lo studio della risolubilità delle equazioni polinomiali, in particolare dato un polinomio $f(x)$ a coefficienti in un campo $\mathbb{K}$ cercheremo di capire se esiste sempre un campo $\mathbb{L}$, contenente $\mathbb{K}$, in cui $f(x)$ si fattorizza come prodotto di fattori di grado uno. Introduciamo dunque la nozione di estensione di campi.

Definizione 7.1. Siano $\mathbb{L}$ e $\mathbb{K}$ campi rispetto alle stesse operazioni. $\mathbb{L}$ si dice **un'estensione** di $\mathbb{K}$ se $\mathbb{K} \subset \mathbb{L}$. Per indicare che $\mathbb{L}$ è una estensione di $\mathbb{K}$ scriveremo anche $\mathbb{L}/\mathbb{K}$.

Definizione 7.2. Sia $\mathbb{L}$ un'estensione del campo $\mathbb{K}$. Un elemento $\alpha \in \mathbb{L}$ si dice **algebrico** su $\mathbb{K}$ se esiste un polinomio $f(x) \in \mathbb{K}[x]$, non identicamente nullo, tale che: $f(\alpha) = 0$. Un elemento $\alpha \in \mathbb{L}$ non algebrico su $\mathbb{K}$ si dice **trascendente** su $\mathbb{K}$.

Osservazione 7.3. Se α è algebrico su $\mathbb{K}$ allora è algebrico su qualsiasi campo $\mathbb{F}$ estensione di $\mathbb{K}$. Infatti il polinomio $g(x) \in \mathbb{K}[x]$ che si annulla in α è in particolare un polinomio a coefficienti in $\mathbb{F}[x]$ se $\mathbb{F}$ contiene $\mathbb{K}$.

Esercizio 7.4. *L'insieme dei polinomi in $\mathbb{K}[x]$ che si annullano in un elemento α di un'estensione di campo $\mathbb{L}$ di $\mathbb{K}$, è un ideale di $\mathbb{K}[x]$ (se α è trascendente è l'ideale $\{0\}$).*

Svolgimento. Sia I l'insieme dei polinomi di $\mathbb{K}[x]$ che si annullano in $\alpha \in \mathbb{L}$. Per ogni coppia $f(x)$, $g(x)$ di elementi di I, e per ogni $h(x) \in \mathbb{K}[x]$ si ha:

$$(f+g)(\alpha) \underbrace{=}_{def.somma\ in\ \mathbb{K}[x]} \underbrace{f(\alpha)}_{f(x)\in I} + \underbrace{g(\alpha)}_{g(x)\in I} = 0 + 0 = 0 \Rightarrow f(x) + g(x) \in I$$

$$h(\alpha)f(\alpha) = h(\alpha) \cdot 0 = 0 \Rightarrow h(x)f(x) \in I$$

Esempio 7.5. Consideriamo $\mathbb{Q} \subset \mathbb{C}$, e mostriamo alcuni esempi di elementi algebrici e trascendenti su $\mathbb{Q}$.

Osserviamo che, per verificare che un elemento α è algebrico su un campo $\mathbb{K}$, *basta* trovare un polinomio a coefficienti in $\mathbb{K}$ che si annulla in α. La dimostrazione che α è trascendente è spesso molto più laboriosa. Non presenteremo dunque dimostrazioni di trascendenza perché esulano dagli scopi di questo libro.

L'aspetto interessante è che esistono "molti" complessi che sono trascendenti su $\mathbb{Q}$, *molti di più* di quanti non siano gli algebrici. Un modo per dimostrare

questa affermazione è *contare* i polinomi di grado n in $\mathbb{Q}$ e sfruttare il fatto che un polinomio di grado n in $\mathbb{Q}$ ha al più n radici distinte in $\mathbb{C}$. I polinomi di grado n a coefficienti in $\mathbb{Q}$ hanno la cardinalità di $\mathbb{Q}^{n+1}$ (bisogna scegliere $n+1$ coefficienti, il primo diverso da 0), che iterando il processo diagonale di Cantor, si dimostra avere cardinalità numerabile. Ognuno di questi polinomi ha al più n radici, dunque la cardinalità delle radici dei polinomi di grado n in $\mathbb{Q}[x]$ è numerabile. L'unione di tutte le radici di polinomi a coefficienti in $\mathbb{Q}$ è quindi un unione numerabile di insiemi numerabili (le possibili radici al variare del grado n in $\mathbb{N}$): si dimostra che unione numerabile di numerabili è numerabile. Quindi i numeri complessi algebrici su $\mathbb{Q}$ sono numerabili, mentre $\mathbb{C}$ che contiene $\mathbb{R}$ ha cardinalità non numerabile. Dunque quello che rimane da $\mathbb{C}$ *togliendo* la quantità numerabile di algebrici è una quantità più che numerabile di elementi che sono proprio i trascendenti. Esempi famosi di non algebrici su $\mathbb{Q}$ sono π e e.

Vediamo però anche esempi di algebrici. Ogni razionale q è algebrico su $\mathbb{Q}$, infatti è radice del polinomio $x-q$ che è in $\mathbb{Q}[x]$. Più in generale ogni elemento k di $\mathbb{K}$ è algebrico su $\mathbb{K}$, in quanto radice del polinomio $x-k$ a coefficienti in $\mathbb{K}$.

Altri esempi di algebrici su $\mathbb{Q}$ sono le radici n-esime di elementi a di $\mathbb{Q}$, infatti esse solo radici del polinomio $f(x)=x^n-a$ a coefficienti in $\mathbb{Q}$.

Esercizio 7.6. *Dimostrare che $\alpha=\sqrt[3]{3}+\sqrt{5}$ è algebrico su $\mathbb{Q}$.*

Svolgimento. In seguito dimostreremo che gli algebrici di un'estensione di un campo $\mathbb{K}$ formano un campo estensione di $\mathbb{K}$ e dunque in particolare sono chiusi per somma, prodotto, opposto e inverso se diversi da zero. Questo risultato permetterebbe di dire che α è algebrico senza fare alcun tipo di calcolo, dall'Esempio 7.5 infatti, sappiamo che $\sqrt[3]{3}$ e $\sqrt{5}$ sono algebrici su $\mathbb{Q}$.

Con gli strumenti teorici a nostra disposizione in questo momento, dobbiamo cercare un polinomio a coefficienti in $\mathbb{Q}$ che si annulli in $\sqrt[3]{3}+\sqrt{5}$:

$$\alpha-\sqrt{5}=\sqrt[3]{3} \;\rightarrow\; (\alpha-\sqrt{5})^5=3 \;\leftrightarrow (\alpha-\sqrt{5})(\alpha^2-2\sqrt{5}\alpha+5)=3$$

quindi:

$$\alpha^3-3\sqrt{5}\alpha^2+15\alpha-5\sqrt{5}=3 \leftrightarrow \alpha^3+15\alpha-3=\sqrt{5}(3\alpha^2+5)$$

abbiamo isolato i termini sotto radice in modo da poter elevare al quadrato e ottenere un equazione che ha come insieme di soluzioni un insieme di soluzioni che contiene quello dell'equazione originaria.

$$\alpha^6+225\alpha^2+9+30\alpha^4-6\alpha^3-90\alpha=45\alpha^4+150\alpha^2+125$$

da cui:

$$\alpha^6-15\alpha^4-6\alpha^3+75\alpha^2-90\alpha-116=0.$$

Dunque il polinomio $f(x)=x^6-15x^4-6x^3+75x^2-90x-116\in\mathbb{Q}[x]$ si annulla in $\alpha=\sqrt[3]{3}+\sqrt{5}$.

Esercizio 7.7. *Sia α algebrico su $\mathbb{K}$, allora $\alpha+k$ e $k\cdot\alpha$ sono algebrici su $\mathbb{K}$ per ogni $k\in\mathbb{K}$, e, se α è diverso da zero, anche α^{-1} lo è.*

Svolgimento. α algebrico su $\mathbb{K}$ significa che esiste $g(x)\in\mathbb{K}[x]$ tale che $g(\alpha)=0$ allora è facile osservare che i polinomi $t(x)=g(x-k)$ e $r(x)=g\left(\frac{x}{k}\right)$ sono a coefficienti in $\mathbb{K}$ e si annullano rispettivamente in $\alpha+k$ e in $k\cdot\alpha$.

Per trattare il caso dell'inverso di α (se α è diverso da zero) consideriamo l'applicazione φ da $\mathbb{K}[x]$ a $\mathbb{K}[x]$ (già incontrata nell'Esercizio 6.113):

$$\varphi(g(x)) = g\left(\frac{1}{x}\right) \cdot x^{deg(g(x))}$$

che associa a $f(x)$ il suo polinomio reciproco. Se $g(x)$ si annulla in $\alpha \neq 0$, allora $g(x)$ non può essere del tipo $a \cdot x^n$ (che si annulla solo in 0), dunque $\varphi(g(x))$ è un polinomio di grado maggiore di 0 che si annulla in α^{-1}.

Sia $\mathbb{L}$ un'estensione del campo $\mathbb{K}$ e α un elemento di $\mathbb{L}$. Indichiamo[1] con $\mathbb{K}[\alpha]$ e $\mathbb{K}(\alpha)$ rispettivamente il minimo sottoanello e il minimo sottocampo di $\mathbb{L}$, contenenti $\mathbb{K}$ e α, ovvero:

$$\mathbb{K}[\alpha] = \{f(\alpha) | f(x) \in \mathbb{K}[x]\}$$

e

$$\mathbb{K}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} | f(x), g(x) \in \mathbb{K}[x], g(\alpha) \neq 0 \right\}$$

Osservazione 7.8. A seguito dell'Esercizio 7.7 si può supporre che, dato α algebrico su $\mathbb{K}$, tutti gli elementi di $\mathbb{K}(\alpha)$ siano algebrici su $\mathbb{K}$. Manca di dimostrare che le potenze di α ad esponente naturale sono algebriche su α. Proveremo questo fatto nel prossimo paragrafo senza dover esibire un polinomio che si annulla in α^n per ogni n naturale, ma utilizzando il legame tra estensioni $\mathbb{K}(\alpha)$ di un campo $\mathbb{K}$ (che chiameremo semplici) con α algebrico su $\mathbb{K}$ e dimensione finita di $\mathbb{K}(\alpha)$ come spazio vettoriale su $\mathbb{K}$.

Dato $\alpha \in \mathbb{L}$, usiamo la funzione valutazione φ_α, che ad ogni polinomio $f(x)$ in $\mathbb{K}[x]$ associa $f(\alpha)$ in $\mathbb{K}[\alpha]$, per stabilire quando α è algebrico o trascendente su $\mathbb{K}$.

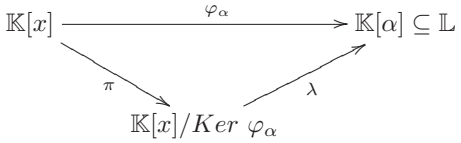
Esercizio 7.9. *Dimostrare che φ_α è un omomorfismo surgettivo di anelli.*

Teorema 7.10. *φ_α è un omomorfismo iniettivo se e solo se α è trascendente su $\mathbb{K}$.*

Dimostrazione. Se α è algebrico su $\mathbb{K}$, esiste un polinomio $f(x) \in \mathbb{K}[x]$ non nullo, tale che $f(\alpha) = 0$, ovvero $f(x) \in Ker\ \varphi_\alpha$ e dunque φ_α non è un omomorfismo iniettivo. Viceversa, se α è trascendente, il polinomio nullo di $\mathbb{K}[x]$ è l'unico che si annulla in α, dunque $Ker\ \varphi_\alpha = \{0\}$. □

Teorema 7.11. *Se α è algebrico su $\mathbb{K}$, allora $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$ (in particolare $\mathbb{K}[\alpha]$ è un campo). Se α è trascendente, allora $\mathbb{K}[\alpha] \cong \mathbb{K}[x]$*

Dimostrazione. Dal teorema di omomorfismo per anelli (Teorema 6.157) sappiamo che il seguente diagramma commuta e che λ è un isomorfismo, visto che (Esercizio 7.9) φ_α è surgettivo):



[1] In generale se T è un sottoinsieme di un campo $\mathbb{L}$ estensione di $\mathbb{K}$ indicheremo con $\mathbb{K}(T)$ e $\mathbb{K}[T]$ rispettivamente il minimo sottocampo e il minimo sottoanello di $\mathbb{L}$ contenente $\mathbb{K}$ e T.

Se φ_α è iniettivo allora è un isomorfismo, dunque $\mathbb{K}[\alpha] \cong \mathbb{K}[x]$.

Se φ_α non è iniettivo (ovvero α è algebrico su $\mathbb{K}$), cerchiamo di "leggere" informazioni su $\mathbb{K}[\alpha]$ tramite l'isomorfismo λ:

$$\mathbb{K}[\alpha] \overbrace{\cong}^{\lambda} \mathbb{K}[x]/Ker\ \varphi_\alpha$$

Sappiamo che $Ker\ \varphi_\alpha$ è un ideale in un anello euclideo, dunque è principale. Perciò esiste $h(x) \in \mathbb{K}[x]$ di grado maggiore[2] di 0 tale che $Ker\ \varphi_\alpha = (h(x))$.

Osserviamo che $\mathbb{K}[\alpha]$ è contenuto nel campo $\mathbb{L}$ dunque è un dominio di integrità (se ci fossero divisori di zero in $\mathbb{K}[\alpha]$ ci sarebbero anche in $\mathbb{L}$), quindi $\mathbb{K}[x]/(h(x))$ è un dominio di integrità. Questo implica che $(h(x))$ è un ideale primo non banale, cioè $h(x)$ è primo.

Sempre per le nostre conoscenze sui domini ad ideali principali, sappiamo che elemento primo equivale ad elemento irriducibile, e che l'ideale generato da un elemento irriducibile è massimale. Dunque $(h(x))$ è massimale in $\mathbb{K}[x]$ e di conseguenza $\mathbb{K}[x]/(h(x))$ è un campo. $\mathbb{K}[\alpha]$, che è isomorfo a $\mathbb{K}[x]/(h(x))$, è esso stesso un campo.

Per concludere osserviamo che in generale $\mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$, in questo caso $\mathbb{K}[\alpha]$ è un campo che contiene sia $\mathbb{K}$ che α, dunque contiene $\mathbb{K}(\alpha)$ (che è il minimo sottocampo di $\mathbb{L}$ con questa caratteristica). Dunque $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$. □

Esempio 7.12. Consideriamo $\alpha = \sqrt{2}$ che è algebrico su $\mathbb{Q}$. Il Teorema 7.11 ci dice che $\mathbb{Q}[\sqrt{2}]$ è un campo: ovvero ogni espressione del tipo $\sum_{i=0}^{n} c_i \sqrt{2}^i$, con $c_i \in \mathbb{Q}$, ha un inverso dello stesso tipo.

Definizione 7.13. Siano $\mathbb{K} \subseteq \mathbb{L}$ campi e $\alpha \in \mathbb{L}$ un elemento algebrico su $\mathbb{K}$. Si dice **polinomio minimo** di α su $\mathbb{K}$ un generatore monico (cioè con primo coefficiente uguale ad 1) dell'ideale $Ker\ \varphi_\alpha$.

Osservazione 7.14. Ricordiamo che, dalla dimostrazione del Teorema 7.11, il polinomio minimo è irriducibile.

Proposizione 7.15. *Siano $\mathbb{K} \subseteq \mathbb{L}$ campi, e $\alpha \in \mathbb{L}$ un elemento algebrico su $\mathbb{K}$. Il polinomio minimo di α su $\mathbb{K}$ è unico, ed in particolare è il polinomio monico di $(Ker\ \varphi_\alpha)$ di grado minimo.*

Dimostrazione. Siano $h(x)$ e $g(x)$ due generatori di $(Ker\ \varphi_\alpha)$. Questo implica che $h(x)$ e $g(x)$ sono reciprocamente uno multiplo dell'altro, ovvero che hanno lo stesso grado n. In particolare tutti gli altri elementi di $(Ker\ \varphi_\alpha)$ hanno grado maggiore o uguale dei generatori. Se $h(x)$ e $g(x)$ fossero diversi ed entrambi monici, avremmo che $h(x) - g(x)$ è un polinomio diverso dal polinomio nullo, di grado strettamente minore di n, che si annulla in α e questo è impossibile perché non potrebbe appartenere (per le questioni di grado di cui sopra) all'ideale $(h(x))$ (o quel che è uguale a $(g(x))$). □

Indicheremo **il** polinomio minimo di α su $\mathbb{K}$ con $\mu_\alpha(x)$, senza far riferimento al campo $\mathbb{K}$ laddove non ci sia ambiguità. L'unicità appena mostrata, ci dice che se troviamo un polinomio monico $h(x) \in \mathbb{K}[x]$ irriducibile in $\mathbb{K}[x]$ con $h(\alpha) = 0$, allora $h(x) = \mu_\alpha(x)$.

[2] $h(x)$ non può essere una costante diversa da zero perché un tale polinomio non ha radici, e non può essere zero perché in tal caso φ_α sarebbe iniettivo.

Osservazione 7.16. Il polinomio minimo di un elemento algebrico su un campo è cosa diversa dal polinomio minimo definito in algebra lineare. In quel caso si dice polinomio minimo di un endomorfismo T di uno spazio vettoriale V il polinomio monico $f(x)$ a coefficienti in V di grado minimo tale che l'applicazione $f(T)$ è l'applicazione nulla su V.

Vediamo, attraverso un esempio, questa differenza. Consideriamo l'endomorfismo T di $\mathbb{R}^2$ che agisce sulla base canonica $e_1 = (1,0),\ e_2 = (0,1)$ di $\mathbb{R}^2$ come segue:

$$T(e_1) = 0 \quad T(e_2) = e_1$$

È facile osservare che T^2 è l'applicazione nulla, infatti:

$$e_1 \xrightarrow{T} 0 \xrightarrow{T} 0$$
$$e_2 \xrightarrow{T} e_1 \xrightarrow{T} 0$$

Il polinomio minimo dell'endomorfismo T di $\mathbb{R}^2$ è dunque x^2 (infatti è divisibile solo per x e le costanti: tutti polinomi che non si "annullano" in T). Ma x^2 non è irriducibile! Osserviamo che, a differenza di quel che accade nel nostro caso, l'anello degli endomorfismi su $\mathbb{R}^2$ (e in generale su un campo $\mathbb{K}$) non è un dominio di integrità.

Esercizio 7.17. *Sia α una radice complessa del polinomio $x^3 - 2x - 2$. Determinare*

(1) *un polinomio $f(x) \in \mathbb{Q}[x]$ tale che $\alpha \cdot f(\alpha) = 1$,*
(2) *il polinomio minimo di $\alpha^2 + 1$ su $\mathbb{Q}$.*

Svolgimento. Affrontiamo separatamente i due punti:

(1) Essendo α una radice del polinomio $x^3 - 2x - 2$, si ha che:

$$\alpha^3 - 2\alpha - 2 = 0$$

Quindi $\alpha \cdot (\alpha^2 - 2) = 2$, da cui:

$$\alpha \cdot (\frac{\alpha^2}{2} - 1) = 1$$

Ovvero il polinomio

$$f(x) = \frac{1}{2} \cdot x^2 - 1$$

è tale che $\alpha \cdot f(\alpha) = 1$.

(2) Il polinomio $x^3 - 2x - 2$ è irriducibile su $\mathbb{Q}[x]$ (per esempio si può usare Eisenstein), dunque $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Osserviamo che $\alpha^2 + 1 \in \mathbb{Q}(\alpha)$ in quanto si ottiene come:

$$\underbrace{\alpha}_{\in\mathbb{Q}(\alpha)} \cdot \underbrace{\alpha}_{\in\mathbb{Q}(\alpha)} + \underbrace{1}_{\in\mathbb{Q}(\alpha)}$$

Dunque $\mathbb{Q}(\alpha^2 + 1) \subseteq \mathbb{Q}(\alpha)$. Quindi il grado di $\mathbb{Q}(\alpha^2 + 1)$ su $\mathbb{Q}$ può essere uguale ad 1 (questo vorrebbe dire che $\mathbb{Q}(\alpha^2 + 1)$ e $\mathbb{Q}$ sono uguali, ovvero che $\alpha^2 + 1 \in \mathbb{Q}$) o a 3. Si verifica facilmente che $\alpha^2 + 1$ non può essere un elemento q di $\mathbb{Q}$ altrimenti $x^2 + 1 - q$ sarebbe un polinomio di $\mathbb{Q}[x]$ che si annulla in α di grado minore di 3. Perciò

$$[\mathbb{Q}(\alpha^2 + 1) : \mathbb{Q}] = 3$$

Ovvero il polinomio minimo di α^2+1 su $\mathbb{Q}$ ha grado 3 e $\mathbb{Q}(\alpha^2+1)=\mathbb{Q}(\alpha)$. Calcoliamoci dunque le potenze di α^2+1:

$$(\alpha^2+1)^0=1$$
$$(\alpha^2+1)^1=\alpha^2+1$$
$$(\alpha^2+1)^2=\alpha^4+2\alpha^2+1 \underbrace{=}_{\alpha^3=2\alpha+2} \alpha\cdot(2\alpha+2)+2\alpha^2+1=4\alpha^2+2\alpha+1$$
$$(\alpha^2+1)^3=\alpha^6+3\alpha^4+3\alpha^2+1=\alpha^3(\alpha^3+3\alpha)+3\alpha^2+1 \underbrace{=}_{\alpha^3=2\alpha+2} 13\alpha^2+14\alpha+5$$

Noi sappiamo che questi quattro elementi sono linearmente dipendenti su $\mathbb{Q}$ (perché, come detto, la dimensione di $\mathbb{Q}(\alpha^2+1)$ su $\mathbb{Q}$ come spazio vettoriale è 3 e questi sono 4 elementi) dunque andiamo a risolvere il sistema a coefficienti interi a,b,c:

$$\underbrace{13\alpha^2+14\alpha+5}_{(\alpha^2+1)^3}+a\cdot(\underbrace{4\alpha^2+2\alpha+1}_{(\alpha^2+1)^2})+b\cdot(\alpha^2+1)+c\cdot 1=0$$

Sappiamo anche che 1, α e α^2 sono indipendenti su $\mathbb{Q}$ (in quanto $\mathbb{Q}(\alpha)$ è generato da α e di grado 3 su $\mathbb{Q}$) e perciò il sistema corrisponde a:

$$\begin{cases} 13+4a+b=0 \\ 14+2a=0 \\ 5+a+b+c=0 \end{cases}$$

Il sistema ha soluzione: $a=-7$, $b=15$ e $c=-13$, dunque il polinomio $x^3-7x^2+15x-13$, che si annulla in α^2+1 per costruzione ed è monico e di grado 3, è il polinomio minimo cercato.

Esercizio 7.18. *Determinare il polinomio minimo di* $\sqrt{2\sqrt{2}-3}$ *su* $\mathbb{Q}$ *e su* $\mathbb{Q}(i)$.

