Teoremi e Lemmi (e anche qualche Esercizio) per il corso di Aritmetica
A.A. 2015/2016
Prof. Giovanni Gaiffi, Massimo Caboara

mattiapuddu@icloud.com

Teoremi fatti a lezione

1. Sia $(G, \star)$ un gruppo. Allora:

   - $\exists!\ e \in G \mid \forall g \in G \ \ g \star e = e \star g = g$;
   - $\forall g \in G\ \exists! g^{-1} \in G \mid g \star g^{-1} = g^{-1} \star g = e$;
   - $\forall g \in G\ (g^{-1})^{-1} = g$;
   - $\forall a, b \in G\ (a \star b)^{-1} = b^{-1} \star a^{-1}$.

   Dimostrazione $(\star)$

   Supponiamo che ci siano due elementi neutri, siano essi e, e'. Allora si avrebbe

   $$e = e \star e' = e',$$

   dove la prima uguaglianza è dovuta al fatto che e' è un elemento neutro, la seconda è dovuta al fatto che e è un elemento neutro.

   Supponiamo che per un elemento $x \in G$ ci siano due elementi inversi, siano essi y, y'. Allora si avrebbe

   $$y' = e \star y' = y \star x \star y' = y \star e = y,$$

   dove la seconda uguaglianza è dovuta al fatto che y è un inverso, la terza è dovuta al fatto che y' è un elemento inverso.

   Il terzo punto è evidente: abbiamo infatti che

   $$a \star a^{-1} = e,$$

   dunque un inverso di a^{-1} è a. Dato che l'inverso è unico abbiamo la tesi.

   E' una semplice verifica:

   $$(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} = a \star a^{-1} = e.$$

2. $(Z(G), \star) < (G, \star)$.

   Dimostrazione $(\star)$

   Basta verificare le condizioni che servono per essere un sottogruppo:

   • $e \in Z(G)$ perché $\forall g \in G \;\; g \star e = e \star g = g$;

   • $a, b \in G \Rightarrow \forall g \in G \; (a \star b) \star g = a \star (b \star g) = a \star (g \star b) = (a \star g) \star b = (g \star a) \star b = g \star (a \star b)$;

   • $a \in G \Rightarrow \forall g \in G \;\; g \star a = a \star g \Rightarrow a^{-1} \star g \star a = a^{-1} \star a \star g \Rightarrow a^{-1} \star g \star a = e \star g = g \Rightarrow\Rightarrow a^{-1} \star g \star a \star a^{-1} = g \star a^{-1} \Rightarrow a^{-1} \star g \star e = a^{-1} \star g = g \star a^{-1}$.

3. Sia $(G, \star)$ un gruppo e sia $a \in G$. Allora $((a), \star) < (G, \star)$.

   Dimostrazione $(\star)$
   Basta verificare le condizioni che servono per essere un sottogruppo:

   • $e \in (a)$: infatti per $i = 0$ si ha $a^0 = e$ per definizione;

   • $b, c \in G \Rightarrow \exists m, n \in \mathbb{N} \mid b = a^m, c = a^n \Rightarrow b \star c = a^m \star a^n = a^{m+n}$;

   • $b \in G \Rightarrow \exists m \in \mathbb{N} \mid b = a^m \Rightarrow b^{-1} = (a^m)^{-1} = a^{-m}$.

4. Sia $(G, \star)$ un gruppo e sia $(H, \star) < (G, \star)$. Allora ogni elemento $w \in G$ è contenuto in uno e un solo $H-$laterale destro: $w \star H$.

   Dimostrazione $(\star)$

   Si ha che $w \in w \star H$: infatti $e \in H$ e $w = w \star e \in w \star H$. Supponiamo che esista una seconda classe laterale $\gamma \star H$ a cui w appartiene: allora $\exists x \in H \mid w = \gamma \star x$. Ma allora

   $$\gamma \star H = \{\gamma \star h \in G \mid h \in H\} = \{\gamma \star (x \star \bar{h}) \in G \mid \bar{h} \in H\} = \{(\gamma \star x) \star \bar{h} \in G \mid \bar{h} \in H\} =$$

   $$= \{w \star \bar{h} \in G \mid \bar{h} \in H\} = w \star H.$$

5. Siano $(G, \star)$ un gruppo, $(H, \star) < (G, \star)$, $g, h \in G$. Allora dati i laterali $g \star H, h \star H$, essi coincidono se e solo se $h \in g \star H$.

   Dimostrazione $(\star)$

   $\Rightarrow$ Immediato.

   $\Leftarrow$ Se avessimo che $h \in g \star H$ avremmo che h apparterrebbe alle due classi laterali $g \star H$ e $h \star H$. Poiché per il teorema precedente un elemento non può appartenere a due classi laterali distinte, ne consegue che le due classi laterali devono essere uguali.

6. **(Teorema di Lagrange)** Sia $(G, \star)$ un gruppo, e $(H, \star) < (G, \star)$. Se G è un gruppo finito, allora $|H| \mid |G|$.

   Dimostrazione $(\star\star)$

   Poiché G è un gruppo finito si può individuare una partizione in $H-$laterali destri, siano essi μ. Se ogni laterale avesse come cardinalità proprio $|H|$ si avrebbe che $|G| = \mu|H|$, da cui la tesi. Abbiamo che ogni elemento di una classe laterale $x \star H$ è della forma $x \star h$, con $h \in H$. Si ha che esiste una corrispondenza biunivoca fra H e una classe laterale $x \star H$, dunque $|H| = |x \star H|$, da cui segue immediatamente la tesi.

7. Sia $(G, \cdot)$ un gruppo finito. Allora ogni elemento $x \in G$ ha ordine finito e tale ordine, $o(x)$, divide $|G|$.

   Dimostrazione $(\star\star)$

   Consideriamo un generico elemento $x \in G$ e le sue potenze positive: $x, x^2, x^3, ...$ Tali potenze sono infinite, e sono tutte elementi di G, che però ha cardinalità finita. Dunque devono esistere due numeri naturali i, j, con $i > j$ tali che

   $$x^i = x^j \Rightarrow x^{i-j} = e.$$

   Dunque esiste un numero naturale $N = i - j$ tale che $x^N = e$.
   Consideriamo l'insieme dei numeri naturali aventi questa proprietà: tale insieme è un sottoinsieme di numeri naturali, ed è non vuoto, dunque per il principio del minimo esso ammette un minimo M. Per la definizione di ordine di un elemento si ha che $o(x) = M$.

   Consideriamo adesso l'insieme

   $$X = \{e, x, x^2, ..., x^{M-1}\}.$$

   Tali elementi sono tutti distinti (se esistessero $0 \leq i, j < M$ tali che $x^i = x^j$ si avrebbe $x^{i-j} = e$ con $i - j < M$, assurdo). Inoltre si ha che $X = (x)$ per immediata verifica. Infine $((x), \cdot) < (G, \cdot)$ per il teorema 3, dunque per il teorema di Lagrange la sua cardinalità, ovvero $o(x)$, divide la cardinalità di G.

8. Sia $(G, \star)$ un gruppo finito. Allora per ogni elemento $x \in G$ si ha che $x^{|G|} = e$.

   Dimostrazione $(\star)$

   Poiché per il teorema precedente l'ordine di x divide la cardinalità di G si ha che

   $$\exists \alpha \in \mathbb{N} \mid |G| = \alpha \cdot o(x).$$

   Dunque

   $$x^{|G|} = x^{\alpha \cdot o(x)} = (x^{o(x)})^\alpha = e^\alpha = e.$$

9. **(Teorema di Eulero)** Siano $m \in \mathbb{N}, a \in \mathbb{Z} \mid (a, m) = 1$. Allora

   $$a^{\phi(m)} \equiv 1 \ (m)$$

   Dimostrazione $(\star\star)$

   Poiché a ed m sono coprimi, si ha che $[a] \in \mathbb{Z}_m^*$. Poiché $(\mathbb{Z}_m^*, \cdot)$ è un gruppo finito (per il teorema 40) con cardinalità $\phi(m)$, per il teorema precedente $[a]^{\phi(m)} = [1]$, che equivale a dire $a^{\phi(m)} \equiv 1 \ (m)$.

10. (**Piccolo teorema di Fermat)** Sia p un numero primo e sia a un intero coprimo con p. Allora

$$a^{p-1} \equiv 1 \ (p).$$

Dimostrazione $(\star)$

Dal teorema di Eulero, poiché $\phi(p) = p - 1$, si deduce immediatamente la tesi.

Dimostrazione alternativa $(\star\star)$

Verifichiamo la tesi per i numeri naturali, per gli interi negativi poi è una semplice verifica. Sappiamo che

$$(a + b)^p \equiv a^p + b^p \ (p),$$

e in particolare se $b = 1$ abbiamo che

$$(a + 1)^p \equiv a^p + 1 \ (p).$$

Procediamo per induzione su a per dimostrare che per ogni a vale $a^p \equiv a \ (p)$, da questa relazione si ricava banalmente la tesi dividendo per a.

Passo base $a = 0$ Banalmente vero;

Passo induttivo $a \Rightarrow a + 1$ Supponiamo di sapere che $a^n \equiv a \ (p)$, vogliamo dimostrare che allora vale anche $(a + 1)^p \equiv a + 1 \ (p)$. Sappiamo infatti che

$$(a + 1)^p \equiv a^p + 1 \equiv a + 1 \ (p),$$

dove l'ultimo passaggio si ha per l'ipotesi induttiva.

11. Siano a, b due numeri primi tra loro. Allora

$$\phi(ab) = \phi(a)\phi(b).$$

Dimostrazione $(\star)$

Un numero q è coprimo con ab se e solo se lo è sia con a che con b, in quanto se è coprimo con ab lo è necessariamente anche con a e con b, e viceversa se è coprimo con a e con b, se esistesse un primo p che divide sia ab sia q allora p dovrebbe dividere anche almeno uno fra a e b, assurdo.

Gli anelli $(\mathbb{Z}_a \times \mathbb{Z}_b, +, \cdot)$, $(\mathbb{Z}_{ab}, +, \cdot)$ sono fra loro isomorfi, pertanto avranno la stessa cardinalità. In particolare il numero di elementi coprimi con ab sarà uguale a quello delle coppie (y, z) dove y è coprimo con a e z con b. Per definizione della funzione ϕ di Eulero si ha la tesi.

12. Sia p un numero primo e n un intero positivo. Allora

$$\phi(p^n) = p^n - p^{n-1}.$$

Dimostrazione ($\star$)

Per definizione, $\phi(p^n)$ è il numero di interi positivi minori di p^n che sono coprimi con quest'ultimo. Ma allora, essendo p primo, basta escludere tutti e soli i numeri che sono multipli di p. Ogni p numeri, quindi, uno va escluso. In tutto sono allora $\frac{p^n}{p} = p^{n-1}$ numeri. Allora:

$$\phi(p^n) = p^n - p^{n-1}.$$

13. Sia m un intero positivo tale che $m = p_1^{\alpha_1}...p_k^{a_k}$. Allora

$$\phi(m) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})...(p_k^{a_k} - p_k^{a_k - 1}).$$

Dimostrazione ($\star\star$)

Segue immediatamente dai due teoremi precedenti.

14. **(Esercizio 6.29)** Se la cardinalità di un gruppo finito è un numero primo, allora il gruppo è ciclico.

Dimostrazione ($\star$)

Sia x un generico elemento del gruppo diverso dall'identità e sia p la cardinalità del gruppo. Per il teorema 7 l'ordine di x, $o(x)$, deve dividere p, e dunque si hanno due possibilità: $o(x) = 1$ oppure $o(x) = p$. Deve esistere almeno un elemento di ordine p, in quanto altrimenti si avrebbe che $G = \{e\}$, dunque ogni elemento del gruppo diverso dall'identità ha ordine p, da cui segue immediatamente la tesi.

15. **(Esercizio 6.30)** Sia $(G, \star)$ un gruppo. Allora

$$\forall x, y \in G \; x \star y = e \Leftrightarrow \; y \star x = e.$$

Dimostrazione ($\star$)

$x \star y = e \Leftrightarrow y \star x \star y = y \star e = y \Leftrightarrow y \star x \star y \star y^{-1} = y \star x = y \star y^{-1} = e.$

16. **(Esercizio 6.34)** Sia p un numero primo dispari. Se $[-1]$ è un quadrato in $\mathbb{Z}_p$ allora p è congruo a 1 modulo 4.

Dimostrazione ($\star$)

Se $[-1]$ è un quadrato in $\mathbb{Z}_p$ allora $\exists x \in \mathbb{N} \mid x^2 \equiv -1 \; (p)$. Ma allora $x^4 \equiv 1 \; (p)$ e $o(x)|4$. Dunque $o(x)$ può solo essere $1, 2, 4$, ma solo l'ultima possibilità è accettabile: $o(x) = 1 \Rightarrow x = 1$, che non è un quadrato in $\mathbb{Z}_p$ per ogni primo p dispari, mentre $o(x) = 2 \Rightarrow x^2 \equiv 1(p)$ ma $x^2 \equiv -1 \; (p)$. Inoltre $o(x) \;\mid\; \phi(p) = p - 1$, da cui si ha la tesi.

17. **(Esercizio 6.35)** Sia p un numero primo tale che $p \equiv 1\ (4)$. Allora

$$\left(\left(\frac{(p-1)}{2}\right)!\right)^2 \equiv -1\ (p).$$

Dimostrazione $(\star\star)$

Poniamo $p = 4k+1, k \in \mathbb{N}$. Allora

$$\left(\left(\frac{(p-1)}{2}\right)!\right)^2 = (2k)!^2 = (1 \cdot 2 \cdot ... \cdot 2k)^2 = (1 \cdot 2 \cdot ... \cdot 2k)(-1 \cdot -2 \cdot ... \cdot -2k).$$

$$(1 \cdot 2 \cdot ... \cdot 2k)(-1 \cdot -2 \cdot ... \cdot -2k) \equiv \Big(1 \cdot 2 \cdot ... \cdot (2k)\Big)\Big((4k) \cdot (4k-1) \cdot ... \cdot (2k+1)\Big) \equiv (4k)! \equiv (p-1)!\ (p).$$

Per il teorema di Wilson

$$(p-1)! \equiv -1\ (p).$$

18. **(Esercizio 6.36)** Esistono infiniti numeri primi congrui a 1 modulo 4.