Svolgimento. $\alpha=\sqrt{2\sqrt{2}-3}$ elevando al quadrato questa uguaglianza si ottiene:

$$\alpha^2=2\sqrt{2}-3 \leftrightarrow \alpha^2+3=2\sqrt{2}$$

e quindi elevando nuovamente al quadrato:

$$\alpha^4+6\alpha^2+9=8 \leftrightarrow \alpha^4+6\alpha^2+1=0.$$

Ovvero α è radice del polinomio:

$$f(x)=x^4+6x^2+1$$

e se indichiamo con $\mu(x)$ e $\lambda(x)$ rispettivamente il polinomio minimo di α su $\mathbb{Q}$ e su $\mathbb{Q}(i)$, questo implica che $\mu(x)|f(x)$ e $\lambda(x)|f(x)$. Inoltre $\mu(x)$ appartiene all'ideale $(\lambda(x))$ quindi in $\mathbb{Q}(i)$ si ha: $\lambda(x)|\mu(x)$.
Osserviamo che:

$$2\sqrt{2}-3=-(3-2\sqrt{2})=-(1-2\sqrt{2}+2)=-(1-\sqrt{2})^2$$

quindi:

$$\alpha=\sqrt{2\sqrt{2}-3}=\sqrt{-(1-\sqrt{2})^2}.$$

Consideriamo $\alpha=i(1-\sqrt{2})$, una delle due radici quadrate complesse di $-(1-\sqrt{2})^2$, allora:

$$\alpha-i=-\sqrt{2}i \to \alpha^2-2i\alpha-1=2 \to \alpha^2-2i\alpha+1=0$$

Quindi:

$$t(x) = x^2 - 2ix + 1$$

è un multiplo di $\lambda(x)$ in $\mathbb{Q}(i)$. Ma $t(x)$ è irriducibile in $\mathbb{Q}(i)$ in quanto $\alpha \notin \mathbb{Q}(i)$ infatti affinchè α appartenga a $\mathbb{Q}(i)$ è necessario e sufficiente che $\sqrt{2} \in \mathbb{Q}(i)$. Ovvero dovrebbero esistere $a, b \in \mathbb{Q}$ tali che:

$$\sqrt{2} = a + ib \to 2 = a^2 - b^2 + 2iab \to \underbrace{2 - a^2 + b^2}_{\in \mathbb{Q}} = 2iab$$

da questo segue che $a = 0$ oppure $b = 0$, ma questo implicherebbe rispettivamente: $ib = \sqrt{2}$ e $a = \sqrt{2}$, questa seconda non è risolvibile in $\mathbb{Q}$, mentre la prima implica che $-b^2 = 2$ e anch'essa non è risolvibile in $\mathbb{Q}$.
L'irriducibilità di $t(x)$ in $\mathbb{Q}(i)$ implica che $t(x)$ è il polinomio minimo di α su $\mathbb{Q}(i)$, cioè $t(x) = \lambda(x)$.
Per quanto riguarda $\mu(x)$ sappiamo che è diviso da un polinomio, $\lambda(x)$, di grado 2 e che divide un polinomio, $f(x)$, di grado 4. Inoltre non può avere grado 3, perché $\mathbb{Q}(\alpha)$ ha come sottoestensione $\mathbb{Q}(\sqrt{2})$ di grado 2, quindi:

$$deg(\mu(x)) = \begin{cases} 2 \Rightarrow \mu(x) = \lambda(x) \\ 4 \Rightarrow \mu(x) = f(x) \end{cases}$$

Ma $\mu(x)$ non può essere uguale a $\lambda(x)$ che non è a coefficienti in $\mathbb{Q}$, quindi $\mu(x) = f(x)$.

2. Grado di una estensione ed estensioni algebriche

Se $(\mathbb{L}, +, \cdot)$ è un'estensione di $(\mathbb{K}, +, \cdot)$, si può definire su $\mathbb{L}$ un prodotto scalare $*$ da $\mathbb{K} \times \mathbb{L}$ in $\mathbb{L}$ che rende $\mathbb{L}$ uno spazio vettoriale su $\mathbb{K}$ (provare per esercizio):

$$\forall k \in \mathbb{K},\ \forall \in \mathbb{L} \quad k * l \overset{def.}{=} k \cdot l$$

Ovvero il prodotto scalare $*$ è, in maniera naturale, il prodotto $\cdot$ in $\mathbb{L} \times \mathbb{L}$ ristretto a $\mathbb{K} \times \mathbb{L}$.

Definizione 7.19. La dimensione dello spazio vettoriale $\mathbb{L}$ su $\mathbb{K}$, si indica con la notazione $[\mathbb{L} : \mathbb{K}]$, ed è detta **grado** dell'estensione $\mathbb{L}$ su $\mathbb{K}$.

Definizione 7.20. $\mathbb{L}$ estensione di $\mathbb{K}$ si dice **finita** se è uno spazio vettoriale di dimensione finita su $\mathbb{K}$, altrimenti si dice **infinita**.

Nel paragrafo precedente, dati $\mathbb{K}$ campo e $\alpha \in \mathbb{L}$ con $\mathbb{L}$ estensione di campo, abbiamo considerato il campo $\mathbb{K}(\alpha)$ (minimo sottocampo di $\mathbb{L}$ contenente $\mathbb{K}$ e α.

Definizione 7.21. Un'estensione $\mathbb{L}$ di un campo $\mathbb{K}$ è detta **semplice** se esiste un elemento α di $\mathbb{L}$ tale che $\mathbb{L} = \mathbb{K}(\alpha)$.

Esempio 7.22. Consideriamo il campo $\mathbb{C}$ dei numeri complessi come estensione del campo $\mathbb{R}$ dei numeri reali. $\mathbb{C}$ è $\mathbb{R}(i)$, il minimo sottocampo contenente tutti i numeri reali e l'unità immaginaria i (l'elemento tale che $i^2 = -1$). Quindi $\mathbb{C}$ è un'estensione semplice di $\mathbb{R}$.

Il prossimo teorema caratterizza le proprietà principali delle estensioni semplici.

Teorema 7.23. *Sia $\mathbb{L}$ un'estensione di $\mathbb{K}$ e $\alpha \in \mathbb{L}$. $\mathbb{K}(\alpha)$ è un'estensione finita di $\mathbb{K}$ se e solo se α è algebrico. In tal caso $[\mathbb{K}(\alpha) : \mathbb{K}] = deg(\mu_\alpha(x))$.*

DIMOSTRAZIONE. Supponiamo α trascendente e $[\mathbb{K}(\alpha) : \mathbb{K}] = n < \infty$. Gli $n+1$ elementi $1, \alpha, \alpha^2, \ldots, \alpha^n$ di $\mathbb{K}[\alpha]$ devono essere linearmente dipendenti (la cardinalità massima di un insieme di elementi linearmente indipendenti su $\mathbb{K}$ in $\mathbb{K}(\alpha)$ è n) quindi esistono $n+1$ elementi $c_i \in \mathbb{K}$ non tutti nulli tali che:

$$\sum_{i=0}^{n+1} c_i \cdot \alpha^i = 0$$

Ovvero α è radice del polinomio $\sum_{i=0}^{n+1} c_i \cdot x^i = 0$ di $\mathbb{K}[x]$: assurdo perché avevamo supposto α trascendente.

Viceversa sia α algebrico su $\mathbb{K}$ con polinomio minimo $\mu_\alpha(x)$ di grado n. Dato $f(x) \in \mathbb{K}[x]$ effettuiamo la divisione euclidea per $\mu_\alpha(x)$:

$$f(x) = q(x)\mu_\alpha(x) + r(x) \quad r(x) = 0 \text{ oppure } 0 \leq deg(r(x)) < n$$

Passando alla valutazione in α si ha:

$$f(\alpha) = q(\alpha)\mu_\alpha(\alpha) + r(\alpha)$$

Ma essendo per ipotesi $\mu_\alpha(\alpha) = 0$ questo equivale a $f(\alpha) = r(\alpha)$, ovvero ogni elemento di $\mathbb{K}[\alpha]$ si può descrivere nella seguente forma:

$$r(\alpha) = \sum_{i=0}^{n-1} c_i \alpha^i$$

Questo ci dice che le potenze, da 0 a $n-1$, di α generano $\mathbb{K}[\alpha]$. Per concludere rimane da mostrare che tali potenze sono linearmente indipendenti su $\mathbb{K}$, consideriamone dunque una combinazione lineare su $\mathbb{K}$ nulla:

$$\sum_{i=0}^{n-1} c_i \alpha^i = 0 \;\; c_i \in \mathbb{K}$$

Da questo segue che il polinomio $g(x) = \sum_{i=0}^{n-1} c_i x^i$ si annulla in α, ovvero $g(x) \in Ker\ \varphi_\alpha = (\mu_\alpha(x))$, quindi esiste $l(x)$ tale che:

$$g(x) = l(x)\mu_\alpha(x) \tag{2.1}$$

Ora a primo membro c'è un polinomio di grado minore di n a secondo membro cè un polinomio di grado $n + deg(l(x))$. Dunque tale uguaglianza può sussistere se e solo se $l(x)$, e di conseguenza $g(x)$, sono uguali al polinomio nullo. □

Osservazione 7.24. Dalla dimostrazione del Teorema 7.23 segue che una base di $\mathbb{K}(\alpha)$ su $\mathbb{K}$ è data dall'insieme:

$$\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

Esempio 7.25. Considerando $\mathbb{Q}(\sqrt[3]{3})$ abbiamo che il polinomio minimo di $\sqrt[3]{3}$ su $\mathbb{Q}$ è $x^3 - 3$ di grado 3. Perciò:

$$\mathbb{Q}(\sqrt[3]{3}) \cong \mathbb{Q}[x]/(x^3 - 3)$$

Gli elementi di $\mathbb{Q}[x]/(x^3 - 3)$ sono i polinomi a coefficienti in $\mathbb{Q}$ di grado minore o uguale a 2 (i polinomi resto della divisione per $x^3 - 3$). Gli elementi del campo isomorfo $\mathbb{Q}(\sqrt[3]{3})$ sono del tipo $a + b\sqrt[3]{3} + c(\sqrt[3]{3})^2$ al variare di a, b, c in $\mathbb{Q}$, infatti una base su $\mathbb{Q}$ di $\mathbb{Q}(\sqrt[3]{3})$ è data da $\{1, \sqrt[3]{3}, (\sqrt[3]{3})^2\}$.

Esercizio 7.26. *Se $\alpha \in \mathbb{L}$ diverso da 0 è algebrico su $\mathbb{K}$, allora $\mu_{\alpha^{-1}}(x) = b^{-1}\mu_\alpha(x)$, dove b è il termine noto di $\mu_\alpha(x)$.*

Svolgimento. Abbiamo già dimostrato che se α è algebrico, allora α^{-1} è algebrico.

È facile osservare che $\mathbb{K}(\alpha) = \mathbb{K}(\alpha^{-1})$, infatti α^{-1} appartiene ad ogni campo contenente $\mathbb{K}$ e α e dunque $\mathbb{K}(\alpha) \supset \mathbb{K}(\alpha^{-1})$, analogamente α appartiene ad ogni campo contenente $\mathbb{K}$ e α^{-1} (in quanto α è l'inverso di α^{-1} e un campo è chiuso per inversi di elementi diversi da zero) e dunque $\mathbb{K}(\alpha) \subset \mathbb{K}(\alpha^{-1})$. Dunque i polinomi minimi di α e α^{-1} hanno lo stesso grado.

L'applicazione φ che associa a $f(x)$ il suo polinomio reciproco praticamente effettua una permutazione sui coefficienti del polinomio $f(x)$ restituendo il polinomio che ha come coefficiente i-esimo a_{n-i}. Ora è facile osservare che φ non è un omomorfismo, infatti φ manda i polinomi composti da un solo monomio in una costante e dunque non può rispettare la struttura additiva, per esempio:

$$\varphi(x^2 + x + 1) = x^2 + x + 1 \neq \varphi(x^2) + \varphi(x) + \varphi(1) = 1 + 1 + 1 = 3$$

ma si *comporta bene* per il prodotto ovvero per ogni $f(x)$, $g(x)$ in $\mathbb{K}[x]$ si ha che:

$$\varphi(f(x) \cdot g(x)) = \varphi(f(x)) \cdot \varphi(g(x))$$

Inoltre se $f(x)$ è di grado maggiore di zero e non è del tipo $a \cdot x^n$ allora il suo polinomio caratteristico $\varphi(f(x))$ ha lo stesso grado di $f(x)$ e $\varphi(\varphi(f(x))) = f(x)$. Da tutto questo si ha che:

$$\mu_\alpha(x) = \mu_{\alpha^{-1}}(x)$$

Definizione 7.27. Un'estensione $\mathbb{F}$ di un campo $\mathbb{K}$ si dice **algebrica** se ogni $\alpha \in \mathbb{F}$ è algebrico su $\mathbb{K}$.

In maniera analoga alla dimostrazione usata nel Teorema 7.23 si dimostra che:

Proposizione 7.28. *Ogni estensione finita è algebrica.*

Dimostrazione. Sia $[\mathbb{F} : \mathbb{K}] = n$ e consideriamo $\alpha \in \mathbb{F}$. Per ipotesi gli $n + 1$ elementi $1, \alpha, \ldots, \alpha^n \in \mathbb{F}$ sono linearmente dipendenti su $\mathbb{K}$, quindi esistono $k_0, k_1, \ldots, k_n \in \mathbb{K}$ non tutti nulli, tali che $\sum_{i=0}^{n} k_i \alpha^i = 0$. Allora il polinomio $\sum_{i=0}^{n} k_i x^i$ di $\mathbb{K}[x]$ è non nullo (perché non tutti i coefficienti sono nulli) e si annulla in α. □

Dai risultati del Teorema 7.23 e della Proposizione 7.28 segue quel che avevamo anticipato di voler provare nel paragrafo precedente, ovvero che:

Corollario 7.29. *Se α è algebrico su $\mathbb{K}$, allora $\mathbb{K}(\alpha)$ è un'estensione algebrica di $\mathbb{K}$. In particolare $\mathbb{K}(\alpha)$ è finita su $\mathbb{K}$ se e solo se $\mathbb{K}(\alpha)$ è un'estensione algebrica su $\mathbb{K}$.*

Teorema 7.30. *Siano $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{F}$ campi, con $\mathbb{E}$ estensione finita di $\mathbb{K}$ di grado m e $\mathbb{F}$ estensione finita di $\mathbb{E}$ di grado n. Allora $\mathbb{F}$ è anch'essa un'estensione finita di $\mathbb{K}$ e inoltre:*

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{K}].$$

Dimostrazione. Indichiamo con $A = \{\alpha_1, \ldots, \alpha_m\}$ una base di $\mathbb{E}$ su $\mathbb{K}$ e con $B = \{\beta_1, \ldots, \beta_n\}$ una base di $\mathbb{F}$ su $\mathbb{E}$. Dobbiamo dimostrare che $[\mathbb{F} : \mathbb{K}] = m \cdot n$, lo facciamo mostrando che l'insieme:

$$I = \{\alpha_i \cdot \beta_j | \alpha_i \in A,\ \beta_j \in B\}$$

è una base di $\mathbb{F}$ su $\mathbb{K}$.

Se $x \in \mathbb{F}$, allora esistono $e_1, \ldots, e_n \in \mathbb{E}$ tali che $x = \sum_{j=1}^{n} e_j \cdot \beta_j$, infatti i β_j sono una base di $\mathbb{F}$ su $\mathbb{E}$. D'altra parte, essendo gli α_i una base di $\mathbb{E}$ su $\mathbb{K}$, gli e_j si possono scrivere come combinazione lineare degli α_i, cioè:

$$e_j = \sum_{i=0}^{m} k_{ji}\alpha_i \quad \text{con} \quad k_{ji} \in \mathbb{K}$$

Perciò possiamo scrivere x proprio come combinazione lineare degli elementi di I, ovvero I è un insieme di generatori dello spazio vettoriale $\mathbb{F}$ su $\mathbb{K}$

$$x = \sum_{j=1}^{n} e_j \cdot \beta_j = \sum_{j=1}^{n} (\sum_{i=1}^{m} k_{ji}\alpha_i)\beta_j = \sum_{j=1}^{n}\sum_{i=1}^{m} k_{ji}\alpha_i\beta_j.$$

Mostriamo adesso che I è un insieme di elementi linearmente indipendenti su $\mathbb{K}$. Infatti supponiamo che esista una combinazione lineare nulla in $\mathbb{K}$ degli elementi di I:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} k_{ji}\alpha_i\beta_j = 0$$

Per ogni j raccogliamo i termini in β_j ottenendo:

$$\sum_{j=1}^{n} \underbrace{(\sum_{i=1}^{m} k_{ji}\alpha_i)}_{\in \mathbb{E}} \beta_j = 0$$

Cioè esistono $e_1, \ldots, e_m \in \mathbb{E}$ tali che:

$$\sum_{j=1}^{n} e_j\beta_j = 0.$$

Essendo $\beta_1, \ldots, \beta_n$ una base di $\mathbb{F}$ su $\mathbb{E}$, questo implica che gli e_j son tutti nulli. Quindi per ogni $j \in \mathbb{N}_n$ si ha che $\sum_{i=1}^{m} k_{ji}\alpha_i = 0$ e usando questa volta l'ipotesi che $\alpha_1, \ldots, \alpha_m$ è una base di $\mathbb{E}$ su $\mathbb{K}$, si ottiene che deve essere $k_{ji} = 0$, per ogni $j \in \mathbb{N}_n$ e per ogni $i \in \mathbb{N}_m$. □

Corollario 7.31. *Il polinomio minimo $\mu_\alpha(x)$ su $\mathbb{K}$ di un elemento $\alpha \in \mathbb{F}$, con $\mathbb{F}/K$ finita, ha grado che divide $[\mathbb{F} : \mathbb{K}]$.*

Dimostrazione. Basta osservare che dal Teorema 7.30 si ha che:

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}(\alpha)] \cdot \underbrace{[\mathbb{K}(\alpha) : \mathbb{K}]}_{deg(h(x))}$$

□

Sia $\mathbb{F}$ un'estensione di un campo $\mathbb{K}$ e consideriamo l'insieme A degli elementi di $\mathbb{F}$ che sono algebrici su $\mathbb{K}$. Se $\mathbb{F}$ è un'estensione algebrica di $\mathbb{K}$ allora $A = \mathbb{F}$ è un campo estensione di $\mathbb{K}$, vogliamo mostrare che questo è vero in generale per qualsiasi estensione di $\mathbb{K}$:

Proposizione 7.32. *Siano $\mathbb{K} \subseteq \mathbb{F}$ campi. Consideriamo l'insieme:*

$$A = \{\alpha \in \mathbb{F} | \alpha \text{ è algebrico su } \mathbb{K}\}.$$

A è un'estensione di $\mathbb{K}$.

DIMOSTRAZIONE. Che A contenga $\mathbb{K}$ lo abbiamo già osservato, quello che dobbiamo dimostrare è che A è un campo. In particolare dimostriamo che se α, β sono in A allora $\alpha+\beta, \alpha\cdot\beta, -\alpha \in A$ e se α è diverso da 0 anche $\alpha^{-1} \in A$. Consideriamo il campo $\mathbb{K}(\alpha,\beta)$ che possiamo indicare anche come $(\mathbb{K}(\alpha))(\beta)$ (sono entrambi il minimo sottocampo contenente $\mathbb{K}$, α e β). Sappiamo (osservazione 7.3) che β è algebrico su $\mathbb{K}(\alpha)$ dunque $(\mathbb{K}(\alpha))(\beta)$ è un'estensione finita su $\mathbb{K}(\alpha)$ e $\mathbb{K}(\alpha)$ è finita su $\mathbb{K}$. Dunque dal Teorema 7.30 si ha:

$$[(\mathbb{K}(\alpha))(\beta):\mathbb{K}] = \underbrace{[(\mathbb{K}(\alpha))(\beta):\mathbb{K}(\alpha)]}_{<\infty} \cdot \underbrace{[\mathbb{K}(\alpha):\mathbb{K}]}_{<\infty} < \infty$$

Dunque per la Proposizione 7.28 $(\mathbb{K}(\alpha))(\beta)$ è algebrica su $\mathbb{K}$, in particolare $\alpha+\beta$, $\alpha\cdot\beta$, $-\alpha$ e (se $\alpha \neq 0$) α^{-1} sono algebrici su $\mathbb{K}$ e quindi elementi di A. □

Esercizio 7.33. *Sia $\alpha \in \mathbb{C}$ radice di $f(x) = x^3+2x-1$. Calcolare il polinomio minimo di $\alpha+1$, α^{-1} e α^2+1 su $\mathbb{Q}$.*

Svolgimento. Il testo dell'esercizio ci dice che α è algebrico su $\mathbb{Q}$ inoltre osserviamo che $f(x)$ non ha radici su $\mathbb{Q}$ ed essendo di grado 3 questo equivale al fatto che $f(x)$ è irriducibile in $\mathbb{Q}[x]$. Perciò $f(x)$ è il polinomio minimo di α su $\mathbb{Q}$, dunque:

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$$

Ora $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha+1) = \mathbb{Q}(\alpha^{-1})$ dunque anche i polinomi minimi di $\alpha+1$ e α^{-1} sono di grado 3 su $\mathbb{Q}$ e quindi sono rispettivamente $f(x-1)$ e il polinomio reciproco $f(\frac{1}{x})\cdot x^{deg(f(x))}$ per -1 (l'inverso di -1 termine noto di $f(x)$). Per quanto riguarda α^2+1 si può osservare che è un elemento di $\mathbb{Q}(\alpha)$, dunque si ha:

$$\mathbb{Q} \subset \mathbb{Q}(\alpha^2+1) \subset \mathbb{Q}(\alpha)$$

e quindi l'estensione $\mathbb{Q}(\alpha^2+1)$ deve avere grado che divide 3 (il grado di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$) ovvero deve essere di grado 1 (cioè $\mathbb{Q}(\alpha^2+1) = \mathbb{Q}$) o di grado 3 ($\mathbb{Q}(\alpha^2+1) = \mathbb{Q}(\alpha)$). Per essere di grado 1 deve essere α^2+1 un elemento di $\mathbb{Q}$. Se così fosse anche α^2 apparterebbe a $\mathbb{Q}$ e dunque il polinomio a coefficienti razionali $x^2-\alpha^2$ si annullerebbe in α e questo è assurdo: abbiamo già notato che l'estensione $\mathbb{Q}(\alpha)$ ha grado 3 su $\mathbb{Q}$. Dunque $\mathbb{Q}(\alpha^2+1) = \mathbb{Q}(\alpha)$ e il polinomio minimo di α^2+1 ha grado 3 su $\mathbb{Q}$. Per trovarlo si può considerare un generico polinomio $g(x) = x^3+ax^2+bx+c$ monico di terzo grado in $\mathbb{Q}[x]$ valutarlo in α^2+1 ed eguagliarlo a 0. Considerando che α è radice di $f(x)$ si ha che:

$$\alpha^3+2\alpha-1 = 0 \leftrightarrow \alpha^3 = -2\alpha+1$$

e quindi otteniamo un sistema del tipo:

$$w_1\alpha^2 + w_2\alpha + w_3 = 0 \tag{2.2}$$

con i w_i che sono funzione delle incognite a, b, c. Una delle conseguenze del Teorema 7.23 è che $1, \alpha, \alpha^2$ è una base dello spazio vettoriale $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$, dunque l'equazione 2.2 ha soluzione se e solo se i w_i sono tutti nulli. Vediamo in pratica come fare:

$$(\alpha^2+1)^0 = 1 \quad (\alpha^2+1)^1 = \alpha^2+1 \quad (\alpha^2+1)^2 = \alpha^4+2\alpha^2+1 = \alpha+1$$

Imponendo che $g(x) = x^3+ax^2+bx+c$ si annulli in α^2+1 si trova:

$$\alpha^2(b+1)+\alpha(a-1)+2+a+b+c$$

Da cui (essendo appunto 1, α, α^2 linearmente indipendenti) il sistema risultante è:

$$\begin{cases} b = -1 \\ a = 1 \\ c = -2 \end{cases}$$

Ed il polinomio minimo è $g(x) = x^3 + x^2 - x - 2$.