Dimostrazione $(\star\star)$

Supponiamo per assurdo che essi siano in numero finito, e che siano in tutto N, chiamiamoli

$$p_1, ..., p_N.$$

Consideriamo dunque il numero

$$X = 4(p_1 ... p_N)^2 + 1 = M^2 + 1.$$

Esso è dispari e congruo a 1 modulo 4, inoltre modulo p_i, $1 \leq i \leq N$ è comunque congruo a 1. Inoltre se per caso un primo della forma $4k+3$ lo dividesse, dovremmo avere che

$$M^2 + 1 \equiv 0\ (4k+3).$$

Ma allora -1 sarebbe un quadrato modulo un primo dispari congruo a 3 modulo 4, assurdo per l'Esercizio 6.34. Dunque abbiamo ottenuto un nuovo primo della forma $4n+1$, assurdo per l'ipotesi iniziale.

19. **(Esercizio 6.37)** Sia $(G, \star)$ un gruppo e $(H, \star)$ un suo sottogruppo. Allora la seguente relazione: $xRy \Leftrightarrow y^{-1} \star x \in H$ è una relazione di equivalenza e inoltre xRy se e solo se appartengono allo stesso laterale destro $xH = yH$.

Dimostrazione $(\star)$

Mostriamo che tale relazione è una relazione di equivalenza.
• Riflessività $\Rightarrow xRx \Leftrightarrow x^{-1} \star x = e \in H$ OK.

• Simmetria $\Rightarrow xRy \Leftrightarrow y^{-1} \star x \in H \Leftrightarrow (y^{-1} \star x)^{-1} = x^{-1} \star y \in H \Leftrightarrow yRx$ OK (Per l'ultimo passaggio, essendo H un sottogruppo, contiene anche gli inversi di tutti i suoi elementi).

• Transitività $\Rightarrow xRy \wedge yRz \Leftrightarrow y^{-1} \star x \in H \wedge z^{-1} \star y \in H \Leftrightarrow z^{-1} \star y \star y^{-1} \star x = z^1 \star x \in H \Leftrightarrow xRz$. OK (Per l'ultimo passaggio, essendo H un sottogruppo, contiene anche il prodotto di due suoi elementi).

Supponiamo ora che due elementi $x, y \in G$ siano in relazione fra loro: dunque $y{-}1 \star x \in H$. Ovviamente $y \in yH = \{y \star h \mid h \in H\}$. Scegliendo $h = y^{-1} \star x$ si ottiene che $y \star y^{-1} \star x = x \in yH$. Per il teorema 4. allora $xH = yH$.
Viceversa siano $x, y \in G$ tali che $xH = yH$. Allora in particolare $y \in xH$, ovvero

$$\exists \bar{h} \in H \mid y = x \star \bar{h} \Rightarrow \bar{h} = x^{-1} \star y \in H \Rightarrow yRx \Rightarrow xRy.$$

20. Sia p un numero primo e $\beta \in \mathbb{N}$ Allora

$$\sum_{\alpha=0}^{\beta} \phi(p^\alpha) = p^\beta.$$

Dimostrazione ($\star$)

Utilizziamo il teorema 11.

$$\sum_{\alpha=0}^{\beta} \phi(p^\alpha) = \sum_{\alpha=0}^{\beta} (p^\alpha - p^{\alpha-1}) = \sum_{\alpha=0}^{\beta} p^\alpha - \sum_{\alpha=0}^{\beta} p^{\alpha-1} = p^\beta.$$

21. Sia $m \in \mathbb{N}$ e $a \in \mathbb{Z}_m$. Allora nel gruppo $(\mathbb{Z}_m, +)$

$$o(a) = \frac{m}{(a, m)}.$$

Dimostrazione ($\star$)

L'ordine di a è infatti la più piccola soluzione intera della congruenza

$$ax \equiv 0 \ (m)$$

che è equivalente a

$$x \equiv 0 \left(\frac{m}{(a, m)}\right),$$

la cui soluzione più piccola è proprio

$$\frac{m}{(m, a)}.$$

22. **(Esercizio 6.37, ma fatto anche a Esercitazioni)** Sia m un intero positivo. Allora

$$\sum_{d|m} \phi(d) = m.$$

Dimostrazione ($\star\star$)

Consideriamo il gruppo $(\mathbb{Z}_m, +)$. Abbiamo che $|\mathbb{Z}_m| = m$, dunque un generico elemento di $\mathbb{Z}_m$ ha ordine che è un divisore di m. Se dimostro che per ogni possibile ordine $d|m$ ci sono $\phi(d)$ elementi con ordine d, ho la tesi.

Sia d un divisore di m. Allora esiste un intero k tale che $m = kd$ e

$$d = o(a) = \frac{m}{(a, m)} = \frac{kd}{(a, kd)}$$

Dunque deve essere

$$k = (a, kd) \Rightarrow \ \exists b \in \mathbb{N} | a = kb \wedge (b, d) = 1, 1 \leq b \leq d$$

Differenti scelte di b producono differenti valori di a. Le possibili scelte di b sono i valori coprimi con d e minori di d, cioè proprio $\phi(d)$.

23. Siano $(G_1, \star), (G_2, \times)$ due gruppi, con le rispettive identità e_1 ed e_2 e $g \in G_1$. Allora, considerato un omomorfismo di gruppi

$$f : G_1 \to G_2,$$

valgono le seguenti:

$$f(e_1) = e_2,$$
$$f(g^{-1}) = f(g)^{-1}.$$

Dimostrazione $(\star)$

Si ha che

$$f(e_1) = f(e_1 \star e_1) = f(e_1) \times f(e_1).$$

Moltiplicando a sinistra ambo i membri per l'inverso di $f(e_1)$ abbiamo che:

$$f(e_1)^{-1} \times f(e_1) = f(e_1)^{-1} \times f(e_1) \times f(e_1),$$

da cui

$$e_2 = e_2 \times f(e_1) = f(e_1).$$

Verifichiamo che effettivamente l'inverso di $f(g)$ è proprio $f(g^{-1})$:

$$f(g) \times f(g^{-1}) = f(g \star g^{-1}) = f(e_1) = e_2.$$

24. $(Aut(G), \circ)$ è un gruppo.

Dimostrazione $(\star)$

Basta verificare le proprietà nella definizione di gruppo.

• La composizione di funzioni è associativa.

• La funzione identità:

$$i : G \to G$$
$$g \mapsto g$$

è chiaramente un automorfismo, e funge da identità per $(Aut(G), \circ)$:

$$\forall f \in Aut(G),\ i \circ f = f \circ i = f.$$

• Se $f \in Aut(G)$, anche $f^{-1} \in Aut(G)$, in quanto se una funzione è biunivoca lo è anche la sua inversa.