Si poteva anche osservare che da $\alpha^3 + 2\alpha - 1 = 0$ segue (essendo α diverso da 0):

$$\alpha^2 + 2 = \alpha^{-1}$$

Ovvero $\alpha^2 + 1 = \alpha^{-1} - 1$ e dunque si poteva ottenere il polinomio minimo[3] di $\alpha^2 + 1$ su $\mathbb{Q}$ *traslando* quello di α^{-1}.

A questo punto andiamo ancora più nel dettaglio sul legame tra estensioni finite e algebriche. Abbiamo dimostrato che un'estensione finita è algebrica e, nel caso particolare delle estensioni semplici, che $\mathbb{K}(\alpha)$ è finita su $\mathbb{K}$ se e solo se $\mathbb{K}(\alpha)$ è algebrica su $\mathbb{K}$. Sarà vera in generale questa identificazione? La risposta è negativa e lo vediamo mostrando esplicitamente un esempio di estensione algebrica non finita.

Esempio 7.34. Consideriamo l'insieme $A = \{\alpha \in \mathbb{C} | \alpha \text{ è algebrica su } \mathbb{Q}\}$, A, per come è definito, è una estensione algebrica di $\mathbb{Q}$. Supponiamo che A sia un'estensione finita di grado m su $\mathbb{Q}$ e consideriamo $\alpha = \sqrt[n]{2}$ con $n > m$. $\alpha \in A$ infatti è radice del polinomio razionale $x^n - 2$ e dunque si ha la seguente catena di estensioni:

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset A$$

Ma il polinomio minimo di α è proprio $x^n - 2$ (perché, per esempio utilizzando Eisenstein, si dimostra che è irriducibile su $\mathbb{Q}$) e dunque:

$$m = [\mathbb{Q}(\alpha) : \mathbb{Q}] > [A : \mathbb{Q}] = n$$

E questo è assurdo. Quindi A non può essere un'estensione finita di $\mathbb{Q}$ seppure sia algebrica.

Proposizione 7.35. *Siano $\mathbb{K}, \mathbb{E}, \mathbb{F}$ campi. Se $\mathbb{E}$ è un'estensione algebrica di $\mathbb{K}$ e $\mathbb{F}$ è un'estensione algebrica di $\mathbb{E}$ allora $\mathbb{F}$ è un'estensione algebrica di $\mathbb{K}$.*

Dimostrazione. Dobbiamo dimostrare che ogni elemento α di $\mathbb{F}$ è algebrico su $\mathbb{K}$. Per ipotesi α è algebrico su $\mathbb{E}$ quindi esiste un polinomio $\sum_{i=0}^{n} e_i x^i \in \mathbb{E}[x]$ diverso dal polinomio nullo (cioè esiste almeno un e_i diverso da 0) che si annulla in α. Essendo gli e_i elementi di $\mathbb{E}$ sono, per ipotesi, algebrici su $\mathbb{K}$, quindi (Corollario 7.29) le estensioni semplici fatte con gli e_i sono finite. Abbiamo dunque la seguente catena di estensioni:

$$\underbrace{\mathbb{K} \subseteq}_{\text{finita}} \underbrace{\mathbb{K}(e_0) \subseteq}_{\text{finita}} \mathbb{K}(e_0, e_1) \subseteq \ldots \underbrace{\subseteq \mathbb{K}(e_0, \ldots, e_n)}_{\text{finita}}$$

Dunque, usando la Proposizione 7.28, l'estensione $\mathbb{L} = \mathbb{K}(e_0, \ldots, e_n)$ è finita su $\mathbb{K}$: il suo grado è il prodotto dei gradi finiti delle precedenti estensioni semplici). Osserviamo che $\sum_{i=0}^{n} e_i x^i$ è un polinomio a coefficienti in $\mathbb{L}$, cioè α è algebrico su

[3] Previa dimostrazione del fatto che l'estensione è di grado 3 o dimostrando poi successivamente che è polinomio minimo verificandone l'irriducibilità su $\mathbb{Q}[x]$.

$\mathbb{L}$ e quindi, sempre per il Corollario 7.29, $\mathbb{L}(\alpha)$ è un'estensione finita di $\mathbb{L}$. Si ha dunque:

$$[\mathbb{L}(\alpha):\mathbb{K}] \underbrace{=}_{Teo.\ 7.30} [\mathbb{L}(\alpha):\mathbb{L}]\cdot[\mathbb{L}:\mathbb{K}] < \infty$$

Ciò implica (Corollario 7.29) che $\mathbb{L}(\alpha)$ è algebrica su $\mathbb{K}$ e in particolare che α è un elemento algebrico su $\mathbb{K}$. □

Osserviamo che il viceversa della Proposizione 7.35 è vero. Infatti, se $\mathbb{E}$ non è un'estensione algebrica di $\mathbb{K}$, allora esiste un $\alpha \in \mathbb{E} \subset \mathbb{F}$ che è trascendente su $\mathbb{K}$. Analogamente se $\mathbb{F}$ non è un'estensione algebrica di $\mathbb{E}$ allora esiste $\omega \in \mathbb{F}$ che è trascendente su $\mathbb{E}$, ovvero non esiste un polinomio in $\mathbb{E}[x]$ che si annulla in ω. Di conseguenza non esiste nessun polinomio in $\mathbb{K}[x]$ che si annulla in ω ($\mathbb{K} \subset \mathbb{E}$) e quindi ω è un elemento di $\mathbb{F}$ trascendente su $\mathbb{K}$. Possiamo dunque dimostrare la seguente caratterizzazione delle estensioni finite di un campo:

Teorema 7.36. *Un'estensione $\mathbb{E}$ di un campo $\mathbb{K}$ è finita se e solo se $\mathbb{E} = \mathbb{K}(\alpha_1,\dots,\alpha_r)$ con $\alpha_i \in \mathbb{E}$ algebrici su $\mathbb{K}$.*

Dimostrazione. Supponiamo che $[\mathbb{E}:\mathbb{K}] = n$. Osserviamo che (Proposizione 7.28) $\mathbb{E}$ è algebrica su $\mathbb{K}$ e procediamo per induzione su n.
Passo base. Se $n = 1$ allora $\mathbb{E} = \mathbb{K}$ e la tesi è vera con $r = 0$.
Passo induttivo. Supponiamo dunque $n \geq 2$ e consideriamo un elemento $\alpha \in \mathbb{E} \setminus \mathbb{K}$, dal Teorema 7.30 segue che:

$$n = [\mathbb{E}:\mathbb{K}] = [\mathbb{E}:\mathbb{K}(\alpha)]\cdot[\mathbb{K}(\alpha):\mathbb{K}]$$

Per quello che abbiamo osservato α è algebrico su $\mathbb{K}$ (il grado dell'estensione semplice è finito) ed $\mathbb{E}$ è algebrica su $\mathbb{K}(\alpha)$ e di grado minore di n (abbiamo scelto α in modo che $[\mathbb{K}(\alpha):\mathbb{K}]$ sia maggiore di uno). Dunque per ipotesi induttiva esistono $\alpha_1,\dots,\alpha_{r-1}$ elementi algebrici su $\mathbb{K}(\alpha)$ tali che:

$$\mathbb{E} = \mathbb{K}(\alpha)(\alpha_1,\dots,\alpha_{r-1}) = \mathbb{K}(\alpha_1,\dots,\alpha_{r-1},\alpha)$$

Dalla Proposizione 7.35 segue che $\mathbb{K}(\alpha)(\alpha_1,\dots,\alpha_{r-1})$ è algebrica su $\mathbb{K}$ e dunque tutti gli α_i sono algebrici su $\mathbb{K}$.

Viceversa siano $\alpha_1,\dots,\alpha_r$ elementi algebrici su $\mathbb{K}$ e consideriamo il campo

$$\mathbb{E} = \mathbb{K}(\alpha_1,\dots,\alpha_r)$$

Dobbiamo dimostrare che $\mathbb{E}$ è un'estensione finita di $\mathbb{K}$. Procediamo per induzione su r. Se $r = 1$ $\mathbb{E}$ è un'estensione semplice algebrica di $\mathbb{K}$ e quindi finita. Se $r \geq 2$ consideriamo il campo $\mathbb{F} = \mathbb{K}(\alpha_1,\dots,\alpha_{r-1})$ ed abbiamo:

$$[\mathbb{E}:\mathbb{K}] = [\mathbb{E}:\mathbb{F}]\cdot[\mathbb{F}:\mathbb{K}]$$

Ora $\mathbb{E} = \mathbb{F}(\alpha_r)$ ed essendo α_r algebrico su $\mathbb{K}$ lo è anche su $\mathbb{F}$ che contiene $\mathbb{K}$: dunque $[\mathbb{E}:\mathbb{F}]$ è finito. Ma per ipotesi induttiva anche $[\mathbb{F}:\mathbb{K}]$ è finito, da cui la tesi. □

Dimostreremo che nel caso di campi $\mathbb{K}$ finiti o di caratteristica zero tutte e sole le estensioni finite sono semplici (ovvero che esiste un elemento α tale che $\mathbb{E}$ del Teorema 7.36 è della forma $\mathbb{K}(\alpha)$).

Esercizio 7.37. *Calcolare* $[\mathbb{Q}(\sqrt[3]{3}+\sqrt{2}):\mathbb{Q}]$.

Svolgimento. Indichiamo con $\alpha = \sqrt[3]{3}$, con $\beta = \sqrt{2}$ e sia $\gamma = \alpha + \beta$. Osserviamo che il campo $\mathbb{Q}(\alpha + \beta)$ è contenuto in $\mathbb{Q}(\alpha, \beta)$. Consideriamo la seguente catena di estensioni:

$$\underbrace{\mathbb{Q} \underbrace{\subseteq}_{d} \mathbb{Q}(\gamma) \underbrace{\subseteq}_{c} \mathbb{Q}(\alpha, \beta)}_{n}$$

Il polinomio $x^3 - 3$ si annulla in α, inoltre per Eisenstein è irriducibile su $\mathbb{Q}$, quindi:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

Sia ora $\mu_\beta(x)$ il polinomio minimo di β su $\mathbb{Q}(\alpha)$. $\mu_\beta(x)$ divide $x^2 - 2$, che è il polinomio minimo di β su $\mathbb{Q}$. Osserviamo che:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

quindi $deg(\mu_\beta(x)) = 2$ se $\sqrt{2} \notin \mathbb{Q}(\alpha)$. E effettivamente $\sqrt{2} \notin \mathbb{Q}(\alpha)$ infatti altrimenti avremmo:

$$\underbrace{\mathbb{Q} \underbrace{\subseteq}_{2} \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)}_{3}$$

e questo è impossibile perché 2 non divide 3. Quindi:

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$$

ed essendo $\mathbb{Q}(\gamma)$ un'estensione intermedia deve avere grado d che divide 6, ovvero appartenente all'insieme $\{2, 3, 6\}$ (non può essere 1 perché $\gamma \notin \mathbb{Q}$). L'insieme

$$\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

è una base di $\mathbb{Q}(\alpha, \beta)$ su $\mathbb{Q}$, mentre l'insieme

$$A = \{1, \gamma, \ldots, \gamma^d\}$$

è linearmente dipendente su $\mathbb{Q}$. Scriviamo le coordinate degli elementi di A rispetto alla base di $\mathbb{Q}(\alpha, \beta)$:

$$\begin{gathered} 1 = (1, 0, 0, 0, 0, 0) \\ \gamma = \alpha + \beta = (0, 1, 0, 1, 0, 0) \\ \gamma^2 = \alpha^2 + 2\alpha\beta + \underbrace{2}_{\beta^2} = (2, 0, 1, 0, 2, 0) \\ \gamma^3 = \underbrace{3}_{\alpha^3} + 2\alpha^2\beta + 2\alpha + \alpha^2\beta + 4\alpha + 2\beta = (3, 6, 0, 2, 0, 3) \end{gathered}$$

Ci possiamo fermare a γ^3, perché è facile vedere, passati alle coordinate, e quindi a $\mathbb{Q}^6$, che questi quattro elementi sono linearmente indipendenti e quindi che $d > 3$, ovvero $d = 6$. Cioè:

$$\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$$

In particolare ci potremmo scrivere α e β come combinazione lineare degli elementi di γ, infatti:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 2 & 0 \\ 3 & 6 & 0 & 2 & 0 & 3 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \end{pmatrix}}_{M} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = \begin{pmatrix} 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \\ \gamma^4 \\ \gamma^5 \end{pmatrix}$$

e la matrice M è invertibile, in quanto gli elementi γ^i sono linearmente indipendenti, quindi:

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 2 & 0 \\ 3 & 6 & 0 & 2 & 0 & 3 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \\ \gamma^4 \\ \gamma^5 \end{pmatrix}$$

Esercizio 7.38. *Sia $\mathbb{K}$ un campo di caratteristica diversa da 2. Studiare le estensioni $\mathbb{E}$ di $\mathbb{K}$ quadratiche (ovvero di grado 2).*

Svolgimento. Sia $f(x) = x^2 + ax + b \in \mathbb{K}[x]$ irriducibile, allora $\mathbb{E} = \mathbb{K}[x]/(f(x))$ è un'estensione di grado 2, e al variare di $f(x)$ nei polinomi di grado 2 irriducibili di $\mathbb{K}[x]$ si generano tutte le estensioni di grado 2 di $\mathbb{K}$. Osserviamo che, essendo $char(\mathbb{K}) \neq 2$ si possono trovare le radici di $f(x)$ in una chiusura algebrica di $\mathbb{K}$ tramite la ben nota formula risolutiva delle equazioni di secondo grado:

$$x = \frac{-a \pm \sqrt{\Delta}}{2}$$

In particolare:

$$\mathbb{E} \cong \mathbb{K}(\frac{-a \pm \sqrt{\Delta}}{2}) = \mathbb{K}(\sqrt{\Delta})$$

Se $f(x)$ è irriducibile in $\mathbb{K}$ allora $\sqrt{\Delta} \notin \mathbb{K}$ (ad esempio in $\mathbb{Q}$ sono tutte le estensioni del tipo $\mathbb{Q}(\sqrt{m})$, con m che non è un quadrato). Vogliamo vedere quando $\sqrt{\alpha}$ e $\sqrt{\beta}$ generano la stessa estensione, ovvero:

$$\mathbb{K}(\sqrt{\alpha}) = \mathbb{K}(\sqrt{\beta}) \Leftrightarrow {}^4\sqrt{\alpha} \in \mathbb{K}(\sqrt{\beta}).$$

perché le due estensioni siano uguali deve quindi essere:

$$\sqrt{\alpha} = c + d\sqrt{\beta}$$

elevando al quadrato questa relazione si ottiene:

$$\alpha = c^2 + d^2\beta + 2cd\sqrt{\beta}$$

ovvero $c \cdot d = 0$. Essendo in un dominio d'integrità questo implica $c = 0$ oppure $d = 0$. Nel primo caso avremmo:

$$\sqrt{\alpha} = d\sqrt{\beta} \text{ ovvero } \frac{\alpha}{\beta} = d^2$$

[4]Basta che valga un contenimento, in questo caso l'uguaglianza è infatti garantita dal fatto che le due estensioni hanno lo stesso grado.

mentre nel secondo caso avremmo:

$$\sqrt{\alpha} = c \text{ impossibile perché } \sqrt{\alpha} \notin \mathbb{K}.$$

Concludendo $\mathbb{K}(\sqrt{\alpha}) = \mathbb{K}(\sqrt{\beta})$ se il rapporto tra α e β è un quadrato in $\mathbb{K}$. In particolare se $\mathbb{K} = \mathbb{Q}$, i $\mathbb{Q}(\sqrt{p})$ con p primo sono tutti distinti, ma più in generale $\mathbb{Q}(\sqrt{m})$ sono tutte le estensioni di $\mathbb{Q}$ di grado 2 distinte se m è libero da quadrati, ovvero nella sua fattorizzazione in primi non ci sono esponenti di grado maggiore di 1.

Esercizio 7.39. *Calcolare* $[\mathbb{Q}(\sqrt{7}, \sqrt{-2}) : \mathbb{Q}]$.

Svolgimento. Risolviamo questo esercizio in due diversi modi, uno dei quali sfrutta quanto dimostrato nell'Esercizio 7.38. Osserviamo che:

$$[\mathbb{Q}(\sqrt{7}, \sqrt{-2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{7}, \sqrt{-2}) : \mathbb{Q}(\sqrt{7})] \cdot [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}]$$

e che $x^2 - 7$ è il polinomio minimo di $\sqrt{7}$ in $\mathbb{Q}[x]$. Quindi:

$$[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$$

Inoltre $x^2 + 2$ è il polinomio minimo di $\sqrt{-2}$ in $\mathbb{Q}[x]$, quindi:

$$[\mathbb{Q}(\sqrt{7}, \sqrt{-2}) : \mathbb{Q}(\sqrt{7})] \leq 2$$

Si tratta di capire se $\mathbb{Q}(\sqrt{7}, \sqrt{-2}) = \mathbb{Q}(\sqrt{7})$. La risposta è no, una spiegazione è che $\sqrt{-2} \in \mathbb{Q}(\sqrt{7})$ se e solo se $\dfrac{-2}{7}$ è un quadrato in $\mathbb{Q}$ e non è questo il caso. Ma potevamo anche osservare che $\mathbb{Q}(\sqrt{7}) \subseteq \mathbb{R}$, mentre $\sqrt{-2} \notin \mathbb{R}$.

3. Chiusura algebrica di un campo $\mathbb{K}$

Il teorema fondamentale dell'algebra dimostra che $\mathbb{C}$ ha la proprietà che ogni polinomio in $\mathbb{C}[x]$ ha almeno una radice in $\mathbb{C}$. Tale proprietà equivale, per Ruffini, al fatto che gli irriducibili in $\mathbb{C}[x]$ sono tutti e soli i polinomi di primo grado. In particolare tutti gli elementi algebrici di $\mathbb{C}$ appartengono a $\mathbb{C}$. Un campo che abbia questa proprietà dei numeri complessi si dice algebricamente chiuso.

Definizione 7.40. Un campo $\mathbb{L}$ si dice **algebricamente chiuso** se ogni polinomio in $\mathbb{L}[x]$ di grado maggiore di zero ha una radice in $\mathbb{L}$.

Se un campo $\mathbb{K}$ non è algebricamente chiuso, e $f(x)$ è un polinomio di $\mathbb{K}[x]$ di grado maggiore di zero senza radici in $\mathbb{K}$, vogliamo capire come costruire (e se sia sempre possibile) un'estensione $\mathbb{E}$ di $\mathbb{K}$ in cui $f(x)$ ha una radice.

Lemma 7.41. *Siano $\mathbb{K}$ un campo e $f(x) \in \mathbb{K}[x]$ irriducibile in $\mathbb{K}[x]$. Allora il campo quoziente $\mathbb{E} = \mathbb{K}[x]/(f(x))$ contiene una radice α di $f(x)$. α è la classe di $x \in \mathbb{K}[x]$ in $\mathbb{E}$ ed $\mathbb{E} \cong \mathbb{K}(\alpha)$ (dunque $\mathbb{E}$ è un'estensione semplice di $\mathbb{K}$, $\mathbb{E} = \mathbb{K}(\alpha)$).*

Dimostrazione. Consideriamo l'immersione λ di $\mathbb{K}$ in $\mathbb{K}[x]$ (ovvero per ogni $k \in \mathbb{K}$, $\lambda(k) = k$) e la proiezione $\pi_{(f(x))} : \mathbb{K}[x] \to \mathbb{E}$. Abbiamo il seguente diagramma:

$$\mathbb{K} \xrightarrow{\lambda} \mathbb{K}[x] \xrightarrow{\pi_{(f(x))}} \mathbb{K}[x]/(f(x)) = \mathbb{E}$$

Dunque $\lambda \circ \pi_{(f(x))}$, che indicheremo con τ, è un omomorfismo iniettivo da $\mathbb{K}$ in $\mathbb{E}$: in particolare $\mathbb{E}$ contiene il campo $\mathbb{K}$ (O per essere più precisi la copia isomorfa

$\tau(\mathbb{K})$ di $\mathbb{K}$). Vogliamo dimostrare che $\alpha = \pi(x)_{(f(x))}$ è radice del polinomio $f(x)$. Sia $f(x) = \sum_{i=0}^{n} a_i x^i$ e valutiamolo in α:

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$$

Sostituendo $\pi_{(f(x))}(x)$ al posto di α e osservando che $\pi_{(f(x))}$ lascia fissi gli elementi di $\mathbb{K}$ si ha:

$$f(\alpha) = \sum_{i=0}^{n} \pi_{(f(x))}(a_i)(\pi(x))^i \underbrace{=}_{\pi_{(f(x))}\ omo.} \pi_{(f(x))}(\sum_{i=0}^{n} a_i x^i) = \pi_{(f(x))}(f(x)) = 0$$

Osserviamo inoltre che $\mathbb{E} \cong \mathbb{K}(\alpha)$ infatti "contiene" (nel senso che contiene una copia isomorfa) $\mathbb{K}$ e α e quindi contiene $\mathbb{K}(\alpha)$ (che è il più piccolo sottocampo che li contiene entrambi). Viceversa ogni elemento di $\mathbb{E}$ è una classe di resto modulo $f(x)$ e dunque si può scrivere come somme finite di elementi di $\mathbb{K}$ per potenze di $\pi_{(f(x))}(x) = \alpha$ ed è dunque contenuto in $\mathbb{K}(\alpha)$. Ovvero $\mathbb{E}$ è un'estensione semplice di (un campo isomorfo a) $\mathbb{K}$. □

Teorema 7.42. *Siano $\mathbb{K}$ un campo e $f(x) \in \mathbb{K}[x]$ di grado maggiore di zero. Allora esiste un campo $\mathbb{E}$ contenente[5] $\mathbb{K}$ tale che $f(x)$ ha una radice in $\mathbb{E}$.*

Dimostrazione. Basta notare che una radice di un fattore irriducibile qualsiasi di $f(x)$ è anche una radice di $f(x)$ e applicare il Lemma 7.41 ad un fattore irriducibile di $f(x)$. □

Proposizione 7.43. *Sia $\mathbb{K}$ un campo e $f_1(x), \ldots, f_n(x) \in \mathbb{K}[x]$ polinomi con grado maggiore di zero. Allora esiste un campo $\mathbb{E}$ contenente $\mathbb{K}$ tale che ognuno degli $f_i(x)$ ha una radice in $\mathbb{E}$.*

Dimostrazione. Procediamo per induzione sul numero n dei polinomi di $\mathbb{K}[x]$.
Passo base. Se $n = 1$ la tesi equivale a quanto già dimostrato nel Lemma 7.41.
Passo induttivo. Supponiamo dunque che dati comunque $n-1$ polinomi in $\mathbb{K}[x]$ esista un campo $\mathbb{L}$ contenente $\mathbb{K}$ in cui gli $n-1$ polinomi hanno almeno una radice. Consideriamo il campo $\mathbb{L}$ con questa proprietà rispetto ai polinomi $f_i(x)$, con i compreso tra 1 e $n-1$. Il polinomio $f_n(x)$ appartiene in particolare ad $\mathbb{L}[x]$ e, applicando nuovamente il Lemma 7.41, troviamo un campo $\mathbb{E}$ che contiene $\mathbb{L}$ (e dunque $\mathbb{K}$ e almeno una radice per ogni $f_i(x)$ con i compreso tra 1 e $n-1$) in cui $f_n(x)$ ha una radice. □

Più in generale, si può dimostrare che dato un campo $\mathbb{K}$ esiste una sua estensione che contiene una radice di ogni polinomio in $\mathbb{K}[x]$ di grado positivo.