25. Sia $(G, \star)$ un gruppo, e sia $g \in G$. Allora la funzione coniugio C_g è un automorfismo di $(G, \star)$.

Dimostrazione $(\star)$

Bisogna verificare che C_g è un endomorfismo bigettivo.

Evidentemente è un omomorfismo, in quanto $\forall x, y \in G$

$$C_g(x \star y) = g \star (x \star y) \star g^{-1} = g \star (x \star g^{-1} \star g \star y) \star g^{-1} =$$

$$= (g \star x \star g^{-1}) \star (g \star y \star g^{-1}) = C_g(x) \star C_g(y).$$

Se trovo un'inverso per tale isomorfismo, evidentemente si ha la tesi. Tale inversa è la funzione:

$$C_{g^{-1}} : G \to G$$

$$x \mapsto g^{-1} \star x \star g.$$

26. Siano $(G_1, \star), (G_2, \times)$ due gruppi e

$$f : G_1 \to G_2$$

un omomorfismo di gruppi. Allora:

$$(Ker(f), \star) < (G_1, \star),$$

$$(Im(f), \times) < (G_2, \times).$$

Dimostrazione $(\star)$

Verifichiamo la prima asserzione.

- $f(e_1) = e_2 \Rightarrow e_1 \in Ker(f)$;
- $a, b \in Ker(f) \Rightarrow f(a) = e_2 = f(b) \Rightarrow f(a) \times f(b) = f(a \star b) = e_2 \times e_2 = e_2 \Rightarrow a \star b \in Ker(f)$;
- $a \in Ker(f) \Rightarrow f(a) = e_2 \Rightarrow e_2 = f(e_1) = f(a^{-1} \star a) = f(a^{-1}) \times f(a) = f(a^{-1}) \times e_2 = f(a^{-1})$.

Verifichiamo la seconda asserzione.

- $f(e_1) = e_2 \Rightarrow e_2 \in Im(f)$;
- $a, b \in Im(f) \Rightarrow \exists x, y \in G_1 \mid f(x) = a \wedge f(y) = b \Rightarrow f(x \star y) = f(x) \times f(y) = a \times b \Rightarrow a \times b \in Im(f)$;
- $a \in Im(f) \Rightarrow \exists x \in G_1 \mid f(x) = a \Rightarrow a^{-1} = f(x^{-1}) \times f(x) \times a^{-1} = f(x^{-1}) \times a \times a^{-1} = f(x^{-1}) \Rightarrow$

$$\Rightarrow a^{-1} \in Im(f).$$

27. Siano $(G_1, \star), (G_2, \times)$ due gruppi e
$$f : G_1 \to G_2$$
un omomorfismo di gruppi. Allora f è iniettivo se e solo se $Ker(f) = \{e_1\}$.

Dimostrazione $(\star)$

$(\Rightarrow)$ Supponiamo che f sia iniettivo e sia $g \in Ker(f)$ Allora $f(g) = e_2 = f(e_1)$. Per non violare l'iniettività, l'unica possibilità è che $g = e_1$.

$(\Leftarrow)$ Viceversa supponiamo che $Ker(f) = \{e_1\}$. Se per assurdo f non fosse iniettivo esisterebbero
$$g, h \in G_1,\ g \neq h \mid f(g) = f(h) \Rightarrow e_2 = f(g^{-1}) \times f(g) = f(g^{-1}) \times f(h) = f(g^{-1} \star h) \Rightarrow$$
$$\Rightarrow g^{-1} \star h \in Ker(f) \Rightarrow g^{-1} \star h = e_1 \Rightarrow g = h,$$
(assurdo).

Un altro modo per dimostrare la seconda implicazione è il seguente: siano $x,\ y \in G_1 \mid f(x) = f(y)$. Allora
$$f(x)f(y^{-1}) = e_2 \Rightarrow f(xy^{-1}) = e_2 \Rightarrow xy^{-1} \in Ker(f) \Rightarrow xy^{-1} = e_1 \Rightarrow x = y.$$

28. Siano $(G_1, \star), (G_2, \times)$ due gruppi e
$$f : G_1 \to G_2$$
un omomorfismo di gruppi. Allora $Ker(f)$ è invariante per coniugio, ovvero
$$\forall g \in G_1,\ C_g(Ker(f)) = Ker(f).$$

Dimostrazione $(\star)$

Dimostriamo la doppia inclusione.

$(\subseteq)$
$$x \in C_g(Ker(f)) \Rightarrow \exists h \in Ker(f) \mid x = g \star h \star g^{-1} \Rightarrow$$
$$\Rightarrow f(x) = f(g \star h \star g^{-1}) = f(g) \times f(h) \times f(g^{-1}) = f(g) \times f(g^{-1}) = f(g \star g^{-1}) = f(e_1) = e_2 \Rightarrow x \in Ker(f)$$

$(\supseteq)$ Dal punto precedente, scelto come g l'elemento g^{-1},
$$C_{g^{-1}}(Ker(f)) \subseteq Ker(f) \Rightarrow Ker(f) = C_g(C_{g^{-1}}(Ker(f)) \subseteq C_g(Ker(f)).$$

29. Sia $(S_n, \circ)$ il gruppo simmetrico con $n \geq 2$ elementi. Sia $\sigma \in S_n$: se σ si può scrivere come prodotto di t trasposizioni e anche come prodotto di k trasposizioni, allora $t \equiv k\ (2)$.

Dimostrazione $(\star\star)$

Sia $\mathbb{R}[x_1, ..., x_n]$, l'insieme dei polinomi a coefficienti reali in n variabili e consideriamo il seguente polinomio:

$$p(x_1, ..., x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Facciamo agire il gruppo simmetrico su di esso, nel seguente modo:

$$\sigma \cdot p(x_1, ..., x_n) = p(x_{\sigma(1)}, ..., x_{\sigma(n)}).$$

Consideriamo ora una trasposizione $\tau = (a, b),\ 1 \leq a < b \leq n$. Abbiamo che gli effetti sul polinomio di τ sono i seguenti:

- Per tutti gli $m < a, \tau$ scambia fra loro i fattori $x_m - x_a$ e $x_m - x_b$;
- Per tutti gli $m > b, \tau$ scambia fra loro i fattori $x_a - x_m$ e $x_b - x_m$;
- Per tutti gli $a < m < b, \tau$ scambia fra loro i due fattori $x_a - x_m$ e $x_m - x_b$, invertendone i segni. Tuttavia il segno del loro prodotto, e dunque quello del polinomi, risulta invariato;
- Infine, il fattore $x_a - x_b$ viene trasformato in $x_b - x_a$. Il segno di tale fattore viene dunque invertito.

In definitiva: $\tau \cdot p(x_1, ..., x_n) = -p(x_1, ..., x_n)$ Ora, se una permutazione si può scrivere come prodotto di più trasposizioni, diciamo t, abbiamo che per analizzarne il suo effetto sul polinomio, basta applicare una dopo l'altra queste t trasposizioni. Allora: $\sigma \cdot p(x_1, ..., x_n) = (-1)^t \cdot p(x_1, ..., x_n)$. Se σ si può scrivere anche come prodotto di k trasposizioni, si ha anche che:

$$\sigma \cdot p(x_1, ..., x_n) = (-1)^k \cdot p(x_1, ..., x_n).$$

Allora si deve avere che

$$(-1)^t = (-1)^k$$

che è equivalente a dire che $t \equiv k\ (2)$.