Teorema 7.44. *Sia $\mathbb{K}$ un campo. Esiste un campo $\mathbb{E}$ contenente $\mathbb{K}$ tale che ogni polinomio $f(x) \in \mathbb{K}[x]$ di grado maggiore di zero, abbia una radice in $\mathbb{E}$.*

Dimostrazione. Consideriamo l'anello:

$$A = \mathbb{K}[x_f]_{f \in F} \quad F = \{f(x) \in \mathbb{K}[x] | deg(f) \geq 1\}$$

Cioè l'anello dei polinomi a coefficienti in $\mathbb{K}$ con una variabile per ogni polinomio di grado maggiore di zero. Sia $I = (f(x_f))_{f \in F}$, vogliamo mostrare che I è un ideale

[5]Nel senso specificato precedentemente che contiene un campo isomorfo a $\mathbb{K}$.

proprio, in particolare quindi che $1 \notin I$.
Procediamo per assurdo, supponiamo che $1 \in I$, allora:

$$1 = \sum_{i=0}^{n} g_i f_i(x_{f_i}) \quad g_i \in A.$$

Per semplicità di notazione scriviamo x_i in luogo di x_{f_i} e supponiamo che tutte le variabili in gioco nell'equazione precedente siano: $x_1, ..., x_n, x_{n+1}, ..., x_N$:

$$1 = \sum_{i=0}^{n} g_i(x_1, ..., x_N) f_i(x_i). \tag{3.1}$$

Siano $\mathbb{F} \supseteq \mathbb{K}$ un campo e $\alpha \in \mathbb{F}$ e consideriamo l'applicazione φ_α tale che:

$$\forall\ f(x) \in \mathbb{K}[x] :\ \varphi_\alpha(f(x)) = f(\alpha).$$

φ_α è un omomorfismo così come l'applicazione che a tutti i polinomi in due variabili $f(x, y)$ associa $f(\alpha, \beta)$. Sia $\mathbb{E}$ un campo contenente una radice α_i di ognuno degli f_i e consideriamo la seguente valutazione da A in $\mathbb{E}$:

$$\forall\ 1 \leq i \leq n\ \varphi(x_i) = \alpha_i \quad \forall\ i \notin \{1, ..., n\}\ \varphi(x_i) = 0.$$

Applichiamo l'omomorfismo φ all'equazione 3.1:

$$1 = \sum_{i=1}^{n} g_i(\alpha_1, ..., \alpha_n, 0, ..., 0) f_i(\alpha_i) = 0.$$

Assurdo, quindi $I \neq A$. Questo implica che esiste un ideale massimale M che contiene I (ogni ideale proprio è contenuto in un ideale massimale): $I \subseteq M \subset A$. Il campo $\mathbb{E} = A/M$ contiene una copia isomorfa di $\mathbb{K}$, infatti la composizione dei seguenti omomorfismi:

$$\mathbb{K} \longrightarrow \mathbb{K}[x_f]_{f \in F} \longrightarrow \mathbb{K}[x_f]_{f \in F}/M$$

è iniettiva, in quanto l'immagine di $1 \in \mathbb{K}$ non è nulla. Inoltre in $\mathbb{E}$, c'è una radice per ogni polinomio $f(x)$ di $\mathbb{K}[x]$. Consideriamo infatti il corrispondente polinomio $f(x_f) \in A$ allora $\pi(x_f)$, proiezione in $\mathbb{E}$, è una radice:

$$f(\overline{x_f}) = \overline{f(x_f)} = \overline{0}$$

□

Dal Teorema 7.44 segue che:

Corollario 7.45. *Dato un campo $\mathbb{K}$ esiste un campo $\mathbb{L}$ algebricamente chiuso contenente $\mathbb{K}$.*

Dimostrazione. Osserviamo che il Teorema 7.44 dimostra che esiste un campo $\mathbb{E}$, che contiene $\mathbb{K}$, in cui sono contenute tutte le radici dei polinomi di grado positivo in $\mathbb{K}[x]$. Ora vogliamo dimostrare che esiste una estensione $\mathbb{L}$ di $\mathbb{K}$ in cui sono contenute tutte le radici dei polinomi di grado positivo in $\mathbb{L}[x]$.

Iteriamo il risultato del Teorema 7.44 per costruire la seguente catena di campi:

$$\mathbb{E}_0 = \mathbb{K} \subseteq \mathbb{E}_1 \subseteq \ldots \subseteq \mathbb{E}_n \subseteq \ldots$$

dove gli $\mathbb{E}_i$ sono campi tali che ogni polinomio in $\mathbb{E}_i[x]$ ha almeno una radice in $\mathbb{E}_{i+1}$. L'insieme $\mathbb{L} = \cup_{i \in \mathbb{N}} \mathbb{E}_i$ è un campo, in quanto unione di campi *incapsulati* (ovvero uno contenuto nell'altro), inoltre se $f(x) \in \mathbb{L}[x]$ allora esiste n tale che

$f(x) \in \mathbb{E}_n[x]$ e quindi per costruzione in $\mathbb{E}_{n+1}$ (che è contenuto in $\mathbb{L}$ esiste una radice di $f(x)$). □

Definizione 7.46. Un'estensione $\overline{\mathbb{K}}$ di un campo $\mathbb{K}$ si dice una **chiusura algebrica** di $\mathbb{K}$ se è algebricamente chiusa e se ogni α di $\overline{\mathbb{K}}$ è algebrico su $\mathbb{K}$ (cioè $\overline{\mathbb{K}}$ è un'estensione algebrica di $\mathbb{K}$).

Esempio 7.47. $\mathbb{C}$ non è la chiusura algebrica di $\mathbb{Q}$ infatti pur essendo algebricamente chiuso non è una estensione algebrica di $\mathbb{Q}$ (contiene elementi trascendenti su $\mathbb{Q}$). Potevamo inoltre osservare che la chiusura algebrica di $\mathbb{Q}$ ha cardinalità numerabile (in quanto le possibili radici di polinomi a coefficienti razionali sono una unione numerabile di numerabili) a differenza di $\mathbb{C}$.

Dalla dimostrazione del corollario 7.45 segue che:

Corollario 7.48. *Dato un campo $\mathbb{K}$, esiste un campo $\overline{\mathbb{K}}$ algebricamente chiuso, contenente $\mathbb{K}$ e algebrico su $\mathbb{K}$.*

Dimostrazione. Consideriamo il campo $\mathbb{L}$ della tesi del corollario 7.45 e definiamo $\overline{\mathbb{K}}$ come il sottocampo (Proposizione 7.32) di $\mathbb{L}$ degli algebrici su $\mathbb{K}$. Gli elementi di $\mathbb{K}$ sono contenuti in $\mathbb{L}$ e algebrici su $\mathbb{K}$ dunque $\overline{\mathbb{K}}$ contiene il campo $\mathbb{K}$ dobbiamo dimostrare che è algebricamente chiuso. Sia $f(x) \in \overline{\mathbb{K}}[x]$ di grado maggiore di zero, allora esiste una radice β di $f(x)$ in $\mathbb{L}$. Dalla Proposizione 7.35 segue che $\overline{\mathbb{K}}(\beta)$ è algebrica su $\mathbb{K}$: questo significa che l'elemento β di $\mathbb{L}$ è algebrico su $\mathbb{K}$ e quindi $\beta \in \overline{\mathbb{K}}$. □

Più in generale:

Teorema 7.49. *Dato un campo $\mathbb{K}$ esiste una e una sola (a meno di isomorfismi di anelli) chiusura algebrica $\mathbb{E}$ di $\mathbb{K}$.*

Nel seguito prenderemo in considerazione solo campi $\mathbb{K}$ tali che ogni polinomio irriducibile $f(x)$ di grado n a coefficienti in $\mathbb{K}$ abbia n radici distinte in una chiusura algebrica di $\mathbb{K}$.

Col prossimo teorema mostriamo che tale proprietà è sempre verificata per polinomi a coefficienti in $\mathbb{K}$, con $\mathbb{K}$ campo di caratteristica 0 o uguale a $\mathbb{Z}_p$.

Teorema 7.50. *Sia $\mathbb{K}$ di caratteristica 0 oppure $\mathbb{K} = \mathbb{Z}_p$. Un polinomio $f(x)$ irriducibile di grado n di $\mathbb{K}[x]$ ha n radici distinte in un campo algebricamente chiuso $\mathbb{L}$ contenente $\mathbb{K}$.*

Dimostrazione. Indichiamo con $\mathbb{L}$ una chiusura algebrica di $\mathbb{K}$ e sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$ $(a_n \neq 0)$ irriducibile con radici $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$, vogliamo mostrare che gli α_i sono tutti distinti. Se $deg(f(x)) = 1$ non c'è niente da mostrare, dunque possiamo supporre $deg(f(x)) > 1$. Calcoliamo la derivata di $f(x)$:

$$f'(x) = \sum_{i=1}^{n} i a_i \cdot x^{i-1}$$

Se α è una radice multipla di $f(x)$ allora $f'(\alpha) = f(\alpha) = 0$, quindi $f'(x)$ deve essere un multiplo del polinomio minimo $h(x)$ di α in $\mathbb{K}[x]$ che ha grado n (sarà del tipo $h(x) = c \cdot f(x)$ con c costante che rende $f(x)$ monico).

Se $\mathbb{K}$ è di caratteristica 0 allora il coefficiente di grado $n-1$ di $f'(x)$ è $a_n \cdot (n-1)$ che è diverso da zero in quanto $n-1$ deve essere maggiore di zero (se $f(x)$ avesse

grado 1 avrebbe un'unica radice di molteplicità 1) e $\mathbb{K}$ è un dominio di integrità. Perciò $deg(f'(x)) = n-1$ e $f'(x)$ non può essere un multiplo di $h(x)$.

Se $\mathbb{K}$ è del tipo $\mathbb{Z}_p$ come prima $f'(x)$ non può essere multiplo di $f(x)$ a meno che non sia uguale a zero. Osserviamo che se $a_i \neq 0$, il coefficiente del termine di grado $i-1$ in $f'(x)$ che è $i \cdot a_i$, è 0 se e solo se $i = 0$ ovvero se e solo se p divide i. Quindi $f'(x) = 0$ se e solo se[6] $f(x)$ è della forma:

$$f(x) = \sum_{i=0}^{\frac{n}{p}} a_{i \cdot p} x^{i \cdot p}$$

Usando il fatto che per ogni $a, b \in \mathbb{Z}_p$ vale che $a^p = a$ e $a^p + b^p = (a+b)^p$, si ha:

$$f(x) = \sum_{i=0}^{\frac{n}{p}} a_{i \cdot p}^p (x^i)^p = (\sum_{i=0}^{\frac{n}{p}} a_{i \cdot p} x^i)^p$$

e $f(x)$ sarebbe riducibile. □

Definizione 7.51. Un'estensione algebrica $\mathbb{E}$ di un campo $\mathbb{K}$ si dice **separabile** se, per ogni α in $\mathbb{E}$, le radici del polinomio minimo su $\mathbb{K}$ di α in una chiusura algebrica di $\mathbb{K}$ sono tutte distinte.

Quello che abbiamo mostrato col Teorema 7.50 è che tutte le estensioni algebriche di campi $\mathbb{K}$ di caratteristica 0 o finiti del tipo $\mathbb{Z}_p$ sono separabili. Nei prossimi paragrafi tratteremo estensioni separabili.

4. Campi di spezzamento

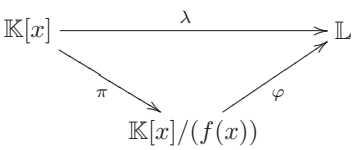
Siano $\mathbb{K}$ un campo e $f(x) \in \mathbb{K}[x]$ un polinomio irriducibile. $\mathbb{E} = \mathbb{K}[x]/(f(x))$ è un campo contenente $\mathbb{K}$ (o più precisamente c'è un omomorfismo iniettivo da $\mathbb{K}$ in $\mathbb{E}$) in cui esiste una radice di $f(x)$. Indicando con $\mathbb{L}$ un campo algebricamente chiuso contenente $\mathbb{K}$ vogliamo trovare un omomorfismo $\varphi : \mathbb{E} \longrightarrow \mathbb{L}$ tale che $\varphi|_K = id$[7]. Basta trovare $\lambda : \mathbb{K}[x] \longrightarrow \mathbb{L}$ tale che:

$$\forall k \in \mathbb{K}\ \lambda(k) = k \text{ e } \lambda(x) = c \in \mathbb{L}$$

e inoltre c deve essere una radice del polinomio $f(x)$, infatti:

$$Ker\ \lambda \supseteq (f(x)) \Leftrightarrow f(x) \in Ker\ \lambda \Leftrightarrow f(c) = 0$$

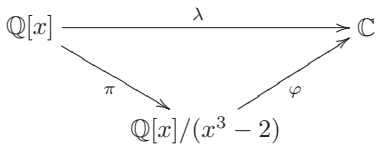
Come si può vedere dal seguente diagramma:



[6]Ricordiamo che il grado di $f(x)$ non è nullo perché per ipotesi $f(x)$ è irriducibile in $\mathbb{K}[x]$.

[7]Osserviamo che un omomorfismo che ha come dominio un campo o è l'omomorfismo banale oppure è iniettivo.

Esempio 7.52. Siano $\mathbb{K} = \mathbb{Q}$ e $f(x) = x^3 - 2$. Consideriamo $\mathbb{L} = \mathbb{C}$, allora:



Dove λ, definita su $\mathbb{Q}[x]$, deve essere costante sugli elementi di $\mathbb{Q}$, mentre può mandare x in una qualsiasi delle tre radici del polinomio $x^3 - 2$ in $\mathbb{C}$, ovvero:

$$\sqrt[3]{2},\ \sqrt[3]{2}\xi,\ \sqrt[3]{2}\xi^2$$

con ξ radice terza dell'unità.
Abbiamo quindi ottenuto tre campi isomorfi a $\mathbb{Q}[x]/(x^3 - 2)$ in $\mathbb{C}$:

$$\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\xi), \mathbb{Q}(\sqrt[3]{2}\xi^2).$$

Mostriamo che questi tre campi sono distinti:

- $\mathbb{Q}(\sqrt[3]{2})$ è distinto da $\mathbb{Q}(\sqrt[3]{2}\xi)$ e da $\mathbb{Q}(\sqrt[3]{2}\xi^2)$, perché a differenza di questi ultimi due è contenuto in $\mathbb{R}$.
- $\mathbb{Q}(\sqrt[3]{2}\xi) \neq \mathbb{Q}(\sqrt[3]{2}\xi^2)$ infatti se fossero uguali $\sqrt[3]{2}\xi$ apparterrebbe anche a $\mathbb{Q}(\sqrt[3]{2}\xi^2)$, così come $\mathbb{Q}(\sqrt[3]{2}\xi^2)$. Allora in $\mathbb{Q}(\sqrt[3]{2}\xi^2)$ ci starebbe anche il rapporto dei due elementi:

  $$\frac{\sqrt[3]{2}\xi^2}{\sqrt[3]{2}\xi} = \xi \in \mathbb{Q}(\sqrt[3]{2}\xi^2)$$

  da cui:

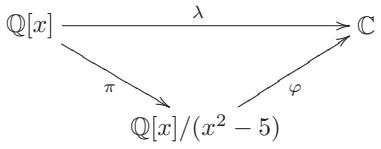
  $$\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\sqrt[3]{2}\xi^2)$$

  Quindi $\mathbb{Q}(\sqrt[3]{2}\xi^2)$ sarebbe una estensione di $\mathbb{Q}(\xi)$, ma il grado delle estensioni del tipo $\mathbb{K}(\alpha)$ su $\mathbb{K}$, con α algebrico su $\mathbb{K}$, sappiamo essere uguali al polinomio minimo di α su $\mathbb{K}$. In questo caso $\mathbb{Q}(\sqrt[3]{2}\xi^2)$ avrebbe grado 3 su $\mathbb{Q}$, mentre il polinomio minimo della radice terza dell'unità ξ è:

  $$\frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

  dunque $\mathbb{Q}(\xi)$ ha grado 2. Osservando che se $\mathbb{K} \subseteq \mathbb{E} \subset \mathbb{F}$ sono tre campi, allora $[\mathbb{F} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}]$, si ha che il grado di $\mathbb{Q}(\sqrt[3]{2}\xi^2)$ su $\mathbb{Q}$ dovrebbe essere un multiplo del grado di $\mathbb{Q}(\xi)$ su $\mathbb{Q}$. L'assurdo è dovuto alla supposizione che $\mathbb{Q}(\sqrt[3]{2}\xi)$ e $\mathbb{Q}(\sqrt[3]{2}\xi^2)$ fossero uguali.

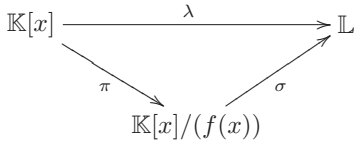
Esempio 7.53. Con gli stessi campi dell'esempio precedente consideriamo il polinomio irriducibile in $\mathbb{Q}[x]$: $x^2 - 5$. Allora abbiamo il solito diagramma:



Con λ che è l'omomorfismo che tiene fisso $\mathbb{Q}$ e manda x in una delle due radici $(\sqrt{5}, -\sqrt{5})$ complesse di $x^2 - 5$. Le due estensioni di $\mathbb{Q}$ che risultano essere isomorfe

a $\mathbb{Q}[x]/(x^2-5)$ sono quindi $\mathbb{Q}(\sqrt{5})$ e $\mathbb{Q}(-\sqrt{5})$. Gli omomorfismi λ sono diversi, ma i campi risultanti sono uguali, quindi in $\mathbb{C}$ c'è un solo campo isomorfo a $\mathbb{Q}[x]/(x^2-5)$.

In generale dati $f(x)$ irriducibile di $\mathbb{K}[x]$ e $\mathbb{L}$ una chiusura algebrica di $\mathbb{K}$, possiamo considerare il campo $\mathbb{E} = \mathbb{K}[x]/(f(x))$ e costruire un omomorfismo $\lambda : \mathbb{K}[x] \longrightarrow \mathbb{L}$ che lascia fissi gli elementi di $\mathbb{K}$ e che manda x in una qualsiasi delle radici distinte del polinomio $f(x)$ in $\mathbb{L}$. Supponiamo che $f(x)$ abbia n radici distinte, allora ci sono n modi di costruire l'omomorfismo λ, con n che è il grado di f o anche $[\mathbb{K}[x]/(f(x)) : \mathbb{K}]$. Definito λ, abbiamo per passaggio al quoziente , un omomorfismo $\varphi : \mathbb{E} \longrightarrow \mathbb{L}$ che ristretto a $\mathbb{K}$ è l'identità.
Sia $\varphi : \mathbb{K} \longrightarrow \mathbb{L}$ un omomorfismo di campi. Ci chiediamo quanti sono gli omomorfismi σ che estendono φ tali che: $\sigma : \mathbb{K}[x]/(f(x)) \longrightarrow \mathbb{L}$ e $\sigma|_{\mathbb{K}} = \varphi$. Basta estenderlo a $\lambda : \mathbb{K}[x] \longrightarrow \mathbb{L}$ con $Ker\ \lambda \supseteq (f(x))$ e poi per passaggio al quoziente si trova σ, come mostra il seguente diagramma:



Come condizione abbiamo che $f(x) \in Ker\ \lambda$, ovvero se $f(x) = \sum_{i=0}^{n} a_i x^i$:

$$\lambda(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \lambda(a_i)\lambda(x^i) = \sum_{i=0}^{n} \varphi(a_i)[\lambda(x)]^i = 0.$$

Quindi si può scegliere $\lambda(x)$ in tanti modi quante sono le radici distinte del polinomio in $\mathbb{L}[T]$: $\sum_{i=0}^{n} \varphi(a_i)T^i$.

Proposizione 7.54. *Sia $\mathbb{K}$ un campo di caratteristica 0 e $\mathbb{L}$ una chiusura algebrica di $\mathbb{K}$. Sia $\mathbb{E} \supseteq \mathbb{K}$ una estensione finita di $\mathbb{K}$ con $[\mathbb{E} : \mathbb{K}] = n$. Allora esistono n omomorfismi $\varphi : \mathbb{E} \longrightarrow \mathbb{L}$ tali che $\varphi|_K = id$.*

Dimostrazione. Nel caso in cui $\mathbb{E} = \mathbb{K}(\alpha) \cong \mathbb{K}[x]/(f(x))$ lo abbiamo già mostrato. Altrimenti avremo la seguente catena di estensioni:

$$\mathbb{K} \subseteq \mathbb{K}(\alpha_1) \subseteq \mathbb{K}(\alpha_1, \alpha_2) \subseteq \ldots \subseteq \mathbb{E} = \mathbb{K}(\alpha_1, \ldots, \alpha_m)$$

Si procede per induzione sul numero m di estensioni intermedie semplici. In quanti modi si può estendere l'omomorfismo identità da $\mathbb{K}$ a $\mathbb{L}$ ad un omomorfismo da $\mathbb{K}(\alpha)$ a $\mathbb{L}$? In $n_1 = [\mathbb{K}(\alpha) : \mathbb{K}]$ modi. In generale possiamo estendere l'identità su $\mathbb{K}$, a $\mathbb{E}$ in $n_1 \cdot \ldots \cdot n_m = n$ modi (dove m è il numero di estensioni che dobbiamo fare). □

Definizione 7.55. Sia $f(x) \in \mathbb{K}[x]$. Si dice **campo di spezzamento** del polinomio $f(x)$, un'estensione algebrica di $\mathbb{K}$ generata da tutte le radici del polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$. Se per esempio $\alpha_1, \ldots \alpha_t \in \mathbb{L}$ (con $t \leq n$) sono le radici distinte di $f(x)$, allora il campo di spezzamento è $\mathbb{K}(\alpha_1, \ldots, \alpha_t)$.[8]

Osservazione 7.56. Consideriamo $\mathbb{E} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ campo di spezzamento di un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$ e una chiusura algebrica $\mathbb{L}$ di $\mathbb{K}$. Vogliamo

[8]Non è detto che qualche radice non sia "superflua": $\mathbb{Q}(\sqrt{5}, -\sqrt{5})$, campo di spezzamento di $x^2 - 5 \in \mathbb{Q}[x]$, è uguale a $\mathbb{Q}(\sqrt{5})$.

costruire un omomorfismo $\sigma : \mathbb{E} \longrightarrow \mathbb{L}$ che ristretto a $\mathbb{K}$ sia l'identità. Sfruttando il fatto che σ è un omomorfismo e che su $\mathbb{K}$ è l'identità si ha:

$$0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha))$$

ovvero σ manda radici di f in radici di f, e inoltre manda radici distinte in radici distinte, in quanto non essendo l'omomorfismo banale (su $\mathbb{K}$ è l'identità) deve essere iniettivo. Perciò $\sigma(\mathbb{E}) \subseteq \mathbb{E}$, ma in realtà sappiamo che $\mathbb{E}$ è uno spazio vettoriale di dimensione n su $\mathbb{K}$, e allora la sua immagine tramite un omomorfismo iniettivo sarà ancora di dimensione n su $\mathbb{K}$, ovvero $\sigma(\mathbb{E}) = \mathbb{E}$.
Conclusione: I campi di spezzamento $\mathbb{E}$ di un polinomio $f(x) \in \mathbb{K}[x]$, hanno la proprietà che ogni omomorfismo $\sigma : \mathbb{E} \longrightarrow \mathbb{L}$ (con $\mathbb{L}$ chiusura algebrica di $\mathbb{K}$) che ristretto a $\mathbb{K}$ è l'identità, ha la proprietà che lascia fisso $\mathbb{E}$ (che non significa che è l'identità su $\mathbb{E}$ ma che $\sigma(\mathbb{E}) = \mathbb{E}$, cioè che σ è un automorfismo di $\mathbb{E}$.)