30. $(A_n, \circ) < (S_n, \circ)$ e $|A_n| = \frac{n!}{2}$.

Dimostrazione $(\star\star)$

Consideriamo la seguente funzione:

$$\epsilon : (S_n, \circ) \to (\mathbb{Z}_2, +)$$

$$\sigma \mapsto \begin{cases} 0 & \sigma \text{ è } \textit{una permutazione pari} \\ 1 & \sigma \text{ è } \textit{una permutazione dispari} \end{cases}$$

Essa è un morfismo fra i gruppi $(S_n, \circ)$ e $(\mathbb{Z}_2, +)$. Infatti: $\epsilon(\sigma \circ \tau) = 0$ implica che $\sigma \circ \tau$ è una permutazione pari. Segue che entrambe le permutazioni devono essere o pari o dispari. In ogni caso

$$\epsilon(\sigma) + \epsilon(\tau) = 0 = \epsilon(\sigma \circ \tau).$$

Il caso in cui $\epsilon(\sigma \circ \tau) = 1$ è pressoché identico.

Inoltre notiamo che $Ker(\epsilon) = A_n$ e dunque è un sottogruppo di $(S_n, \circ)$

Lo si può dimostrare, alternativamente, per via diretta verificando le proprietà nella definizione. Infatti l'identità $e \in A_n$, in quanto la si può vedere come una permutazione pari, la composizione di due permutazioni pari è ancora pari e l'inversa di una permutazione pari è ancora una permutazione pari.

Sappiamo che A_n è l'insieme di tutte le permutazioni pari. Inoltre è una A_n-classe laterale. Esiste anche un'altra classe laterale, che si può esprimere nella seguente forma: $\sigma \circ A_n$, dove σ è una trasposizione. I suoi elementi sono ovviamente tutte e sole le permutazioni dispari. L'insieme $\{A_n, \sigma \circ A_n\}$ costituisce una partizione di S_n. Poiché le classi laterali hanno tutte la stessa cardinalità, e $|S_n| = n!$, si ha che $|A_n| = \frac{n!}{2}$.

31. **(Esercizio 7.32)** Sia $n \geq 2$. Allora $Z(S_n) = \{e\}$.

Dimostrazione $(\star\star)$

Sia $\sigma \in Z(S_n)$: allora $\forall y \in S_n,\ \sigma \circ y = y \circ \sigma$.

Sicuramente $e \in Z(S_n)$. Supponiamo ora che esista $x \in Z(S_n),\ x \neq e$. Allora

$$\exists\ a, b \in \{1, ..., n\},\ a \neq b \mid x(a) = b.$$

Sia $c \in \{1, ..., n\} \mid c \neq a \wedge c \neq b$. Consideriamo $\tau = (b\ c)$, si ha che:

$$(\tau \circ x)(a) = c$$

$$(x \circ \tau)(a) = b$$

Allora $x \notin Z(S_n)$. Dunque si ha che

$$Z(S_n) = \{e\}.$$

32. **(Esercizio 7.35)** Per un intero $n \geq 2$, si ha che ogni permutazione di S_n si può scrivere come composizione di trasposizioni.

Dimostrazione ($\star\star$)

Una qualsiasi permutazione α si può scrivere come composizione di cicli disgiunti. Basta dunque dimostrare che ogni ciclo si può scrivere come composizione di trasposizioni. Sia $\sigma = (a_1 \ ... \ a_n)$ un ciclo. Allora dimostriamo per induzione sulla lunghezza del ciclo che: $\sigma = (a_1 \ a_n) \circ (a_1 \ a_{n-1}) \circ ... \circ (a_1 \ a_2)$.
Passo base $n = 1$
Ovvio, in quanto $(a_1 \ a_n)$ è già una trasposizione.
Passo induttivo $n \Rightarrow (n+1)$
Supponiamo di sapere che $\alpha = (a_1 \ ... \ a_n) = (a_1 \ a_n) \circ (a_1 \ a_{n-1}) \circ ... \circ (a_1 \ a_2)$. Allora per $\alpha' = (a_1 \ ... \ a_{n+1})$ abbiamo che $\alpha' = (a_1 \ a_{n+1}) \circ \alpha$.
Per ipotesi induttiva α si scrive come composizione di trasposizioni, e dunque anche α'.

33. **(Esercizio 7.42, ma fatto anche a Esercitazioni)** Siano $(G_1, \star), (G_2, \times)$ due gruppi e

$$f : G_1 \to G_2$$

un omomorfismo di gruppi. Allora

$$\forall x \in G_1 \ o(f(x)) | o(x).$$

Inoltre, f è iniettivo, se e solo se vale $o(f(x)) = o(x)$.

Dimostrazione ($\star$)

Sia $y = o(x)$: allora $f(x^y) = f(e_1) = e_2$. In particolare si ha che

$$f(x^y) = f(x)^y = e_2,$$

da cui la tesi.

Supponiamo che f sia iniettivo e che esista $g \mid o(f(g)) = m < n = o(g)$. Allora

$$f(x)^m = f(x^m) = e_2 \Rightarrow x^m \in Ker(f).$$

Ma $m < n \Rightarrow x^m \neq e_1$, (0assurdo).

Viceversa, supponiamo che valga $o(f(x)) = o(x)$, e sia $y \in Ker(f)$. Allora

$$f(y) = e_2 \Rightarrow o(f(y)) = 1 \Rightarrow o(y) = 1.$$

Dunque tutti e soli gli elementi in $Ker(f)$ sono gli elementi di G_1 di ordine 1, ovvero la sola identità.

34. Siano $(H,\cdot) \triangleleft (G,\cdot)$. Allora è possibile definire un prodotto $\boxdot$ sull'insieme G/H, in modo tale che $(G/H, \boxdot)$ sia un gruppo.

Dimostrazione $(\star)$

Definiamo il seguente prodotto:

$$(g_1H) \boxdot (g_2H) = g_1g_2H.$$

Esso è ben definito, in quanto, presi due differenti elementi delle classi laterali considerate, g_1h_1H, g_2h_2H si ha che:

$$(g_1h_1H) \boxdot (g_2h_2H) = g_1h_1g_2h_2H = g_1g_2g_2^{-1}h_1g_2H = g_1g_2(g_2^{-1}h_1g_2)H = g_1g_2\bar{h}H = g_1g_2H.$$

Inoltre abbiamo che eH si comporta da identità, poiché

$$\forall x \in G,\ xH \boxdot eH = (xe)H = xH = (ex)H = eH \boxdot xH.$$

Poi notiamo che ogni elemento xH ha un inverso, $x^{-1}H$:

$$xH \boxdot x^{-1}H = (xx^{-1})H = eH.$$

Infine, l'associatività di $\boxdot$ è una diretta conseguenza di quella del prodotto di G.