Definizione 7.57. Un'estensione algebrica $\mathbb{E}$ di un campo $\mathbb{K}$ si dice **normale** se possiede la proprietà che per ogni σ omomorfismo da $\mathbb{E}$ in una chiusura algebrica $\mathbb{L}$ di $\mathbb{K}$ tale che $\sigma|_K = id$ si ha $\sigma(\mathbb{E}) = \mathbb{E}$.

Osservazione 7.58. Supponiamo che $\mathbb{E}$ sia una estensione normale di $\mathbb{K}$ e prendiamo in considerazione l'insieme G degli omomorfismi da $\mathbb{E}$ in una chiusura algebrica $\mathbb{L}$ di $\mathbb{K}$ che fissano $\mathbb{K}$. Osserviamo che:

- L'identità è un elemento di G perché in particolare lascia fisso $\mathbb{K}$.
- Se σ e γ appartengono a G, allora la loro composizione è sempre un omomorfismo da $\mathbb{E}$ in $\mathbb{L}$ che lascia fisso $\mathbb{K}$ e quindi $(\sigma \circ \gamma) \in G$.
- Se $\sigma \in G$ allora σ è iniettivo, l'inverso è ancora un omomorfismo da $\mathbb{E}$ (perché sappiamo che $\sigma(\mathbb{E}) = \mathbb{E}$) in $\mathbb{L}$ (in quanto $\mathbb{E} \subseteq \mathbb{L}$) e naturalmente lascia fisso $\mathbb{K}$. Perciò $\sigma^{-1} \in G$.

Abbiamo dunque mostrato che $(G, \circ)$ è un gruppo.

Definizione 7.59. Il gruppo G degli omomorfismi da $\mathbb{E}$, estensione normale di $\mathbb{K}$, a $\mathbb{L}$, chiusura algebrica di $\mathbb{K}$, che lasciano fissi $\mathbb{K}$ è detto **gruppo di Galois** dell'estensione $\mathbb{E}$.

Osservazione 7.60. Dalla Proposizione 7.54 segue che l'ordine del gruppo di Galois dell'estensione $\mathbb{E}$ su $\mathbb{K}$ è uguale a $[\mathbb{E} : \mathbb{K}]$.

Studiamo alcune proprietà del gruppo di Galois, di estensioni normali $\mathbb{E}$ di un campo $\mathbb{K}$. In particolare, sapendo che un campo di spezzamento di un polinomio $f(x)$ irriducibile in $\mathbb{K}[x]$ è un'estensione normale, studiamo il gruppo di Galois di queste particolari estensioni algebriche di $\mathbb{K}$.

Consideriamo $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$ irriducibile e sia $\mathbb{E} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ il campo di spezzamento di $f(x)$. Vogliamo dare una stima superiore al grado di $\mathbb{E}$ su $\mathbb{K}$, in funzione del grado n di $f(x)$. Costruiamo una serie di estensioni "semplici" consecutive, aggiungendo una alla volta, le n radici distinte (ricordiamoci che siamo nell'ipotesi di separabilità) $\alpha_1, \ldots, \alpha_n$ di $f(x)$ in una chiusura algebrica $\overline{\mathbb{K}}$ di $\mathbb{K}$. Indichiamo dunque con $\mathbb{F}_0$ il campo $\mathbb{K}$, e con F_i il campo $\mathbb{K}(\alpha_1, \ldots, \alpha_i)$ (per ogni i naturale minore di n). In particolare $\mathbb{F}_n = \mathbb{E}$ e:

$$[\mathbb{E} : \mathbb{K}] = \prod_{i=1}^{n} [\mathbb{F}_i : \mathbb{F}_{i-1}]$$

Essendo $f(x)$ irriducibile in $\mathbb{K}[x]$, $\mathbb{K}(\alpha_1) \cong \mathbb{K}[x]/(f(x))$ e l'estensione $\mathbb{F}_1$ ha grado n su $\mathbb{K}$ (uguale al grado di $f(x)$ che è il polinomio minimo di α_1). In generale $\mathbb{F}_i = \mathbb{F}_{i-1}(\alpha_i)$, dunque $[\mathbb{F}_i : \mathbb{F}_{i-1}]$ è uguale al grado del polinomio minimo $h(x)$ di α_i su $\mathbb{F}_{i-1}$. Osserviamo che, la fattorizzazione di $f(x)$ in $\mathbb{F}_{i-1}[x]$ è:

$$f(x) = h_{i-1}(x) \underbrace{\prod_{j=0}^{i-1}(x - \alpha_j)}_{g(x)}$$

con $h_{i-1}(\alpha_i) = 0$ (α_i è una radice di $f(x)$ e non lo è di $g(x)$). Il polinomio minimo di α_i su $\mathbb{F}_{i-1}$ divide $h_{i-1}(x)$ e perciò ha grado minore o uguale di $deg(h_{i-1}(x))$ che è $n - (i-1)$. Abbiamo dunque mostrato che $[\mathbb{F}_i : \mathbb{F}_{i-1}] \leq n - (i-1)$ e perciò:

$$[\mathbb{E} : \mathbb{K}] = \prod_{i=1}^{n} [\mathbb{F}_i : \mathbb{F}_{i-1}] \leq n!$$

Conclusione: $n | [\mathbb{E} : \mathbb{K}] \leq n!$.

Teorema 7.61. *Sia $\mathbb{E} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ il campo di spezzamento di $f(x) \in \mathbb{K}[x]$ irriducibile. Allora il gruppo di Galois G di $\mathbb{E}$ su $\mathbb{K}$ è isomorfo ad un sottogruppo di $\mathcal{S}_n$, il gruppo delle permutazioni di n elementi.*

Dimostrazione. Dobbiamo mostrare che esiste un omomorfismo iniettivo da G a $\mathcal{S}_n$. Consideriamo un elemento $\sigma \in G$, sappiamo che σ sull'insieme delle radici di $f(x)$ agisce come una permutazione e quindi che per ogni $i \leq n$:

$$\sigma(\alpha_i) = \alpha_{\lambda(i)} \text{ con } \lambda \in \mathcal{S}_n.$$

Consideriamo l'applicazione che associa a $\sigma \in G$ la permutazione $\lambda \in \mathcal{S}_n$.

- Questa applicazione è un omomorfismo, infatti siano $\sigma, \tau \in G$ associate alle permutazioni λ, μ. Allora sappiamo che $\sigma \circ \tau$ è sempre un elemento di G, dobbiamo vedere che la permutazione ad esso associata sia $\lambda \circ \mu$:

$$\forall \alpha_i : \ \alpha_i \xrightarrow{\tau} \alpha_{\mu(i)} \xrightarrow{\sigma} \alpha_{\lambda(\mu(i))} = \alpha_{\lambda \circ \mu(i)}.$$

- L'omomorfismo è iniettivo, infatti il suo nucleo è composto dagli elementi del gruppo di Galois a cui è associata la permutazione identità dell'insieme delle radici di $f(x)$, cioè da omomorfismi che tengono fissi sia $\mathbb{K}$ che $\{\alpha_1, ..., \alpha_n\}$ e perciò tengono fisso tutto $\mathbb{E}$. L'unico omomorfismo da $\mathbb{E}$ in $\mathbb{L}$ che tiene fisso tutto $\mathbb{E}$ è l'omomorfismo identità.

□

Esempio 7.62 (Campi di spezzamento e gruppi di Galois associati)**.** Vediamo di descrivere in qualche caso particolare, di polinomi con grado basso, minore di 5, il campo di spezzamento e il gruppo di Galois. Indicheremo con $\alpha_1, ...\alpha_n$ le radici del polinomio $f(x) \in \mathbb{K}[x]$ in una chiusura algebrica di $\mathbb{K}$.

(1) Sia $f(x) = ax^2 + bx + c$ un polinomio di grado 2 (quindi $a \neq 0$) in $\mathbb{K}[x]$. $f(x)$ in $\mathbb{K}[x]$ può essere:
   - riducibile e allora:

$$f(x) = a(x - \alpha_1)(x - \alpha_2)$$

con $\alpha_1, \alpha_2 \in \mathbb{K}$ e quindi il campo di spezzamento è $\mathbb{K}(\alpha_1, \alpha_2) = \mathbb{K}$ mentre il gruppo di Galois è composto da quegli omomorfismi da $\mathbb{K}$

in $\mathbb{L}$ che tengono fisso $\mathbb{K}$. Ovvero il gruppo di Galois contiene solo l'omomorfismo identità;

- irriducibile, allora $\mathbb{E} = \mathbb{K}(\alpha_1, \alpha_2)$ con $\alpha_1, \alpha_2 \notin \mathbb{K}$. Sappiamo che il grado dell'estensione è multiplo di 2 e minore o uguale a 2! e quindi sarà 2, perciò abbiamo la seguente catena di estensioni con i rispettivi gradi delle estensioni:

$$\mathbb{K} \underbrace{\subseteq}_{2} \mathbb{K}(\alpha_1) \underbrace{\subseteq}_{1} \mathbb{K}(\alpha_1, \alpha_2) = \mathbb{E}.$$

Ovvero $\mathbb{E} = \mathbb{K}(\alpha_1)$, mentre il gruppo di Galois è composto da due elementi: l'identità e l'omomorfismo σ che scambia le radici di $f(x)$, ovvero:

$$\sigma(\alpha_1) = \alpha_2 \quad \sigma(\alpha_2) = \alpha_1.$$

(2) Sia $f(x) = x^3 + ax^2 + bx + c \in \mathbb{K}[x]$ [9] allora, come prima, $f(x)$ in $\mathbb{K}[x]$ può essere:

- riducibile e può essere riducibile in due modi diversi:
  - $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ con $\alpha_i \in \mathbb{K}$ per ogni i, e allora $\mathbb{E} = \mathbb{K}$ e il gruppo di Galois è banale.
  - $f(x) = (x-\alpha_1) \underbrace{(x^2 + dx + e)}_{g(x) \text{ irriducibile}}$ allora $\mathbb{K}(\alpha_1) = \mathbb{K}$ e quindi $\mathbb{E} = \mathbb{K}(\alpha_2, \alpha_3)$ con α_2, α_3 radici di $g(x)$. Il gruppo di Galois di $\mathbb{E}$ su $\mathbb{K}$ è come prima composto dall'identità e da σ che scambia α_2 con α_3, ovvero $G \cong \mathbb{Z}_2$;
- irriducibile e allora abbiamo la seguente catena di estensioni:

$$\mathbb{K} \underbrace{\subseteq}_{3} \mathbb{K}(\alpha_1) \subseteq \mathbb{K}(\alpha_1, \alpha_2) \subseteq \mathbb{K}(\alpha_1, \alpha_2\alpha_3) = \mathbb{E}$$

e sappiamo che $G < \mathcal{S}_3$ e che 3 divide l'ordine di G che a sua volta divide $3! = 6$. G ha quindi due possibilità, può essere tutto $\mathcal{S}_3$ oppure il sottogruppo ciclico di $\mathcal{S}_3$ di ordine 3, ovvero $G \cong \mathbb{Z}_3$ e composto dai tre cicli:

$$G = \{id, (1,2,3), (1,3,2)\}.$$ [10]

Vediamo un esempio numerico di questo tipo:

$$f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$$

Per il criterio di Ruffini non ha radici in $\mathbb{Q}$ e inoltre $f'(x) = 3x^2 + 1$ non ha radici reali e quindi $f(x)$ ha una sola radice reale α, e due radici complesse coniugate β e $\overline{\beta}$. Osserviamo che $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ e quindi $\mathbb{Q}(\alpha)$ è strettamente contenuto in $\mathbb{Q}(\alpha, \beta)$. Quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \neq 1$ perciò:

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] > 3$$

[9] La riducibilità di $f(x)$ non dipende dall'eventuale moltiplicazione per un elemento invertibile, quindi non è restrittivo supporre $f(x)$ monico.

[10] Abbiamo identificato, come faremo anche in seguito, la radice con l'indice per semplicità di notazione, cioè il ciclo $(1,2,3)$ corrisponde all'omomorfismo in G che manda α_1 in α_2, α_2 in α_3 e α_3 in α_1.

da cui:

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 6.$$

Quindi $G = \mathcal{S}_3$ ogni volta che il polinomio irriducibile in $\mathbb{Q}$ di terzo grado ha un'unica radice reale, infatti il ragionamento fatto funziona in generale.

Provare per esercizio che, nel caso in cui $f(x)$ abbia tre radici reali α, β, γ, il gruppo di Galois di $\mathbb{Q}(\alpha,\beta,\gamma)$ è $\mathbb{Z}_3$ se $(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 \in \mathbb{N}$ ed è un quadrato.

(3) Sia $f(x) \in \mathbb{K}[x]$ un polinomio di grado 4, ormai abbiamo capito che se $f(x)$ è riducibile in fattori lineari in $\mathbb{K}[x]$, ovvero se tutte le radici di $f(x)$ sono in $\mathbb{K}$, allora $\mathbb{K}$ è il campo di spezzamento di $f(x)$ e quindi il gruppo di Galois di $\mathbb{K}$ su $\mathbb{K}$ è banale.

Studiamo il caso in cui $f(x)$ è riducibile nel prodotto di due polinomi di grado 2 irriducibili in $\mathbb{K}[x]$:

$$f(x) = \underbrace{(x^2+ax+b)}_{g(x) \text{ irriducibile}} \cdot \underbrace{(x^2+cx+d)}_{h(x) \text{ irriducibile}}$$

Indichiamo con α_1, α_2 e β_1, β_2 le radici, rispettivamente di $g(x)$ e $h(x)$ in una chiusura algebrica $\mathbb{L}$. Sappiamo che:

$$\mathbb{K} \underbrace{\subseteq}_{2} \mathbb{K}(\alpha_1) \underbrace{\subseteq}_{1} \mathbb{K}(\alpha_1,\alpha_2)$$

mentre:

$$\mathbb{K} \underbrace{\subseteq}_{2} \mathbb{K}(\alpha_1) \underbrace{\subseteq}_{\leq 2} \mathbb{K}(\alpha_1,\beta_1) = \mathbb{E}$$

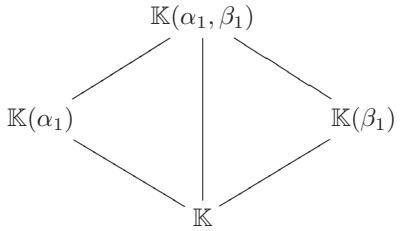
Bisogna quindi stabilire quando $\mathbb{K}(\alpha) = \mathbb{K}(\beta)$. Osserviamo che dalla formula risolutiva di secondo grado si ha che α e β sono radici quadrate (a meno di somma e moltiplicazione per elementi di $\mathbb{K}$) di elementi che non sono quadrati in $\mathbb{K}$ (ovvero di elementi $k \in K$ tali che $x^2 - k$ è irriducibile in $\mathbb{K}[x]$). Possiamo quindi porre $\alpha = \sqrt{k_1}$ e $\beta = \sqrt{k_2}$ con $k_1, k_2 \in \mathbb{K}$. Dobbiamo perciò stabilire quando $\mathbb{K}(\sqrt{k_1}) = \mathbb{K}(\sqrt{k_2})$. Questo accade (Esercizio 7.38) se e solo se $\dfrac{k_1}{k_2}$ è un quadrato in $\mathbb{K}$ (se e solo se $\sqrt{k_1} \cdot \sqrt{k_2} \in \mathbb{K}$). Ricapitolando:

- Se $\left(\dfrac{\alpha}{\beta}\right)^2$ è un quadrato in $\mathbb{K}$ allora il campo di spezzamento di $f(x)$ è $\mathbb{E} = \mathbb{K}(\alpha_1)$ di grado 2 su $\mathbb{K}$ e il gruppo di Galois è composto dall'omomorfismo identità e da σ tale che:

$$\sigma(\alpha_1) = \alpha_2 \quad \sigma(\alpha_2) = \alpha_1$$
$$\sigma(\beta_1) = \beta_2 \quad \sigma(\beta_2) = \beta_1$$

  Ovvero $G \cong \mathbb{Z}_2$.[11]
- Se $\mathbb{K}(\alpha_1) \subseteq \mathbb{K}(\alpha_1,\beta_1) = \mathbb{E}$ è un'estensione propria allora è di grado 2 e quindi $\mathbb{E}$ è di grado 4 su $\mathbb{K}$. Il seguente diagramma riassume come si può arrivare ad $\mathbb{E}$ tramite le estensioni intermedie:

[11] In G non ci possono essere le trasposizioni che scambiano tra loro due radici e lasciano fisse le altre due, perché essendo $\mathbb{K}(\alpha_1) = \mathbb{K}(\beta_1)$ si ha che $\alpha_1 = k \cdot \beta_1$ e quindi un elemento di G che "sposta" α_1 non può lasciare fisso β_1.



Il gruppo di Galois dell'estensione $\mathbb{E}$ è formato dall'omomorfismo identità, dalle due trasposizioni $(\alpha_1\ \alpha_2)$ e $(\beta_1\ \beta_2)$ e dalla loro composizione: $(\alpha_1\ \alpha_2)(\beta_1\ \beta_2)$, quindi:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

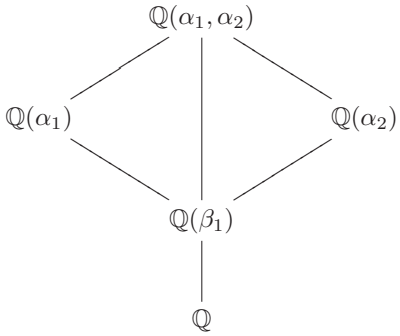
Consideriamo il polinomio $f(x) = x^4 - 6x^2 + 2 \in \mathbb{Q}[x]$. Per Eisenstein è irriducibile. Indichiamo con β_1, β_2 le radici di $y^2 - 6y + 2 \in \mathbb{Q}[y]$, ovvero $3 \pm \sqrt{7}$. Le radici del polinomio $f(x)$ sono $\alpha_1, -\alpha_1, \alpha_2, -\alpha_2$ con $\alpha_i^2 = \beta_i$. Sappiamo che il campo di spezzamento $\mathbb{E}$ su $\mathbb{Q}$ ha grado che è un multiplo di 4 ed è minore di $4! = 24$. Sappiamo anche che:

$$[\mathbb{Q}(\beta_1) : \mathbb{Q}] = 2$$

Inoltre:

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4.$$

Abbiamo cioè il seguente diagramma:



Dove conosciamo il grado dell'estensione fino a $\mathbb{Q}(\alpha_1)$ si tratta di capire il grado di $\mathbb{Q}(\alpha_1, \alpha_2)$ su $\mathbb{Q}(\alpha_1)$. Osserviamo che:

$$\alpha_1 = \sqrt{3 + \sqrt{7}} \quad \alpha_2 = \sqrt{3 - \sqrt{7}}$$

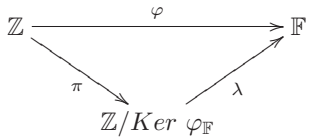
e che:

$$\alpha_1 \cdot \alpha_2 = \sqrt{2} \notin \mathbb{Q}(\beta).$$

Quindi $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] = 2$ e perciò $\mathbb{E}$ ha grado 8 su $\mathbb{Q}$ e il gruppo di Galois è il sottogruppo di $\mathcal{S}_4$ con 8 elementi composto dai 4 elementi che corrispondono al gruppo di Galois di $\mathbb{Q}(\alpha_1, \alpha_2)$ su $\mathbb{Q}(\beta_1)$ e che lasciano fisse β_1, β_2 e dalle quattro permutazioni analoghe che scambiano β_1 con β_2. Osserviamo che il gruppo di Galois è isomorfo a D_4, perché ogni sottogruppo di $\mathcal{S}_4$ con 8 elementi lo è.

5. Campi finiti

In questo paragrafo vogliamo caratterizzare i campi finiti: ovvero i campi con un numero finito di elementi. Abbiamo introdotto il concetto di caratteristica per gli anelli e visto esempi (gli $\mathbb{Z}/m\mathbb{Z}$) di anelli di caratteristica m per qualsiasi $m \in \mathbb{Z}$. Nel caso dei campi il cerchio delle possibili caratteristiche si restringe: sia infatti $\mathbb{F}$ un campo e consideriamo l'omomorfismo di anelli $\varphi_{\mathbb{F}} : \mathbb{Z} \longrightarrow \mathbb{F}$ definito da $\varphi_{\mathbb{F}}(1) = 1_{\mathbb{F}}$. Dal teorema di omomorfismo di anelli abbiamo il seguente diagramma:



dove λ è un omomorfismo iniettivo. Dunque $Ker\ \varphi_{\mathbb{F}}$ deve essere un ideale primo di $\mathbb{Z}$ (in quanto $\mathbb{F}$ che è un dominio d'integrità contiene un'immagine isomorfa di $\mathbb{Z}/Ker\ \varphi_{\mathbb{F}}$ che dunque è a sua volta un dominio d'integrità) ovvero $Ker\ \varphi_{\mathbb{F}}$ è uguale a $\{0\}$ oppure è della forma $p\mathbb{Z}$ con p primo. Nel primo caso $\mathbb{F}$ contiene un'immagine isomorfa di $\mathbb{Z}$, e quindi essendo un campo, un'immagine isomorfa di $\mathbb{Q}$ ed è dunque infinito, nel secondo caso $\mathbb{F}$ contiene un'immagine isomorfa di $\mathbb{Z}/p\mathbb{Z}$.