35. **(Primo teorema di omomorfismo di gruppi)** Siano $(G_1,\cdot), (G_2,\times)$ due gruppi e

$$f : G_1 \to G_2$$

un omomorfismo di gruppi. Allora

$$G_1/Ker(f) \cong Im(f).$$

Dimostrazione $(\star)$

Per completare la dimostrazione basta trovare un isomorfismo fra i due gruppi. Osserviamo preliminarmente che il gruppo $G_1/Ker(f)$ è ben definito, in quanto $Ker(f) \triangleleft G_1$.

Consideriamo la seguente funzione:

$$\phi :\ G_1/Ker(f) \to Im(f)$$

$$x\ Ker(f) \mapsto f(x)$$

Verifichiamo che essa è ben definita. Preso un differente elemento della stessa classe laterale considerata, $xh\ Ker(f)$,

$$\phi(xh\ Ker(f)) = f(xh) = f(x) \times f(h) = f(x)$$

Dunque verifichiamo che è effettivamente un omomorfismo:

$$\phi((x\ Ker(f))(y\ Ker(f))) = \phi(xy\ Ker(f)) = f(xy) = f(x) \times f(y) = \phi(x\ Ker(f))\phi(y\ Ker(f))$$

Adesso mostriamo che è iniettivo, facendo vedere che $Ker(\phi) = \{Ker(f)\}$. Sia $x\ Ker(f) \in Ker(\phi)$. Allora:

$$\phi(x\ Ker(f)) = f(x) = e_2 \Rightarrow x \in Ker(f).$$

Infine mostriamo che è surgettivo: preso un generico elemento $f(\alpha) \in Im(f)$, basta prendere $\alpha\ Ker(f)$:

$$\phi(\alpha\ Ker(f)) = f(\alpha)$$

36. Siano $(G_1, \star), (G_2, \times)$ due gruppi e
$$f : G_1 \to G_2$$
un omomorfismo di gruppi surgettivo. Allora:
$$G_1/Ker(f) \cong G_2.$$

Dimostrazione $(\star)$

Banale applicazione del teorema 34.

37. Siano $(G_1, \star), (G_2, \times)$ due gruppi e
$$f : G_1 \to G_2$$
un omomorfismo di gruppi iniettivo. Allora:
$$G_1 \cong Im(f).$$

Dimostrazione $(\star)$

Banale applicazione del teorema 34.

38. **(Esercizio 8.11)** $(H, \cdot) \triangleleft (G, \cdot) \Leftrightarrow \forall g \in G\ gH = Hg$.

Dimostrazione $(\star)$

$(\Rightarrow)$ Se H è normale, allora
$$\forall g \in G\ gHg^{-1} = H \Rightarrow gHg^{-1}g = gH = Hg.$$
$(\Leftarrow)$ Se per ogni $g \in G$ si ha che $gH = Hg$ allora moltiplicando a destra ambo i membri per l'inverso di g si ottiene
$$gHg^{-1} = H$$
che è la proprietà richiesta affinché H sia normale.

39. **(Esercizio 8.12)** Sia $(G, \cdot)$ un gruppo e $(H_i,\ \cdot) < (G,\ \cdot)\ \forall i \in I$ (dove I è una famiglia di indici, anche infinita). Allora:
$$\left(\bigcap_{i\in I} H_i, \cdot\right) < (G,\ \cdot)$$
Inoltre se $(H_i,\ \cdot) \triangleleft (G,\ \cdot)\ \forall i \in I$ si ha che $\left(\bigcap_{i\in I} H_i,\ \cdot\right) \triangleleft (G,\ \cdot)$

Dimostrazione$(\star\star)$
Infatti
$$e \in H_i\ \forall i \in I \Rightarrow e \in \bigcap_{i\in I} H_i;$$
$$a, b \in H_i\ \forall i \in I \Rightarrow ab \in H_i\ \forall i \in I \Rightarrow ab \in \bigcap_{i\in I} H_i;$$
$$a \in H_i\ \forall i \in I \Rightarrow a^{-1} \in H_i\ \forall i \in I \Rightarrow a^{-1} \in \bigcap_{i\in I} H_i.$$
Sia H_i normale per ogni $i \in I$. Allora $\forall g \in G$
$$gH_ig^{-1} = H_i,$$
$$\bigcap_{i\in I} H_i = \bigcap_{i\in I} gH_ig^{-1} = g\left(\bigcap_{i\in I} H_i\right)g^{-1}.$$

40. **(Esercizio 9.7)** Sia $(R, +, \cdot)$ un anello. Allora $(R^*, \cdot)$ è un gruppo.

Dimostrazione $(\star)$
Basta verificare le proprietà che lo rendono tale. Infatti:

• L'identità per la moltiplicazione dell'anello $(R, +, \cdot)$ fa da identità anche per la moltiplicazione tra elementi di R^*, essendo $R^* \subset R$. Inoltre $e \in R^*$, in quanto e è invertibile ($e^{-1} = e$).

• La moltiplicazione è associativa, in quanto $R^* \subset R$ e per tutti gli elementi di R lo è.

• Per stessa definizione di R^*, ogni elemento ha inverso.

41. Se p è un numero primo allora $\mathbb{Z}_p$ è un campo.

Dimostrazione $(\star)$

Consideriamo un generico elemento $\mathbb{Z}_p$ diverso dall'identità, $[x]_p$. Allora in particolare $(x,\ p) = 1$, e dunque esiste una soluzione per la congruenza

$$ax \equiv 1\ (p),$$

cioè esiste $b \in \mathbb{Z}$ tale che

$$ab \equiv 1\ (p).$$

Allora l'inverso di $[a]_p$ è $[b]_p$.

42. Sia $(R, +, \cdot)$ un anello. Allora $\forall a, b \in R$:

- $a0 = 0a = 0$;
- $-(-a) = a$;
- $a(-b) = (-a)b = -(ab)$;
- $(-a)(-b) = ab$.

Dimostrazione $(\star)$

$$a0 = a(0 + 0) = a0 + a0 \Rightarrow a0 = 0.$$
$$0a = (0 + 0)a = 0a + 0a \Rightarrow 0a = 0.$$

$$a + (-a) = 0.$$

Dunque l'inverso di $-a$, che sappiamo essere unico, è a, ovvero

$$-(-a) = a.$$

Si ha che l'inverso di ab è $-ab$, che sappiamo essere unico. Pertanto bisogna verificare che $a(-b) + ab = 0,\ (-a)b + ab = 0$.

$$a(-b) + ab = a(-b + b) = a0 = 0,$$
$$(-a)b + ab = b(-a + a) = b0 = 0.$$

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

43. Siano $(R, +, \cdot)$ *e* $(S, \boxdot, \times)$ due anelli e $\phi : R \to S$ un omomorfismo di anelli. Allora $Ker(\phi)$ è un ideale dell'anello $(R, +, \cdot)$.