Dunque se $\mathbb{F}$ è un campo finito deve avere caratteristica p con p primo (il viceversa non lo possiamo affermare in quanto quello che abbiamo mostrato è che l'insieme dei campi di caratteristica 0 è contenuto nell'insieme dei campi infiniti), inoltre $\mathbb{F}$ contiene $\mathbb{Z}/p\mathbb{Z}$ e dunque può essere visto come spazio vettoriale di dimensione finita su $\mathbb{Z}/p\mathbb{Z}$. Se n è la dimensione di $\mathbb{F}$ su $\mathbb{Z}/p\mathbb{Z}$ e $\{f_1, \ldots, f_n\}$ una base di $\mathbb{F}$ su $\mathbb{Z}/p\mathbb{Z}$ allora, per definizione di base, gli elementi di $\mathbb{F}$ si scrivono in modo unico, al variare degli a_i in $\mathbb{Z}/p\mathbb{Z}$, come:

$$a_1 \cdot f_1 + \ldots + a_n \cdot f_n$$

E dunque $\mathbb{F}$ ha p^n elementi. Abbiamo quindi dimostrato il seguente teorema:

Teorema 7.63. *Se $\mathbb{F}$ è un campo finito allora ha caratteristica p, con p primo, ed ha cardinalità uguale a p^n per un certo $n \in \mathbb{N}$ positivo.*

In particolare dal Teorema 7.63 segue che non esistono campi con $p \cdot q$ elementi con p e q primi distinti: per esempio non esiste un campo con 14 elementi. Il seguente teorema caratterizza in maniera definitiva i campi finiti:

Teorema 7.64. *Per ogni primo p e ogni $n \in \mathbb{N}$ positivo esiste un campo finito con p^n elementi. Tale campo è unico fissata una chiusura algebrica di $\mathbb{Z}/p\mathbb{Z}$, e lo indicheremo con $\mathbb{F}_{p^n}$.*

Dimostrazione. Indichiamo con $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ il campo con p elementi e consideriamone una chiusura algebrica $\overline{\mathbb{F}_p}$. Sia F l'insieme delle radici del polinomio $x^{p^n} - x$ in $\overline{\mathbb{F}_p}$:

$$F = \{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^n} = \alpha\}$$

Osserviamo innanzitutto che il polinomio $f(x) = x^{p^n} - x$ ha derivata $f'(x) = p^n x^{p^n+1} - 1 = -1$ e dunque $(f(x), f'(x)) = 1$. Questo implica che $f(x)$ non ha fattori multipli e quindi ha p^n radici distinte in $\overline{\mathbb{F}_p}$ ovvero $|F| = p^n$.

Dimostriamo adesso che l'insieme F così definito è effettivamente un campo ovvero che se α, β sono elementi di F (ovvero $\alpha^{p^n} = \alpha$ e $\beta^{p^n} = \beta$) e α è diverso da zero allora $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$ e α^{-1} sono elementi di F.

- Dimostriamo per induzione su n che in un campo di caratteristica p (come $\overline{\mathbb{F}_p}$) se $\alpha^{p^n} = \alpha$ e $\beta^{p^n} = \beta$) allora $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$. Se $n = 1$ abbiamo che per la caratteristica del campo $(\alpha + \beta)^p$ è uguale ad $\alpha^p + \beta^p$ che per ipotesi è $\alpha + \beta$. Supponiamo vera la tesi per $n - 1$ e prendiamo in esame il caso $(\alpha + \beta)^{p^n}$:
$$(\alpha + \beta)^{p^n} = ((\alpha + \beta)^{p^{n-1}})^p = (\alpha + \beta)^p = \alpha + \beta$$
- $\alpha \cdot \beta)^{p^n}$ è uguale (essendo $\overline{\mathbb{F}_p}$ commutativo) ad $\alpha^{p^n} \cdot \beta^{p^n}$ che per ipotesi è uguale a $\alpha \cdot \beta$.
- $(-\alpha)^{p^n}$ è uguale a $(-1)^{p^n}\alpha^{p^n}$ che per ipotesi è $(-1)^{p^n}\alpha$. Ora se p è dispari otteniamo $-\alpha$ e se $p = 2$ allora $(-1)^{2^n} = 1$ ma $-\alpha = \alpha$.
- Se $\alpha \neq 0 \in \mathbb{F}$ allora
$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$$

Sia H un campo con p^n elementi contenuto in una fissata chiusura algebrica $\overline{\mathbb{F}_p}$ di $\mathbb{F}_p$, allora $|H^*| = p^n - 1$ e dunque ogni elemento di H diverso da 0 è radice del polinomio $x^{p^n-1} - 1$. Perciò ogni elemento di H è soluzione di $x^{p^n} - x = 0$ e quindi $H \supset F$. D'altro canto H e F devono avere lo stesso numero di elementi e di conseguenza devono essere uguali. □

Osservazione 7.65. Osserviamo che se con $\mathbb{F}_p$ indichiamo come detto $\mathbb{Z}/p\mathbb{Z}$, un $\mathbb{F}_{p^n}$ non sarà $\mathbb{Z}/p^n\mathbb{Z}$ (in quanto quest ultimo non è un campo) e, per la stessa ragione, nemmeno isomorfo come anello al prodotto diretto di n copie di $\mathbb{Z}/p\mathbb{Z}$ (i due insiemi sono però isomorfi come spazi vettoriali su $\mathbb{Z}/p\mathbb{Z}$).

$\mathbb{F}_{p^n}$ è il campo di spezzamento del polinomio $x^{p^n} - x$ su $\mathbb{Z}_p$ ($[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$), in particolare $\mathbb{F}/\mathbb{Z}_p$ è un'estensione normale e ne possiamo considerare il gruppo di Galois.

Teorema 7.66. *Il gruppo Galois*$(\mathbb{F}_{p^n}/\mathbb{F}_p) = G$ *è ciclico di grado* n *ed è generato dall'automorfismo di Frobenius:*[12]
$$\phi : \mathbb{F}_{p^n} \longrightarrow \overline{\mathbb{F}}_p$$
definito come segue:
$$\forall x \in \mathbb{F}_{p^n} : \phi(x) = x^p$$

Dimostrazione. Sappiamo che $|G| = n$, e innanzitutto osserviamo che l'automorfismo di Frobenius è un elemento di G, infatti per il teorema di Fermat, per ogni $\alpha \in \mathbb{F}_p$ si ha:
$$\phi(\alpha) = \alpha^p = \alpha.$$
Consideriamo $< \phi >= H < G$, e supponiamo che $ord(H) = ord(\phi)$ sia k, in particolare $k|n$:
$$\forall \alpha \in \mathbb{F}_{p^n} : \phi^k(\alpha) = \underbrace{(\phi \circ ... \circ \phi)}_{k \text{ volte}}(\alpha) = \alpha^{p^k} = \alpha.$$
Questo implica che ogni α in $\mathbb{F}_{p^n}$ è radice del polinomio:
$$x^{p^k} - x.$$

[12] Questo risultato insieme alla Proposizione 7.54 ci dice che per qualsiasi campo $\mathbb{K}$ di quelli da noi presi in considerazione (cioè con estensioni tutte separabili), se $\mathbb{E}$ è un'estensione normale di grado n allora: $n = |Gal(\mathbb{E}/\mathbb{K})|$.

Allora deve essere:

$$p^k \geq p^n \Leftrightarrow k \geq n$$

e quindi $k = n$. □

Il seguente teorema ci dice quando dati due campi finiti $\mathbb{F}_{p^m}$ e $\mathbb{F}_{p^n}$, con p primo, uno dei due è contenuto nell'altro:

Teorema 7.67. $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m|n$.

DIMOSTRAZIONE. $\Rightarrow$) Se $\mathbb{F}_{p^n}$ è un'estensione di $\mathbb{F}_{p^m}$ allora si può considerare la seguente catena di sottoestensioni:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$$

Dunque per la Proposizione 7.30:

$$\underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_{n} = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot \underbrace{[\mathbb{F}_{p^m} : \mathbb{F}_p]}_{m}$$

Da cui m divide n.
$\Leftarrow$) Dobbiamo mostrare che, se $n = m \cdot k$, l'insieme delle radici del polinomio $x^{p^m} - x$ è contenuto nell'insieme delle radici del polinomio $x^{p^n} - x$. Basta far vedere che (con l'ipotesi m divide n) $p^m - 1$ divide $p^n - 1$:

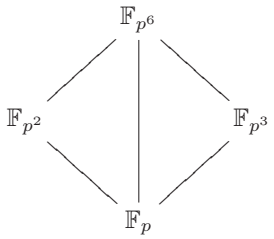
$$p^n - 1 = p^{m \cdot k} - 1 = (p^m)^k - 1^k$$

Chiamando $p^m = y$ scriviamo $p^n - 1$ come $y^k - 1$ che sappiamo fattorizzare in

$$(y-1) \cdot \sum_{i=0}^{k-1} y^i = (p^m - 1) \cdot \sum_{i=0}^{k-1} p^{i \cdot m}$$

□

Esempio 7.68. Mostriamo che esiste $\alpha \in \mathbb{F}_{p^6}$ tale che $\mathbb{F}_{p^6} = \mathbb{F}_p(\alpha)$. Per ogni $\alpha \in \mathbb{F}_p^6$ è evidente che $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^6}$. Consideriamo il seguente diagramma:



Osserviamo che:

- Gli α tali che $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$, cioè tali che $\alpha^{p^2} - \alpha = 0$ sono p^2.
- Gli α tali che $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^3}$, cioè tali che $\alpha^{p^3} - \alpha = 0$ sono p^3.

Allora:

$$|\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| = p^3 + p^2 - |\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}| = p^3 + p^2 - p < p^6.$$

Quindi esistono elementi che generano $\mathbb{F}_{p^6}$ (per il Teorema 7.67 non esistono altre sottoestensioni di $\mathbb{F}_{p^6}$ oltre a $\mathbb{F}_{p^2}$ e $\mathbb{F}_{p^3}$):

$$\mathbb{F}_{p^6} = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f(x)) \text{ con } f \text{ irriducibile e } deg(f(x)) = 6$$

Riassumiamo i risultati ottenuti sui campi finiti:

(1) I possibili ordini dei campi finiti sono tutti i p^n con p primo e n intero maggiore di zero. I campi finiti con p^n elementi hanno caratteristica p.
(2) Per ogni primo p e per ogni $n \geq 1$ esiste uno e un solo campo finito con p^n elementi che è il campo di spezzamento di $x^{p^n} - x \in \mathbb{Z}_p[x]$ (fissata una chiusura algebrica di $\mathbb{Z}_p$.)
(3) Il gruppo di Galois dell'estensione $\mathbb{F}_{p^n}/\mathbb{F}_p$ è ciclico di ordine n e generato dall'automorfismo di Frobenius: $\phi(x) = x^p$.

Abbiamo osservato anche (Teorema 7.67) che $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m|n$. Osserviamo che anche l'estensione $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ è normale, in quanto, se $\sigma : \mathbb{F}_{p^n} \longrightarrow \overline{\mathbb{F}}_p$ è un omomorfismo che, ristretto a $\mathbb{F}_{p^m}$, è l'identità. In particolare σ è iniettivo, e quindi $\sigma(\mathbb{F}_{p^n})$ è un campo con p^n elementi, contenuto nella stessa chiusura algebrica di $\mathbb{F}_p$. Ma l'unicità ricordata al punto 2 implica che $\sigma(\mathbb{F}_{p^n}) = \mathbb{F}_{p^n}$. Vogliamo studiare $G = Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$, dimostrando che è un sottogruppo di $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ e quindi che tutti gli omomorfismi σ in G saranno, per il punto 3, del tipo:

$$\sigma(x) = \phi^k(x) = x^{p^k}.$$

Sicuramente $\sigma = \phi^m \in G$ infatti:

$$\sigma(x) = \phi^m(x) = x^{p^m} \rightarrow \sigma|_{\mathbb{F}_{p^m}} = id.$$

Consideriamo $H =< \sigma >$ e supponiamo $ord(H) = ord(\sigma) = k$, allora:

$$\forall x \in \mathbb{F}_{p^n} : \ \sigma^{\frac{n}{m}}(x) = \phi^{m \cdot \frac{n}{m}}(x) = \phi^n(x) = x^{p^n} = x$$

e che, se $k < \dfrac{n}{m}$, $\sigma^k(x) = \phi^{m \cdot k}(x) = x^{p^{m \cdot k}}$. Non tutti gli elementi di $\mathbb{F}_{p^n}$ possono essere una radice del polinomio $x^{p^{m \cdot k}} - x$ (che ha grado $m \cdot k < n$), quindi $\sigma^k \neq id$ e l'ordine di σ è proprio $\dfrac{n}{m}$. Concludendo il gruppo di Galois di $\mathbb{F}_{p^{k \cdot m}}$ su $\mathbb{F}_{p^m}$ è ciclico di ordine k generato dall'automorfismo $\sigma(x) = x^{p^m}$.
Supponiamo $f(x) \in \mathbb{F}_p[x]$, fattorizziamo $f(x)$ in irriducibili di $\mathbb{F}_p[x]$:

$$f(x) = \prod_{i=1}^{k} f_i(x)$$

con f_i irriducibile di grado n_i. Sia α_1 una radice di $f_1(x)$, allora:

$$[\mathbb{F}_p(\alpha_1) : \mathbb{F}_p] = n_1 \Rightarrow \mathbb{F}_p(\alpha_1) = \mathbb{F}_{p^{n_1}}.$$

Le altre radici di $f_1(x)$ stanno in $\mathbb{F}_p(\alpha)$ in quanto ogni altra radice genera la stessa estensione (per l'unicità di un campo finito di cardinalità p^{n_1} fissata una chiusura algebrica). Il campo di spezzamento di $f(x)$ è quindi il più piccolo campo che contiene tutti i campi $\mathbb{F}_{p^{n_i}}$ con i che varia da 1 a k, ovvero è $\mathbb{F}_{p^m}$ con $m = [n_1, \ldots, n_k]$ e il gruppo di Galois di questa estensione sarà il gruppo ciclico di ordine m.

Proposizione 7.69. *Siano $\mathbb{K}$ un campo e G un sottogruppo finito di $\mathbb{K}^*$. Allora G è ciclico.*

Dimostrazione. $G < \mathbb{K}^*$ implica in particolare che G è abeliano. Supponiamo che:

$$|G| = n = \prod_{i=1}^{k} p_i^{a_i} \quad p_i \neq p_j \text{ se } i \neq j$$

allora esistono k sottogruppi H_i di cardinalità $p_i^{a_i}$ tali che:

$$G \cong H_1 \times \ldots \times H_k.$$

Osserviamo che G è ciclico se e solo se gli H_i sono ciclici. Infatti se G è ciclico, ogni suo sottogruppo è ciclico. Viceversa se gli H_i sono ciclici, allora avendo ordini primi tra loro, per il teorema cinese del resto, il loro prodotto diretto è ciclico.
Ci rimane quindi da dimostrare che $H < K^*$ tale che $|H| = p^a$ è ciclico. Sia $h \in H$, l'ordine di h sarà del tipo p^i con $i \leq a$. Per assurdo supponiamo che non esistono elementi di ordine p^a, allora:

$$\forall h \in H : \ h^{p^{a-1}} = 1$$

ma le radici in K^* del polinomio $x^{p^{a-1}} - 1$ sono minori o uguali del grado p^{a-1} del polinomio. Quindi non tutti gli elementi h di H soddisfano $h^{p^{a-1}} = 1$ e dunque H è ciclico. □

Questa proposizione è importante perché se ne deduce in particolare che $(\mathbb{F}_{p^n})^*$ è ciclico. Ovvero esiste α tale che $(\mathbb{F}_{p^n})^* =< \alpha >$.[13] Sia $f(x)$ il polinomio minimo di α ($f(x)$ è irriducibile) allora:

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f(x))$$

dove $deg(f(x)) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. In particolare possiamo concludere che per ogni n esistono polinomi irriducibili di grado n in $\mathbb{F}_p[x]$.
Gli elementi di $\mathbb{F}_{p^k}$ sono le radici di $x^{p^k} - x$, quindi quelli di $\mathbb{F}^*_{p^k}$ sono radici di $x^{p^{k-1}} - 1$ in particolare sono tutte radici dell'unità. Quindi è importante studiare il campo di spezzamento di $x^n - 1$ su $\mathbb{F}_p$ che è l'argomento del prossimo teorema:

Teorema 7.70. *Sia $n = p^a m$ con $(m, p) = 1$. Dimostrare che il campo di spezzamento di $x^n - 1$ su $\mathbb{F}_p$ è contenuto in $\mathbb{F}_{p^k}$ se e solo se $m | p^k - 1$.*

Dimostrazione. $\Rightarrow$) Il polinomio $x^n - 1$ lo possiamo scrivere:

$$x^{mp^a} - 1 = (x^m - 1)^{p^a}$$

in quanto $\mathbb{F}_p$ ha caratteristica p. Indichiamo con $g(x)$ il polinomio $x^m - 1$. Le m radici distinte di $g(x)$ stanno in $\mathbb{F}^*_{p^k}$, ovvero se C_m è l'insieme delle radici di $g(x)$ e indichiamo con $\overline{\mathbb{F}_p}$ una chiusura algebrica di $\mathbb{F}_p$:

$$C_m = \{\alpha \in \overline{\mathbb{F}_p} | \alpha^m = 1\} \subseteq \mathbb{F}^*_{p^k}$$

Poiché $C_m < \mathbb{F}^*_{p^k}$ e $|C_m| = m$, m divide l'ordine di $\mathbb{F}^*_{p^k}$, ovvero $p^k - 1$.
$\Leftarrow$) $\mathbb{F}^*_{p^k}$ ha un sottogruppo A di ordine m, quindi per ogni $a \in A$ $a^m = 1$ e dunque A è costituito dalle m radici di $x^m - 1$ ovvero $A = C_m$. Quindi $\mathbb{F}^*_{p^k}$ contiene il campo di spezzamento di $x^m - 1$ che abbiamo visto essere uguale a quello di $x^n - 1$. □

6. Teorema dell'elemento primitivo

Sia $\mathbb{K}$ un campo (ricordiamo che stiamo considerando campi $\mathbb{K}$ per cui tutte le estensioni sono separabili) e $\mathbb{E}/\mathbb{K}$ un'estensione finita. Vogliamo mostrare che allora $\mathbb{E}$ è un'estensione semplice, cioè esiste $\alpha \in \mathbb{E}$ tale che $\mathbb{E} = \mathbb{K}(\alpha)$. Il passo fondamentale per dimostrare questo importante teorema è il seguente lemma:

Lemma 7.71. *Se $\mathbb{E} = \mathbb{K}(\alpha, \beta)$ ($\mathbb{K}$ infinito), allora esiste $\gamma \in \mathbb{E}$ tale che: $\mathbb{E} = \mathbb{K}(\gamma)$.*

[13] E in particolare anche l'Esempio 7.68 poteva essere dimostrato usando questo risultato.

DIMOSTRAZIONE. Cerchiamo γ tra gli elementi della forma $\alpha + c\beta$ con $c \in \mathbb{K}$. Supponiamo $[\mathbb{E} : \mathbb{K}] = n$ e siano $\sigma_1, \ldots, \sigma_n$ gli n omomorfismi distinti (vedi Proposizione 7.54) da $\mathbb{E}$ in $\mathbb{L}$ (chiusura algebrica di $\mathbb{K}$) che ristretti a $\mathbb{K}$ sono l'identità. Consideriamo il polinomio $F(x) \in \mathbb{L}[x]$ così definito:

$$F(x) = \prod_{i<j} (\sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta)).$$

$F(x) \neq 0$ infatti i σ_i sono distinti e quindi devono dare immagini distinte a α o β (sugli elementi di $\mathbb{K}$ infatti sono l'identità) quindi $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ o $\sigma_i(\beta) \neq \sigma_j(\beta)$. Allora essendo $\mathbb{K}$ infinito esiste $c \in \mathbb{K}$ tale che $F(c) \neq 0$, ovvero per ogni i, j con $i < j$ si ha:

$$\sigma_i(\alpha + c\beta) = \sigma_i(\alpha) + \sigma_i(c\beta) = \sigma_i(\alpha) + c\sigma_i(\beta) \neq \sigma_j(\alpha + c\beta).$$

Consideriamo $\gamma = \alpha + c\beta$, per quanto appena osservato i $\sigma_1(\gamma), \ldots, \sigma_n(\gamma)$ sono tutti distinti, allora $\mathbb{K}(\gamma)$ ha n omomorfismi distinti a valori in $\mathbb{L}$ che lasciano fisso $\mathbb{K}$, quindi $[\mathbb{K}(\gamma) : \mathbb{K}] \geq n$. D'altra parte $\mathbb{K}(\gamma) \subseteq \mathbb{K}(\alpha, \beta)$, quindi $\mathbb{K}(\gamma) = \mathbb{K}(\alpha, \beta)$. □

Teorema 7.72 (Teorema dell'elemento primitivo)**.** *Sia $\mathbb{K}$ un campo (non importa se finito o di caratteristica 0), se $\mathbb{E}/\mathbb{K}$ è un'estensione finita allora esiste $\alpha \in \mathbb{E}$ tale che:*

$$\mathbb{E} = \mathbb{K}(\alpha).$$

DIMOSTRAZIONE. Dividiamo la dimostrazione in due parti, a seconda che il campo abbia caratteristica 0 o sia finito:

- $\mathbb{K}$ finito. Allora $|\mathbb{K}| = p^n$ per un certo n e se $[\mathbb{E} : \mathbb{K}] = m$ allora $|E| = p^{m \cdot n}$. $\mathbb{E}^*$ è ciclico per il Teorema 7.69 e quindi $\mathbb{E}^* =< \alpha >$, ovvero $\mathbb{E} = \mathbb{K}(\alpha)$.
- $char(\mathbb{K}) = 0$. Sia $\alpha_1, \ldots, \alpha_n$ una base di $\mathbb{E}$ su $\mathbb{K}$, ovvero $\mathbb{E} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$, allora abbiamo la seguente catena di estensioni:

  $$\mathbb{K} \subseteq \mathbb{K}(\alpha_1) \subseteq \mathbb{K}(\alpha_1, \alpha_2) \subseteq \ldots \subseteq \mathbb{K}(\alpha_1, \ldots, \alpha_n) = \mathbb{E}$$

  Si può procedere per induzione sul numero n di generatori dell'estensione. Il passo base $n = 2$ è assicurato dal Lemma 7.71. Per il passo induttivo consideriamo $\mathbb{E} = \mathbb{K}(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$:

  $$\mathbb{E} \underbrace{=}_{ip.ind.} \mathbb{K}(\gamma)(\alpha_n) = \mathbb{K}(\gamma, \alpha_n) \underbrace{=}_{lemma 7.71} \mathbb{K}(\lambda)$$

□

7. Corrispondenza di Galois

Se $\mathbb{E}$ è un'estensione normale di un campo $\mathbb{K}$, abbiamo definito il gruppo di Galois di $\mathbb{E}$ su $\mathbb{K}$. Come dimostreremo se $\mathbb{F} \subseteq \mathbb{E}$ è un'estensione di $\mathbb{K}$ in generale non è vero che sia un'estensione normale di $\mathbb{K}$, mentre $\mathbb{E}$ è un'estensione normale di $\mathbb{F}$ e quindi possiamo considerare $Gal(\mathbb{E}/\mathbb{F})$. In questo paragrafo vedremo che $Gal(\mathbb{E}/\mathbb{F})$ è un sottogruppo di $Gal(\mathbb{E}/\mathbb{K})$.

Proposizione 7.73. *Sia $\mathbb{E}$ un'estensione normale di un campo $\mathbb{K}$ e sia $\mathbb{F}$ un campo intermedio: $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$, allora:*

(1) *$\mathbb{E}/\mathbb{F}$ è un'estensione normale.*
(2) *$\mathbb{F}/\mathbb{K}$ in generale non è un'estensione normale.*

Dimostrazione. Indichiamo con $\mathbb{L}$ una chiusura algebrica di $\mathbb{K}$. Sappiamo per ipotesi che $\mathbb{E}/\mathbb{K}$ è un'estensione normale, e consideriamo gli omomorfismi $\sigma : \mathbb{E} \longrightarrow \mathbb{L}$ tali che $\sigma|_{\mathbb{F}} = id.$. In particolare σ lascia fisso $\mathbb{K}$ che è un sottocampo di $\mathbb{F}$. Allora $\sigma(\mathbb{E}) = \mathbb{E}$.
Consideriamo $x^3 - 2 \in \mathbb{Q}[x]$ e siano α, β, γ le tre radici in $\mathbb{C}$ di questo polinomio, con α che è l'unica radice reale. La seguente catena di estensioni:

$$\underbrace{\mathbb{Q}}_{\mathbb{K}} \subseteq \underbrace{\mathbb{Q}(\alpha)}_{\mathbb{F}} \subseteq \underbrace{\mathbb{Q}(\alpha, \beta, \gamma)}_{\mathbb{E}}$$

rispetta le ipotesi della proposizione, infatti $\mathbb{E}$ è il campo di spezzamento di un polinomio in $\mathbb{K}[x]$ e quindi è un'estensione normale di $\mathbb{K} = \mathbb{Q}$.
Consideriamo l'omomorfismo $\sigma : \mathbb{F} \longrightarrow \mathbb{Q}(\beta)$ che tiene fisso $\mathbb{Q}$ e tale che $\sigma(\alpha) = \beta$. Osserviamo che $\mathbb{F} = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, mentre $\beta \notin \mathbb{R}$ e quindi $\mathbb{Q}(\beta) \neq \mathbb{F}$ e $\mathbb{F}$ non è un'estensione normale di $\mathbb{Q}$. □

Proposizione 7.74. *Sia $\mathbb{E}/\mathbb{K}$ un'estensione normale finita e indichiamo con G il gruppo $Gal(\mathbb{E}/\mathbb{K})$. L'insieme:*

$$Fix(G) = \{x \in \mathbb{E} | \forall\ \sigma \in G :\ \sigma(x) = x\}$$

è uguale a $\mathbb{K}$.

Dimostrazione. È ovvio, per definizione, che $Fix(G) \subseteq \mathbb{E}$, mostriamo che è un campo.

- $0 \in Fix(G)$ infatti, per ogni omomorfismo $\sigma \in G$, $\sigma(0) = 0$.
- Se $x, y \in Fix(G)$, allora $\forall \sigma \in G$, $\sigma(x) = x$ e $\sigma(y) = y$, quindi:

  $$\sigma(x + y) = \sigma(x) + \sigma(y) = x + y \quad \sigma(x \cdot y) = \sigma(x) \cdot \sigma(y) = x \cdot y$$

- Per quanto riguarda l'opposto e l'inverso di un elemento di $Fix(G)$ si sfruttano le proprietà di un omomorfismo di campi.

Allora indichiamo con $\mathbb{F}$ il campo $Fix(G)$, per la Proposizione 7.73 $\mathbb{E}/\mathbb{F}$ è un'estensione normale, in particolare:

$$|Gal(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}] \text{ e } [\mathbb{E} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{K}] = [\mathbb{E} : \mathbb{K}]. \tag{7.1}$$

In $Gal(\mathbb{E}/\mathbb{F})$ ci stanno tutti gli omomorfismi da $\mathbb{E}$ in $\mathbb{L}$ che ristretti a $\mathbb{F}$ sono l'identità, quindi sicuramente ci stanno tutti gli omomorfismi in G, perché $\mathbb{F}$ è il campo fisso per G. Perciò $G \subseteq Gal(\mathbb{E}/\mathbb{F})$ e quindi $[\mathbb{E}/\mathbb{K}] \leq [\mathbb{E}/\mathbb{F}]$. Dalle condizioni 7.1 segue che:

$$[\mathbb{F} : \mathbb{K}] \leq 1 \Rightarrow [\mathbb{F}/\mathbb{K}] = 1 \Rightarrow \mathbb{F} = \mathbb{K}$$

□

Queste due proposizioni permettono, a partire da un'estensione normale $\mathbb{E}$ di un campo $\mathbb{K}$ di definire una corrispondenza biunivoca, detta **corrispondenza di Galois** tra campi intermedi $\mathbb{F}$, ovvero $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ e sottogruppi del gruppo $G = Gal(\mathbb{E}/\mathbb{K})$:

- Dato un campo $\mathbb{F}$ tale che $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$, la Proposizione 7.73 afferma che $\mathbb{E}/\mathbb{F}$ è un estensione normale e quindi possiamo considerarne il gruppo di Galois $H = Gal(\mathbb{E}/\mathbb{F})$, che ovviamente è contenuto in G. Quindi abbiamo un'applicazione λ che associa al campo intermedio $\mathbb{F}$ il sottogruppo di G dato da $Gal(\mathbb{E}/\mathbb{F})$.

- Dato un sottogruppo H di G possiamo considerare il campo degli elementi di $\mathbb{E}$ tenuti fissi da H. Per definizione questo campo (che sia un campo è assicurato dalla dimostrazione della Proposizione 7.74) è contenuto in $\mathbb{E}$ e contiene $\mathbb{K}$, in quanto ogni sottoinsieme di G lascia fissi tutti gli elementi di $\mathbb{K}$. Quindi abbiamo un'applicazione μ che associa ad un sottogruppo H di G il campo $Fix(H)$ che è un campo intermedio tra $\mathbb{E}$ e $\mathbb{K}$.

Proposizione 7.75. *Con le notazioni usate si ha che:*

$$\lambda \circ \mu = id_{\mathbb{E}} \quad \mu \circ \lambda = id_G$$

DIMOSTRAZIONE. Sia $\mathbb{F}$ un campo intermedio tra $\mathbb{E}$ e $\mathbb{K}$ e consideriamo $\mu \circ \lambda$:

$$\mathbb{F} \xrightarrow{\lambda} Gal(\mathbb{E}/\mathbb{F}) \xrightarrow{\mu} Fix(Gal(\mathbb{E}/\mathbb{F})) \underbrace{=}_{Proposizione 7.74} \mathbb{F}$$

Viceversa supponiamo H sia un sottogruppo di G e consideriamo $\lambda \circ \mu$:

$$H \xrightarrow{\mu} Fix(H) = \mathbb{F} \xrightarrow{\lambda} Gal(\mathbb{E}/\mathbb{F})$$

Ovviamente $H \subseteq Gal(\mathbb{E}/\mathbb{F})$, in quanto per definizione ogni elemento di H lascia fissi gli elementi di $\mathbb{F}$. Per far vedere che sono uguali, dimostreremo che i due sottogruppi hanno ordine uguale. Siano $n = ord(H)$ e $m = |Gal(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$, sappiamo che $n \leq m$. Per il teorema dell'elemento primitivo esiste $\alpha \in \mathbb{E}$ tale che: $\mathbb{E} = \mathbb{F}(\alpha)$ e indichiamo con σ_i con i che varia tra 1 e n, gli elementi di H (σ_1 sarà l'identità). Consideriamo il seguente polinomio in $\mathbb{E}[x]$:

$$f(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \sum_{i=0}^{n} a_i x^i \text{ con } a_n = 1.$$

Vogliamo dimostrare che i coefficienti di $f(x)$ sono in $\mathbb{F}$. Sia $\sigma \in H$ e consideriamo l'applicazione:

$$\tilde{\sigma} : \mathbb{E}[x] \longrightarrow \mathbb{E}[x] \quad \tilde{\sigma}(q(x)) = \sigma(q(x))$$

$\tilde{\sigma}$ è un isomorfismo e in particolare:

$$\tilde{\sigma}(f(x)) = \sum_{i=0}^{n} \sigma(a_i)x^i = \prod_{i=1}^{n}(x - \sigma(\sigma_i(\alpha)).$$

Osserviamo che $\sigma \in H$ e quindi $\sigma \circ \sigma_i$ è solo una permutazione degli elementi del gruppo, ovvero $\tilde{\sigma}(f(x)) = f(x)$. In particolare questo implica che:

$$\forall \sigma \in H : \ \sigma(a_i) = a_i \Rightarrow a_i \in Fix(H) = \mathbb{F} \Rightarrow f(x) \in \mathbb{F}[x].$$

Osserviamo che:

$$(x - \sigma_1(\alpha)) = (x - \alpha) \Rightarrow f(\alpha) = 0$$

quindi $f(x)$ è un polinomio in $\mathbb{F}[x]$ che si annulla in α, ovvero il polinomio minimo di α divide $f(x)$ e quindi il grado dell'estensione è minore o uguale a n, ovvero $m \leq n$. □

Proposizione 7.76. *Siano $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ tre campi, con $\mathbb{E}/\mathbb{K}$ estensione normale. Allora $\mathbb{F}/\mathbb{K}$ è un'estensione normale se e solo se $H = Gal(\mathbb{E}/\mathbb{F})$ è un sottogruppo normale di G.*

DIMOSTRAZIONE. Sia $\tau \in G$ e indichiamo con $\mathbb{F}'$ l'immagine di $\mathbb{F}$ tramite τ e con H' il corrispondente sottogruppo di G. Se $\sigma \in H$ (cioè lascia fisso $\mathbb{F}$) allora $\tau\sigma\tau^{-1} \in H'$, cioè lascia fisso $\mathbb{F}'$, infatti sia $x' \in \mathbb{F}'$, allora:

$$\underbrace{\tau\,\sigma\,\underbrace{\tau^{-1}(x')}_{\in\mathbb{F}}}_{\in\mathbb{F}} \Rightarrow \tau(\sigma\tau^{-1}(x')) = \tau\tau^{-1}(x') = x'.$$

Quindi $\tau H\tau^{-1} \subseteq H'$. Analogamente si dimostra che $H' \subseteq \tau H\tau^{-1}$, questo infatti è equivalente a dimostrare che $\tau^{-1}H'\tau \subseteq H$. Sia $\gamma \in H'$ e consideriamo $\tau^{-1}\gamma\tau$ e facciamo vedere che lascia fisso il campo $\mathbb{F}$. Sia dunque $x \in \mathbb{F}$, allora:

$$\underbrace{\tau^{-1}\,\gamma\,\underbrace{\tau(x)}_{\in\mathbb{F}'}}_{\in\mathbb{F}'} \Rightarrow \tau^{-1}(\gamma\tau(x)) = \tau^{-1}\tau(x) = x.$$

Abbiamo quindi dimostrato che:

$$H' = \tau H\tau^{-1}.$$

- $\Leftarrow$) Supponiamo che H sia un sottogruppo normale di G, per ogni $\tau \in G$:

$$H' = \tau H\tau^{-1} \underbrace{=}_{H\lhd G} H \Rightarrow \mathbb{F} = \mathbb{F}'.$$

- $\Rightarrow$) Supponiamo che per ogni $\tau \in G$ si abbia $\tau(\mathbb{F}) = \mathbb{F}$, allora $H' = H$ perché sono gli omomorfismi che lasciano fisso lo stesso campo. Quindi per ogni $\tau \in G$:

$$H = \tau H\tau^{-1}$$

cioè H è un sottogruppo normale di G.

□

Corollario 7.77. *Sia $\mathbb{E}/\mathbb{K}$ un'estensione normale e $\mathbb{F}$ un campo intermedio. Sia H il sottogruppo di $G = Gal(\mathbb{E}/\mathbb{K})$ associato a $\mathbb{F}$ tramite la corrispondenza di Galois. Se $\mathbb{F}/\mathbb{K}$ è normale allora:*

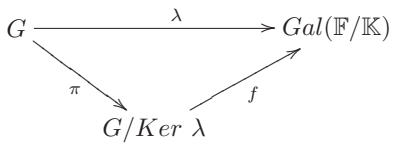
$$Gal(\mathbb{F}/\mathbb{K}) \cong G/H$$

$$\overbrace{\underbrace{\mathbb{E} - - -}_{H}\,\mathbb{F}\,\underbrace{- - -\mathbb{K}}_{G/H}}^{G}$$

DIMOSTRAZIONE. Consideriamo l'applicazione $\lambda : G \longrightarrow Gal(\mathbb{F}/\mathbb{K})$ definita da:

$$\forall\sigma \in G :\ \lambda(\sigma) = \sigma|_{\mathbb{F}}.$$

Osserviamo che l'applicazione è ben definita, in quanto per ipotesi $\mathbb{F}/\mathbb{K}$ è normale e quindi $\sigma(\mathbb{F}) = \mathbb{F}$. Inoltre λ è un omomorfismo surgettivo in quanto ogni omomorfismo $\sigma|_{\mathbb{F}}$ definito in $\mathbb{F}$ che lascia fisso $\mathbb{K}$ si può estendere a più omomorfismi $\sigma \in G$ (tanti quanto è il grado dell'estensione). Possiamo perciò considerare il seguente diagramma:



Sapendo che f è un isomorfismo tra $G/Ker\ \lambda$ e $Gal(\mathbb{F}/\mathbb{K})$. Ma quali sono gli elementi di G che stanno in $Ker\ \lambda$? Sono tutti gli omomorfismi che lasciano fissi tutti i punti di $\mathbb{F}$, ovvero tutti gli omomorfismi appartenenti ad H. □

Esempio 7.78. Consideriamo il polinomio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ e indichiamo con $\mathbb{E}$ il suo campo di spezzamento:

$$\mathbb{E} = \mathbb{Q}(\alpha, \beta, \gamma) \qquad \begin{matrix} \alpha = \sqrt[3]{2} \\ \beta = \sqrt[3]{2}\xi \\ \gamma = \sqrt[3]{2}\xi^2 \end{matrix}$$

dove ξ indica una radice cubica complessa dell'unità: $\xi = \frac{-1+i\sqrt{3}}{2}$ di polinomio minimo:

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

Quindi possiamo scrivere anche $\mathbb{E} = \mathbb{Q}(\alpha, \xi)$ ed essendo $\mathbb{E}$ il campo di spezzamento di un polinomio irriducibile di grado 3 ha gruppo di Galois che è isomorfo ad un sottogruppo di $\mathcal{S}_3$ e di ordine un multiplo di 3. Essendo il polinomio minimo di ξ di grado 2, il grado dell'estensione $\mathbb{E}$ è anche multiplo di 2 e quindi è uguale a 6, ovvero $G = Gal(\mathbb{E}/\mathbb{Q}) \cong \mathcal{S}_3$. Quali sono i sottogruppi di $\mathcal{S}_3$? Elenchiamoli:

(1) I gruppi banali: $\{e\}$ e G.
(2) Un gruppo generato dai 3-cicli: $H = \{id., (1\ 2\ 3), (1\ 3\ 2)\}$.
(3) Tre gruppi di ordine 2 generati da un trasposizione:

$$M_1 = \{id., (1\ 2)\};\ M_2 = \{id., (2\ 3)\};\ M_3 = \{id., (1\ 3)\}.$$

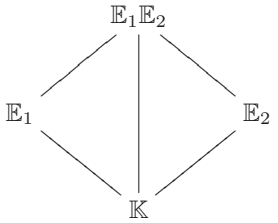
Cerchiamo di trovare a quali sottocampi di $\mathbb{E}$ sono associati questi gruppi:

- $\{e\}$ è associato al campo degli $x \in \mathbb{E}$ che vengono tenuti fissi da e, ovvero tutto $\mathbb{E}$.
- Il campo degli elementi lasciati fissi da tutto G è il campo $\mathbb{Q}$.
- M_1, M_2, M_3 lasciano fissi rispettivamente $\mathbb{Q}(\gamma)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$.
- Osserviamo che $|Gal(\mathbb{E}/\mathbb{Q}(\xi))| = 3 = |H|$, quindi ad H corrisponde $\mathbb{Q}(\xi)$.

Osserviamo che H è un sottogruppo normale di G (e quindi $H \cong A_3$) in quanto ha indice 2, e perciò $\mathbb{F}/\mathbb{K}$ è un'estensione normale. In generale tutte le estensioni di grado 2 sono dunque normali. In particolare sappiamo che:

$$Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \cong G/H \cong \mathcal{S}_3/A_3 \cong \mathbb{Z}_2$$

Osservazione 7.79. Consideriamo il seguente diagramma:



Se $\mathbb{E}_1/\mathbb{K}$ e $\mathbb{E}_2/\mathbb{K}$ sono estensioni normali (con gruppi di Galois G_1 e G_2), allora $\mathbb{E}_1\mathbb{E}_2/\mathbb{K}$ è un'estensione normale (il cui gruppo di Galois indicheremo con G), infatti consideriamo un omomorfismo σ da $\mathbb{E}_1\mathbb{E}_2$ in $\mathbb{L}$ (chiusura algebrica di $\mathbb{K}$) che lasci fisso $\mathbb{K}$. In particolare $\sigma(\mathbb{E}_1) = \mathbb{E}_1$ e $\sigma(\mathbb{E}_2) = \mathbb{E}_2$, quindi:

$$\sigma(\mathbb{E}_1\mathbb{E}_2) = \sigma(\mathbb{E}_1)\sigma(\mathbb{E}_2) = \mathbb{E}_1\mathbb{E}_2.$$

Proposizione 7.80. *La funzione $\lambda : G \longrightarrow G_1 \times G_2$ data da:*

$$\lambda(\sigma) = (\sigma|_{\mathbb{E}_1}, \sigma|_{\mathbb{E}_2})$$

è un omomorfismo iniettivo.

Dimostrazione. È ovvio che λ sia un omomorfismo.

$$Ker\ \lambda = \{\sigma \in G : \sigma|_{\mathbb{E}_1} = id.,\ \sigma|_{\mathbb{E}_2} = id.\}$$

$Fix(\sigma) \supseteq \mathbb{E}_1$ e $Fix(\sigma) \supseteq \mathbb{E}_2$ quindi:

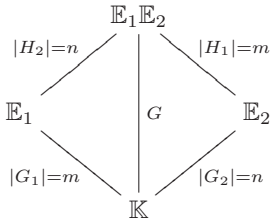
$$Fix(\sigma) \supseteq \mathbb{E}_1\mathbb{E}_2 \Rightarrow Fix(\sigma) = \mathbb{E}_1\mathbb{E}_2 \Rightarrow \sigma = id.$$

□

Nelle stesse ipotesi e usando le stesse notazioni della Proposizione 7.80 se indichiamo con n_i il grado dell'estensione $\mathbb{E}_i$ su $\mathbb{K}$ e supponiamo che

$$[\mathbb{E}_1\mathbb{E}_2 : \mathbb{K}] = [\mathbb{E}_1 : \mathbb{K}] \cdot [\mathbb{E}_2 : \mathbb{K}]^{14}$$

allora λ è anche surgettivo e quindi è un isomorfismo. Indichiamo con H_1, H_2 i sottogruppi di $G = Gal(\mathbb{E}_1\mathbb{E}_2/\mathbb{K})$ associati rispettivamente a $\mathbb{E}_1\mathbb{E}_2/\mathbb{E}_2$ ed $\mathbb{E}_1\mathbb{E}_2/\mathbb{E}_1$ e con G_1, G_2 quelli associati a $\mathbb{E}_1/\mathbb{K}$ e $\mathbb{E}_2/\mathbb{K}$. Abbiamo: $|H_1| = |G_1| = n_1$ e $|H_2| = |G_2| = n_2$. Ovvero si ha il seguente diagramma:



Consideriamo $\varphi : H_1 \longrightarrow G_1$ tale che:

$$\varphi(\sigma) = \sigma|_{\mathbb{E}_1}$$

[14] In particolare questo è vero se $(n_1, n_2) = 1$. Una condizione equivalente è che $\mathbb{E}_1 \cap \mathbb{E}_2 = \mathbb{K}$. Infatti l'immagine della restrizione di $Gal(\mathbb{E}_1\mathbb{E}_2/\mathbb{E}_2)$ a $Gal(\mathbb{E}_1/\mathbb{K})$ è $Gal(\mathbb{E}_1/\mathbb{E}_1 \cap \mathbb{E}_2)$ (basta vedere quale è il campo fisso) e dunque $[\mathbb{E}_1\mathbb{E}_2 : \mathbb{E}_2] = [\mathbb{E}_1 : \mathbb{K}]$ se e solo se $\mathbb{E}_1 \cap \mathbb{E}_2 = \mathbb{K}$.

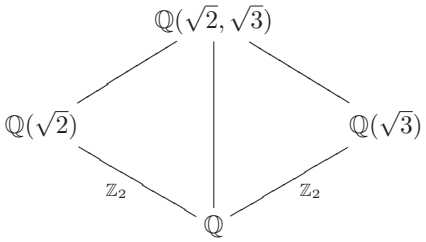
Allora φ è un omomorfismo iniettivo, infatti se $\sigma|_{\mathbb{E}_1} = id$ con $\sigma \in H_1$, per definizione di H_1 $\sigma|_{\mathbb{E}_2} = id$ e quindi $\sigma = id$ in $\mathbb{E}_1\mathbb{E}_2$. Questo, insieme alle considerazioni sulla cardinalità implica che:

$$H_i \cong G_i.$$

In particolare $H_1, H_2 \lhd G$ e $H_1 \cap H_2 = \{e\}$ (perché $\sigma \in H_1 \cap H_2$ lascia fisso sia $\mathbb{E}_1$ che $\mathbb{E}_2$ e quindi è l'identità) e $H_1H_2 = G$ (per questioni di cardinalità), quindi:

$$G \cong H_1 \times H_2$$

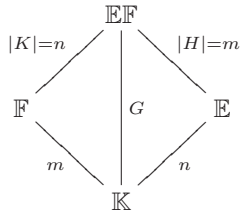
Esempio 7.81. Consideriamo l'estensione $\mathbb{E} = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ di $\mathbb{Q}$ (che è normale perché campo di spezzamento di $f(x) = (x^2 - 2) \cdot (x^2 - 3) \in \mathbb{Q}[x]$), allora possiamo considerare il seguente diagramma:



Allora osserviamo che $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ sono estensioni normali perché di grado 2 e quindi per le considerazioni fatte:

$$G = Gal(\mathbb{E}/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Osservazione 7.82. Consideriamo il seguente diagramma:



E supponiamo che $\mathbb{E}/\mathbb{K}$ sia un'estensione normale. Allora anche $\mathbb{EF}/\mathbb{F}$ è normale. Infatti $[\mathbb{E} : \mathbb{K}] = n$ quindi $\mathbb{E}$ è un'estensione finita di $\mathbb{K}$ e perciò per il teorema dell'elemento primitivo esiste α tale che $\mathbb{E} = \mathbb{K}(\alpha)$. Sia $f(x) \in \mathbb{K}[x]$ il polinomio minimo di α. $f(x)$ ha grado n e siano $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ le radici di $f(x)$. Essendo $\mathbb{E}/\mathbb{K}$ normale $\mathbb{E}$ deve contenere tutte le radici di $f(x)$. Dimostriamo che $\mathbb{EF} = \mathbb{F}(\alpha)$:

- $\mathbb{F}(\alpha) \supseteq \mathbb{F}$.
- $\mathbb{F}(\alpha) \supseteq \mathbb{E}$ che è il più piccolo campo contenente $\mathbb{K}$ e α.
- Viceversa $\mathbb{EF} \supseteq \mathbb{F}$ e $\alpha \in \mathbb{EF}$.