Dimostrazione $(\star)$

Bisogna verificare le proprietà nella definizione. Per il teorema 26. $(Ker(\phi), +) < (R, +)$. Inoltre, siano $x \in Ker(\phi)$ e $y \in R$. Allora

$$\phi(x) = e_2 \Rightarrow \phi(xy) = \phi(x) \times \phi(y) = e_2 \times \phi(y) = e_2 \Rightarrow xy \in Ker(\phi);$$

$$\phi(x) = e_2 \Rightarrow \phi(yx) = \phi(y) \times \phi(x) = \phi(y) \times e_2 = e_2 \Rightarrow yx \in Ker(\phi).$$

44. **(Esercizio 9.20)** Siano $(R, +, \cdot)$ *e* $(S, \boxdot, \times)$ due anelli e $\phi : R \to S$ un omomorfismo di anelli. Allora $(\phi(R), \boxdot, \times)$ è un sottoanello di $(S, \boxdot, \times)$.

Dimostrazione $(\star)$

Bisogna verificare le proprietà nella definizione.

- Poiché $\phi(1_R) = 1_S \Rightarrow 1_S \in \phi(R)$
- Per il teorema 25. $(\phi(R), \boxdot) < (S, \boxdot)$.
- Siano $\phi(\alpha), \phi(\beta) \in \phi(R)$. Allora consideriamo l'elemento $\alpha\beta \in R$: si ha che

$$\phi(\alpha\beta) = \phi(\alpha) \times \phi(\beta) \in \phi(R)$$

45. **(Primo teorema di omomorfismo di anelli)** Siano $(R, +, \cdot), (S, \boxdot, \times)$ due anelli e

$$f : R \to S$$

un omomorfismo di anelli. Allora

$$R/Ker(f) \cong Im(f).$$

Dimostrazione $(\star)$

Per completare la dimostrazione basta trovare un isomorfismo fra i due anelli. Consideriamo la seguente funzione:

$$\sigma : \ R/Ker(f) \to Im(f)$$
$$x + Ker(f) \mapsto f(x).$$

Verifichiamo che essa è ben definita. Preso un differente elemento della stessa classe laterale considerata, $x + h + Ker(f)$,

$$\sigma(x + h + Ker(f)) = f(x + h) = f(x) \ \boxdot \ f(y) = f(x) \ \boxdot \ 0_S = f(x).$$

Dunque verifichiamo che è effettivamente un omomorfismo di anelli:

$$\sigma(1_R + Ker(f)) = f(1_R) = 1_S$$

$$\sigma((a + Ker(f)) + (b + Ker(f))) = \sigma(a + b + Ker(f)) = f(a + b) = f(a) \boxdot f(b) =$$
$$\sigma(a + Ker(f)) \boxdot \sigma(b + Ker(f))$$
$$\sigma((a + Ker(f))(b + Ker(f))) = \sigma(ab + Ker(f)) = f(ab) = f(a) \times f(b) =$$
$$\sigma(a + Ker(f)) \times \sigma(b + Ker(f)).$$

Adesso mostriamo che è iniettivo.

$$Ker(\sigma) = \{a + Ker(f) \in R/Ker(f) \mid \sigma(a + Ker(f)) = e_2\} =$$
$$= \{a + Ker(f) \in R/Ker(f) \mid f(a) = e_2\} = \{a + Ker(f) \in R/Ker(f) \mid a \in Ker(f)\} \Rightarrow$$
$$Ker(\sigma) = \{Ker(f)\}.$$

Infine mostriamo che è surgettivo: preso un generico elemento $f(\alpha) \in Im(f)$, basta prendere $\alpha + Ker(f)$:

$$\sigma(\alpha + Ker(f)) = f(\alpha).$$

46. **(Esercizio 9.32)** Si consideri l'anello $(\mathbb{Z}, +, \cdot)$ e l'ideale $I = (m) = m\mathbb{Z}$.Allora

$$R/I \cong \mathbb{Z}_m.$$

Dimostrazione ($\star$)

Sfruttiamo il primo teorema di omomorfismo di anelli.
Considero la seguente funzione:

$$\phi : \mathbb{Z} \to \mathbb{Z}_m$$
$$x \to [x]_m$$

Questo è un morfismo fra gli anelli $(\mathbb{Z}, +, \cdot),\ (\mathbb{Z}_m, +', \cdot')$ infatti:

$$\phi(1) = [1]_m;$$
$$\phi(a+b) = [a+b]_m = [a]_m +' [b]_m = \phi(a) +' \phi(b);$$
$$\phi(ab) = [ab]_m = [a]_m \cdot' [b]_m = \phi(a) \cdot' \phi(b).$$

Inoltre si ricava immediatamente che è surgettivo (per avere la classe $[x]_m$ basta scegliere l'elemento $x \in \mathbb{Z}$) e che $Ker(\phi) = (m)$ La tesi segue dal primo teorema di omomorfismo.

In alternativa si potrebbe cercare un isomorfismo di anelli. Ad esempio andrebbe bene il seguente

$$\phi : \mathbb{Z}/I \to \mathbb{Z}_m$$
$$x + I \mapsto [x]_m.$$

47. Un dominio d'integrità finito $(D, +, \cdot)$ è un campo.

Dimostrazione

Supponiamo che $|D| = n$ e $D = \{0, 1, x_1, ..., x_{n-2}\}$ e supponiamo per assurdo che ci sia un elemento diverso da $0,\ 1$ che non abbia inverso. Ciò equivale ad affermare che esiste $1 \leq j \leq n-2$ tale che $\forall 1 \leq h \leq n-2 \in D,\ x_j x_h \neq 1$. I possibili prodotti del tipo $x_j x_h$ sono in tutto $n-2$ al variare di $1 \leq h \leq n-2$, e sono $x_1, ..., x_{n-2}$ ($0,\ 1$ non sono accettabili, rispettivamente perché siamo in un dominio e perché altrimenti si avrebbe che x_j è invertibile.). Supponiamo che tali prodotti siano tutti distinti. Allora esiste k per cui

$$x_j x_k = x_j \Rightarrow x_k(x_j - 1) = 0 \Rightarrow x_j = 1 \vee x_k = 0\ (Assurdo)$$

Allora devono esserci due prodotti uguali fra loro, ovvero esistono $\alpha,\ \beta$ distinti per cui

$$x_j x_\alpha = x_j x_\beta \Rightarrow x_j(x_\alpha - x_\beta) = 0 \Rightarrow x_j = 0 \vee x_\alpha = x_\beta\ (Assurdo)$$

Allora ogni elemento ha un inverso, da cui la tesi.

48. Sia $(R, +, \cdot)$ un anello commutativo e I un suo ideale. Allora l'anello $(R/I, +, \cdot)$ è un dominio d'integrità se e solo se I è un ideale primo.

Dimostrazione $(\star)$

($\Rightarrow$) Supponiamo che $(R/I, +, \cdot)$ sia un dominio di integrità, e supponiamo che $ab \in I$. Allora, guardiamo in R/I al prodotto $(a + I)(b + I)$. Si ha che

$$(a + I)(b + I) = (ab + I) = I.$$

Ma poiché R/I è un dominio allora $a \in I \vee b \in I$, dunque I è un ideale primo.