In particolare $\alpha_i \in \mathbb{EF}$ per ogni i, quindi $\mathbb{EF}$ è campo di spezzamento del polinomio $f(x) \in \mathbb{F}[x]$ e quindi è un'estensione normale di $\mathbb{F}$.
Supponiamo che $\mathbb{EF}/\mathbb{K}$ sia un'estensione normale, allora dalla Proposizione 7.76, segue che $H \lhd G = Gal(\mathbb{EF}/\mathbb{K})$. Sappiamo inoltre che $H \cap K = \{id\}$ in quanto

un omomorfismo appartenente a $H \cap K$ lascia fissi sia $\mathbb{F}$ che $\mathbb{E}$ e quindi lascia fisso tutto $\mathbb{EF}$. In questo caso $HK = G$ e quindi:

$$G \cong H \rtimes_{\varphi} K.$$

Esercizio 7.83. *Dimostrare che, se con ξ indichiamo la prima*[15] *radice n-esima complessa dell'unità diversa da 1 allora:*

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$$

dove ϕ è la funzione di Eulero.

Svolgimento. Innanzitutto osserviamo che l'insieme C_n delle radici complesse di $f(x) = x^n - 1$ è ciclico di ordine n generato da ξ ed è isomorfo come gruppo moltiplicativo a $\mathbb{Z}_n$ tramite l'isomorfismo ψ:

$$\psi(\xi^i) = i$$

e osserviamo che i è un generatore di $\mathbb{Z}_n$ se e solo se $(i, n) = 1$.
Indichiamo con d il grado dell'estensione $\mathbb{Q}(\xi)$ su $\mathbb{Q}$. Vogliamo dimostrare che $d = \phi(n)$. d è il grado del polinomio minimo $\mu(x) \in \mathbb{Q}[x]$ di ξ, in particolare $\mu(x)|f(x)$ quindi $f(x) = \mu(x)g(x)$ e, non avendo $f(x)$ radici in comune con la sua derivata nx^{n-1}, $\mu(x)$ e $g(x)$ sono primi tra loro.
Dimostriamo che l'estensione $\mathbb{Q}(\xi)$ di $\mathbb{Q}$ è normale, consideriamo gli omomorfismi da $\mathbb{Q}(\xi)$ in $\mathbb{C}$ che ristretti a $\mathbb{Q}$ sono l'identità. Allora ξ deve andare in una radice dell'unità ξ^i che abbia ordine n e quindi ci sono $\phi(n)$ possibili scelte. Dobbiamo mostrare che $\mu(x)$ ha come radici tutti gli elementi ξ^i con i primo con n. Basta vedere che tutti gli elementi del tipo ξ^p, con p primo e primo con n, sono radici di $\mu(x)$.
Supponiamo per assurdo che $\mu(\xi^p) \neq 0$, allora essendo ξ^p una radice dell'unità si ha

$$f(\xi^p) = \mu(\xi^p)g(\xi^p) = 0 \Rightarrow g(\xi^p) = 0.$$

Allora $g(x^p)$ ha ξ come radice, ovvero $\mu(x)$ divide $g(x^p)$:

$$g(x^p) = \mu(x)h(x).$$

Possiamo passare a considerare i polinomi in $\mathbb{Z}_p$ in quanto i polinomi considerati sono monici e $(p, n) = 1$ quindi si conserva il grado:

$$\overline{g(x^p)g(x)}^p = \overline{\mu(x)} \cdot \overline{h(x)}$$

Quindi:

$$\overline{\mu(x)}|\overline{g(x)}^p \Rightarrow (\overline{\mu(x)}, \overline{g(x)}) = \overline{\lambda(x)} \text{ e } deg(\overline{\lambda(x)}) \geq 1$$

Allora:

$$\overline{f(x)} = \overline{\mu(x)} \cdot \overline{g(x)} \Rightarrow \overline{\lambda(x)}^2 | \overline{f(x)} \Rightarrow \overline{\lambda(x)}|\overline{f'(x)} = \overline{n}x^{n-1} \neq 0.$$

Questo è assurdo, perché $\overline{f'(x)}$ avrebbe come unica radice 0, quindi 0 sarebbe anche radice di $\overline{\lambda(x)}$ e quindi anche di $\overline{f(x)}$, ma 0 non è radice di $\overline{f(x)}$.
Abbiamo quindi dimostrato che $\mathbb{Q}(\xi)/\mathbb{Q}$ è un'estensione normale e che ha ordine $\phi(n)$, in particolare se $(i, n) = 1$:

$$\sigma_i : \xi \longrightarrow \xi^i$$

e

$$\sigma_{ij}(\xi) = \sigma_i \circ \sigma_j(\xi) = \sigma_i(\xi^j) = \xi^{ij} = \xi^{\overline{ij}}$$

[15] Prima nel senso che ha argomento più piccolo delle altre radici.

dove $\overline{ij}$ indica la classe modulo n. Quindi:

$$Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}_n)^*$$

Esercizio 7.84. *Calcolare il grado del campo di spezzamento e il gruppo di Galois di x^4+1 su $\mathbb{Q}$.*

Svolgimento. Cerchiamo di applicare i risultati dell'esercizio precedente. Il polinomio x^4+1 moltiplicato per x^4-1 è uguale a x^8-1, quindi:

$$x^8-1 = (x^4+1)(x^2+1)(x-1)(x+1)$$

Se indichiamo con $\mathbb{K}$ il campo di spezzamento di x^4+1, abbiamo quindi le seguenti inclusioni tra campi:

$$\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{Q}(\xi_8)$$

Sappiamo che il polinomio minimo di ξ_8 (radice ottava dell'unità non reale) è di grado $\phi(8)=4$, quindi è x^4+1. Troviamo le radici di x^4+1 in $\mathbb{C}$:

$$x^4+1 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) \in \mathbb{C}[x]$$

Il campo di spezzamento di x^4+1 è quindi

$$\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

in particolare $\xi_8 \in \mathbb{K}$, dunque $\mathbb{K} = \mathbb{Q}(\xi_8)$ e ha grado 4 e gruppo di Galois isomorfo a $\mathbb{Z}_8^*$. (In particolare le radici di x^4+1 sono le radici ottave dell'unità che non sono radici quarte dell'unità.)
Si osservi che il polinomio x^4+1 , considerato come polinomio a coefficienti in F_p, è riducibile per ogni p. Infatti, se $p=2$ si ha $x^4+1=(x+1)^4$ e, se p è dispari, allora $8|p^2-1$ e dunque le radici ottave di 1 sono certamente contenute in F_{p^2}; ne segue che i fattori irriducibili di x^4+1 hanno grado al più 2.

Esercizio 7.85. *Sia $f(x)=(x^3+1)(x^3-5)$, determinare il grado del campo di spezzamento e il gruppo di Galois di $f(x)$ su $\mathbb{Q}$ e su $\mathbb{F}_7$.*

Svolgimento. Studiamo separatamente il campo di spezzamento e il gruppo di Galois di $f(x)$ su $\mathbb{Q}$ e su $\mathbb{F}_7$.
Per quanto riguarda $\mathbb{Q}[x]$, il fattore x^3+1 di $f(x)$ non è irriducibile in $\mathbb{Q}[x]$ infatti:

$$x^3+1 = (x-1)(x^2-x+1)$$

mentre il fattore x^3-5 per il criterio di Eisenstein è irriducibile, quindi la fattorizzazione in irriducibili di $f(x)$ è:

$$f(x) = (x-1)\underbrace{(x^2-x+1)}_{g(x)}\underbrace{(x^3-5)}_{h(x)}.$$

Il campo di spezzamento di questo polinomio deve contenere le radici di $g(x)$, ovvero:

$$x_{1,2} = \frac{1 \pm \sqrt{-3}}{2}$$

e quelle di $h(x)$, ovvero:

$$x_{3,4,5} = \sqrt[3]{5},\ \sqrt[3]{5}\xi_3,\ \sqrt[3]{5}\xi_3^2$$

dove ξ_3 è una radice terza dell'unità diversa da 1. Mentre la radice 1 del fattore $x-1$ è un elemento di $\mathbb{Q}$. In conclusione il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è il campo:

$$\mathbb{E} = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{5}, \xi_3).$$

Osserviamo però che una radice terza dell'unità è:

$$\xi_3 = \frac{-1 + i\sqrt{3}}{2}$$

ovvero $\mathbb{Q}(\xi_3) = \mathbb{Q}(i\sqrt{3})$ e quindi:

$$\mathbb{E} = \mathbb{Q}(\xi_3, \sqrt[3]{5}).$$

Sappiamo che il polinomio minimo di $\sqrt[3]{5}$ su $\mathbb{Q}$ ha grado 3, mentre il polinomio minimo di ξ_3 su $\mathbb{Q}$ è $x^2 + x + 1$, ovvero ha grado 2, quindi $\mathbb{Q}(\xi)$ non può essere un campo intermedio tra $\mathbb{Q}$ e $\mathbb{Q}(\sqrt[3]{5})$, ovvero l'estensione $\mathbb{Q}(\sqrt[3]{5}, \xi_3)/\mathbb{Q}(\sqrt[3]{5})$ non è banale. Dunque:

$$[\mathbb{Q}(\sqrt[3]{5}, \xi_3) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{5}, \xi_3) : \mathbb{Q}(\sqrt[3]{5})]}_{2} \cdot \underbrace{[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]}_{3} = 6$$

Basta osservare che G è isomorfo ad un sottogruppo di $\mathcal{S}_3$, in quanto permuta le radici di $x^3 - 5$, ed ha 6 elementi, quindi $G = \mathcal{S}_3$.
Altrimenti potevamo procedere osservando che il sottogruppo

$$H = Gal(\mathbb{Q}(\sqrt[3]{5}, \xi_3) : \mathbb{Q}(\xi_3)]$$

del gruppo di Galois $G = Gal(\mathbb{Q}(\sqrt[3]{5}, \xi_3)$ è normale (perché $\mathbb{Q}(\xi_3)/\mathbb{Q}$ è un'estensione di grado 2 e quindi normale), ed essendo un gruppo di ordine 3 (un primo) è ciclico e dunque isomorfo a $\mathbb{Z}_3$. Osserviamo che $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ non è un'estensione normale perché:

$$\mathbb{Q}(\sqrt[3]{5}) \neq \mathbb{Q}(\sqrt[3]{5}\xi_3) \text{ e } \mathbb{Q}(\sqrt[3]{5}) \neq \mathbb{Q}(\sqrt[3]{5}\xi_3^2)$$

in quanto $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$, mentre gli altri due campi non sono contenuti nei reali. Possiamo quindi concludere che:

$$G \cong \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$$

con $\varphi : \mathbb{Z}_2 \longrightarrow Aut(\mathbb{Z}_3)$. Gli automorfismi associati a $\mathbb{Z}_2$ sono l'identità e l'automorfismo che associa ad a il suo inverso a^{-1}.
Per quanto riguarda $\mathbb{F}_7$, calcoliamoci i cubi degli elementi di $\mathbb{F}_7$:

$$\begin{cases} 1^3 = 1 \\ 2^3 = 1 \\ 3^3 = 6 \\ 4^3 = 1 \\ 5^3 = 6 \\ 6^3 = 6 \end{cases}$$

Quindi in $\mathbb{F}_7$ $f(x)$ può essere fattorizzato come segue:

$$f(x) = (x-3)(x-5)(x-6)(x^3-5)$$

con $x^3 - 5$ che è irriducibile in $\mathbb{F}_7$ in quanto come abbiamo visto nessun elemento al cubo è uguale a 5. Perciò il campo di spezzamento di $f(x)$ in $\mathbb{F}_7$ ha grado 3, ovvero è uguale a $\mathbb{F}_{7^3}$ e il gruppo di Galois, ha ordine 3, e quindi è ciclico e isomorfo a $\mathbb{Z}_3$.

Esercizio 7.86. *Trovare il campo di spezzamento $\mathbb{K}$ su $\mathbb{Q}$ del polinomio:*

$$f(x) = x^7 - 5$$

e il gruppo di Galois di $\mathbb{K}/\mathbb{Q}$.

Svolgimento. $f(x)$, per il criterio di Eisenstein, è irriducibile, in particolare se indichiamo con d il grado dell'estensione $\mathbb{K}$ su $\mathbb{Q}$, sappiamo che $7|d$ e $d|7!$. Osserviamo che se ξ_7 è una radice settima dell'unità primitiva (cioè che genera il gruppo ciclico delle radici settime dell'unità), allora al campo di spezzamento $\mathbb{K}$ appartengono sia $\xi_7^i \sqrt[7]{5}$ (per ogni i: $0 \leq i \leq 6$) che $\sqrt[7]{5}$, e quindi anche $\xi_7 \in \mathbb{K}$ (è il rapporto tra $\xi_7 \sqrt[7]{5}$ e $\sqrt[7]{5}$). In particolare:

$$\mathbb{K} = \mathbb{Q}(\sqrt[7]{5}, \xi_7)$$

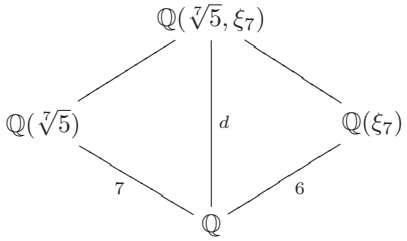
Osserviamo che il polinomio minimo di ξ_7 su $\mathbb{Q}$ è:

$$g(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

mentre il polinomio minimo di $\sqrt[7]{5}$ su $\mathbb{Q}$ è, in quanto abbiamo osservato essere irriducibile, $f(x)$. Allora:

$$[\mathbb{Q}(\sqrt[7]{5}, \xi_7) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[7]{5}, \xi_7) : \mathbb{Q}(\sqrt[7]{5})]}_{\leq 6} \cdot \underbrace{[\mathbb{Q}(\sqrt[7]{5}) : \mathbb{Q}]}_{=7} \leq 7 \cdot 6$$

Possiamo quindi considerare il seguente diagramma:



In particolare:

$$\begin{cases} d \equiv 0 \ (6) \\ d \equiv 0 \ (7) \end{cases} \Rightarrow d \equiv 0 \ (42) \Rightarrow d = 42$$

Quindi il polinomio minimo di ξ_7 su $\mathbb{Q}(\sqrt[7]{5})$ è sempre $g(x)$.
Cerchiamo ora di descrivere il gruppo $G = Gal(\mathbb{K}/\mathbb{Q})$. Sia $\varphi \in G$ allora φ deve tenere fisso $\mathbb{Q}$ e mandare $\sqrt[7]{5}$ e ξ_7 in radici del loro polinomio minimo, ovvero:

$$\varphi(\sqrt[7]{5}) \in \{\xi_7^i \sqrt[7]{5} | 0 \leq i \leq 6\} \quad \varphi(\xi_7) \in \{\xi_7^j | 0 < j \leq 6 \ (j, 7) = 1^{16}\}$$

Ci chiediamo se possiamo trovare dei generatori di G, l'idea, dopo aver descritto un generico elemento di G, è quella di considerare gli omomorfismi che muovono ξ_7 e lasciano fisso $\sqrt[7]{5}$ e viceversa quelli che muovono $\sqrt[7]{5}$ e lasciano fisso ξ_7. Consideriamo:

$$\sigma_j \in G : \begin{cases} \sigma_j(\sqrt[7]{5}) = \xi_7^j \sqrt[7]{5} \\ \sigma(\xi_7) = \xi_7 \end{cases}$$

Di σ_j distinti ce ne sono 7, al variare di j tra 0 e 6, infatti se $j > 7$ allora $j = 7q + r$ con $0 \leq r < 6$ e:

$$\xi_7^j = \xi_7^{7q+r} = \xi_7^r$$

[16] In questo caso è superflua la richiesta perché tutti i numeri minori di un numero primo p, maggiori di zero, sono primi con p. Ma se ξ_n è una radice n-esima dell'unità, con n non primo, allora vogliamo che l'immagine di ξ_n tramite φ vada ancora in un generatore del gruppo moltiplicativo delle radici n-esime dell'unità.

In particolare $\sigma_j = \sigma_1^j$ infatti:

$$\begin{cases} \sigma_1^2(\sqrt[7]{5}) = \sigma_1(\sigma_1(\sqrt[7]{5})) = \sigma_1(\xi_7\sqrt[7]{5}) = \xi_7^2\sqrt[7]{5} \\ \sigma_1^j(\sqrt[7]{5}) = \sigma_1(\sigma_1^{j-1}(\sqrt[7]{5})) \underbrace{=}_{ip.ind.} \sigma_1(\xi_7^{j-1}\sqrt[7]{5}) = \xi_7^j\sqrt[7]{5} \end{cases}$$

Consideriamo inoltre gli omomorfismi che muovono ξ_7 e lasciano fisso $\sqrt[7]{5}$:

$$\tau_j \in G : \begin{cases} \tau_j(\sqrt[7]{5}) = \sqrt[7]{5} \\ \tau_j(\xi_7) = \xi_7^j \end{cases}$$

Gli omomorfismi τ_j distinti sono $\phi(7)$. Mostriamo che il generico $\varphi \in G$ appartiene a $< \sigma_1, \tau_1, ..., \tau_6 >$ e quindi che $\sigma_1, \tau_1, ..., \tau_6$ generano G:

$$\begin{cases} \varphi(\sqrt[7]{5}) = \xi_7^k\sqrt[7]{5} \\ \varphi(\xi_7) = \xi_7^h \end{cases} \Rightarrow \varphi = \sigma_k \circ \tau_h$$

Indichiamo con H il sottogruppo di G generato da $< \sigma >$ e con K il sottogruppo composto dagli omomorfismi τ_j. Allora, per questioni di ordine:

$$H \cap K = \{id\} \text{ e } HK = G$$

Dimostriamo che H è normale. Facciamo vedere che H è caratteristico in G: se ci fosse H' diverso da H e di ordine 7, si avrebbe:

$$|HH'| = \frac{|H| \cdot |H'|}{|H \cap H'|} = \frac{7 \cdot 7}{1} = 49$$

ma questo è assurdo perché $HH' \subseteq G$ che sappiamo avere 42 elementi.
Possiamo quindi concludere che:

$$G \cong H \rtimes_\varphi K \cong \mathbb{Z}_7 \rtimes_\varphi (\mathbb{Z}_7)^*$$

dove $\varphi : K \longrightarrow Aut(H)$ è definito da:

$$(\varphi(\tau_j))(\sigma_1) = \tau_j \circ \sigma_1 \circ \tau_j^{-1} = \sigma_1^j$$

Esercizio 7.87. *Sia $\mathbb{E} = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$, con p_i primi distinti.*

(1) *Calcolare $[\mathbb{E} : \mathbb{Q}]$.*
(2) *Dimostrare che $\mathbb{E}/\mathbb{Q}$ è normale.*
(3) *Descrivere $Gal(\mathbb{E}/\mathbb{Q})$.*

Svolgimento. Rispondiamo per ultimo alla prima domanda, infatti dimostreremo che il gruppo di Galois di $\mathbb{E}/\mathbb{Q}$ è isomorfo a $(\mathbb{Z}_2)^n$ e quindi che:

$$[\mathbb{E} : \mathbb{Q}] = 2^n$$

Innanzitutto osserviamo che $\mathbb{E}$ è normale in quanto campo di spezzamento su $\mathbb{Q}$ del polinomio

$$(x^2 - p_1) \cdot \ldots \cdot (x^2 - p_n)$$

Dimostriamo per induzione che:

$$Gal(\mathbb{E}/\mathbb{Q}) \cong (\mathbb{Z}_2)^n$$

- Se $n = 1$, $\mathbb{E}$ è un'estensione di grado 2 (le due radici del polinomio $x^2 - p$ generano la stessa estensione su $\mathbb{Q}$).

- Consideriamo $\mathbb{K} = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, per ipotesi induttiva:
$$\mathbb{K} \cong (\mathbb{Z}_2)^{n-1}$$
Consideriamo $\mathbb{F} = \mathbb{Q}(\sqrt{p_n})$, allora $Gal(\mathbb{F}/\mathbb{Q}) \cong \mathbb{Z}_2$:
$$\mathbb{F} \cap \mathbb{K} = \begin{matrix} \mathbb{Q} \\ \mathbb{Q}(\sqrt{p_n}) \end{matrix}$$
Vogliamo dimostrare che l'intersezione tra $\mathbb{K}$ e $\mathbb{F}$ è sempre $\mathbb{Q}$. In questo caso:
$$Gal(\underbrace{\mathbb{F}\mathbb{K}}_{=\mathbb{E}}/\mathbb{Q}) \cong Gal(\mathbb{F}/\mathbb{Q}) \times Gal(\mathbb{K}/\mathbb{Q}) \cong (\mathbb{Z}_2)^n$$
Osserviamo che $\mathbb{K} \cap \mathbb{F} = \mathbb{Q}(\sqrt{p_n})$ se e solo se
$$\sqrt{p_n} \in \mathbb{K} \Leftrightarrow \mathbb{Q}(\sqrt{p_n}) \subseteq \mathbb{K}$$
Per la corrispondenza di Galois, sappiamo che il numero di sottoestensioni di $\mathbb{K}$ di grado 2 su $\mathbb{Q}$ è uguale al numero di sottogruppi di indice 2 di $(\mathbb{Z}_2)^{n-1}$. Ma essendo quest'ultimo un gruppo abeliano, ogni gruppo di indice due ne individua uno di ordine 2. In conclusione le possibili sottoestensioni di $\mathbb{K}$ di grado 2 su $\mathbb{Q}$ sono tante quante i sottogruppi di ordine 2 di $(\mathbb{Z}_2)^{n-1}$, ovvero $2^{n-1} - 1$.[17]
Osserviamo che scegliendo $i_1, \ldots, i_k$ distinti nell'insieme dei primi $n-1$ numeri si ha che:
$$\mathbb{Q}(\sqrt{p_{i_1}} \cdot \ldots \cdot \sqrt{p_{i_k}})$$
è una sottoestensione di $\mathbb{K}$ di grado 2 su $\mathbb{Q}$. Inoltre scelte diverse degli indici danno luogo ad estensioni distinte infatti siano $i_1, \ldots, i_k$ e $j_1, \ldots, j_t$ due scelte diverse, allora per il teorema di fattorizzazione non esiste nessun quadrato $a \in \mathbb{Q}$ tale che:
$$p_{i_1} \cdot \ldots \cdot p_{i_k} = a \cdot p_{j_1} \cdot \ldots \cdot p_{j_t}$$
e quindi per l'Esercizio 7.38:
$$\mathbb{Q}(\sqrt{p_{i_1}} \cdot \ldots \cdot \sqrt{p_{i_k}}) \neq \mathbb{Q}(\sqrt{p_{j_1}} \cdot \ldots \cdot \sqrt{p_{j_t}})$$
Quante sono le possibili scelte degli indici? Sono tutti i possibili sottoinsiemi dei primi $n-1$ elementi, ovvero 2^{n-1}. Cioè in questo modo abbiamo elencato tutte le possibili sottoestensioni di $\mathbb{K}$ di grado 2 su $\mathbb{Q}$. Quindi per avere che $\mathbb{F} \cap \mathbb{K} = \mathbb{Q}(\sqrt{p_n})$ deve essere:
$$\mathbb{Q}(\sqrt{p_n}) = \mathbb{Q}(\sqrt{p_{i_1}} \cdot \ldots \cdot \sqrt{p_{i_k}})$$
per qualche scelta di $i_1, \ldots, i_k$ in $\{1, \ldots, n-1\}$. Ma questo è impossibile sempre per l'Esercizio 7.38.

[17] Tutti gli elementi tranne l'identità hanno ordine 2 e quindi generano un sottogruppo di ordine 2.

Indice analitico

Finito di stampare nel mese di febbraio 2015
da Tipografia Monteserra S.n.c. - Vicopisano
per conto di Pisa University Press