($\Leftarrow$) Supponiamo che I sia un ideale primo, e che $ab \in I$. Per definizione di ideale primo allora $a \in I$ o $b \in I$. Allora, guardiamo in R/I all'elemento I. Si ha che

$$I = ab + I = (a + I)(b + I)$$

Poiché I è primo, almeno uno fra a e b appartiene ad I, vale a dire, $(R/I, +, \cdot)$ è un dominio di integrità.

49. Sia $(R, +, \cdot)$ un anello commutativo e I un suo ideale. Allora l'anello $(R/I, +, \cdot)$ è un campo se e solo se I è un ideale massimale.

Dimostrazione $(\star\star)$

($\Rightarrow$) Supponiamo che $(R/I, +, \cdot)$ sia un campo e supponiamo che esista un ideale J tale che

$$I \subseteq J \subseteq R.$$

Se $J = I$ abbiamo finito, se $J \neq I$ allora $\exists j \in J \mid j \notin I$. Questo vuol dire che $j + I \neq I$, e poiché R/I è un campo, $j + I$ ha un inverso, sia esso $k + I$. Allora

$$(j + I)(k + I) = (jk + I) = (1 + I)$$

Dunque per un certo $i \in I$ si ha che $1 = jk + i$. Ma allora $1 \in J \Rightarrow J = R$.

($\Leftarrow$) Supponiamo ora che I sia un ideale massimale. Allora per avere la tesi bisogna mostrare che ogni elemento della forma $m + I,\ m \notin I$, ha un inverso. Prendiamo l'ideale $(m) + I$. Ovviamente $I \subsetneq (m) + I$, dunque per la massimalità di I, deve essere $(m) + I = R$. Allora in particolare $1 \in (m) + I$ e dunque

$$\exists \alpha \in R, \exists \beta \in I \mid 1 = \alpha m + \beta.$$

Allora verifichiamo che l'inverso cercato è $\alpha + I$:

$$(\alpha + I)(m + I) = 1 - \beta + I = 1 + I.$$

50. Sia $(R, +, \cdot)$ un anello commutativo. Allora un suo ideale massimale è anche primo.

Dimostrazione $(\star\star)$

Supponiamo che $I \subseteq R$ sia un ideale massimale, allora in particolare $(R/I, +, \cdot)$ è un campo per il teorema precedente, e in particolare è un dominio d'integrità. Ma allora per il teorema 48. I è un ideale primo.

51. **(Esercizio 10.7)** Sia $(S,+,\cdot)$ un anello commutativo e $(R,+,\cdot)$ un suo sottoanello. Allora, preso $\alpha \in S$ la funzione

$$\theta : \ R[x] \to S$$
$$p(x) \mapsto p(\alpha)$$

è un omomorfismo di anelli, noto come omomorfismo di valutazione.

Dimostrazione $(\star)$

Basta verificare le proprietà nella definizione.

$\bullet \theta(1_R) = 1_S$;

$\bullet \theta(p(x)+q(x)) = \theta((p+q)(x)) = (p+q)(\alpha) = p(\alpha)+q(\alpha) = \theta(p(x))+\theta(q(x))$;

$\bullet \theta(p(x)q(x)) = \theta((pq)(x)) = (pq)(\alpha) = p(\alpha)q(\alpha) = \theta(p(x))\theta(q(x))$.

52. Sia $(R,+,\cdot)$ un anello euclideo e siano $a,b \neq 0$. Se $b|a$ ma $a \nmid b$ allora $gr(b) < gr(a)$.

Dimostrazione $(\star\star)$

Poiché b divide a possiamo scrivere, per un certo k, $a = bk$. Inoltre si può svolgere la divisione euclidea di b per a, e dunque esistono $q,\ r$ tali che

$$b = aq + r$$

con $r \neq 0$ e $gr(r) < gr(a)$. Allora

$$r = b - aq = b - bkq = b(1-kq)$$

da cui si deduce $gr(r) \geq gr(b)$ e dunque $gr(a) > gr(r) \geq gr(b)$.

53. Sia $(R,+,\cdot)$ un anello euclideo. Allora $\forall x \in R\ gr(x) \geq gr(1)$. In particolare $gr(x) = gr(1)$ se e solo se x è invertibile.

Dimostrazione $(\star\star)$

Per ogni $b \in R$ vale che $gr(b1) \geq gr(1)$, dunque $gr(1)$ è il minimo fra i gradi degli elementi dell'anello.

$(\Rightarrow)$ Supponiamo che $gr(b) = gr(1)$ e sia $a \in R$. Allora svolgendo la divisione euclidea di a per b

$$a = bq + r,$$

con $r = 0$ oppure $gr(r) < gr(a)$. Ma poiché b ha il grado minimo possibile deve essere $r = 0$ e dunque $a \in (b) \forall a \in R$, vale a dire $R = (b)$.

$(\Leftarrow)$ Supponiamo che $b \in R^*$. Allora $R = (b)$ e quindi

$$\forall a \in R\ \exists k \in R \mid a = bk \Rightarrow \forall a \in R,\ gr(b) \leq gr(a),$$

e quindi $gr(b)$ è il minimo possibile dei gradi, ovvero $gr(b) = gr(1)$.

54. $(\mathbb{Z}[i], +, \cdot)$ è euclideo.

Dimostrazione $(\star\star\star)$

Bisogna definire una funzione grado. Consideriamo la seguente:

$$gr : \mathbb{Z}[i] - \{0\} \to \mathbb{N}$$
$$a + bi \mapsto a^2 + b^2$$

Verifichiamo le proprietà della definizione.

• Siano $x = a + bi, y = c + di \in R$ non nulli. Allora

$$gr(xy) = gr(ac-bd+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2 = a^2c^2+b^2d^2+a^2d^2+b^2c^2 = (a^2+b^2)(c^2+d^2)$$
$$gr(x) = a^2 + b^2$$

Allora $c + di \neq 0 \Rightarrow c \neq 0,\ d \neq 0 \Rightarrow c^2 + d^2 \geq 1$. Dunque $gr(xy) \geq gr(x)$.

• Per l'ultima proprietà, consideriamo il piano e un riferimento cartesiano con ascisse intere e ordinate del tipo $iz,\ z \in \mathbb{Z}$. Siano $\alpha,\ \beta \in \mathbb{Z}[i],\ \beta \neq 0$. Consideriamo tutti i multipli di β in $\mathbb{Z}_i$, questi individuano nel piano complesso un reticolo dato dai vertici di quadrati di lato $|\beta|$.. Sia $q\beta$ un vertice del quadrato che ha distanza minima da α: tale distanza è nel peggiore dei casi

$$\frac{|\beta|}{\sqrt{2}},$$

quando α è nel centro del quadrato, dunque: $|\alpha - q\beta| \leq \frac{|\beta|}{\sqrt{2}}$. Segue che $gr(\alpha - q\beta) \leq \frac{gr(\beta)}{2} < gr(\beta)$. Prendiamo dunque q come quoziente e $\alpha - q\beta$ come resto per avere la divisione euclidea cercata.

55. L'anello $(\mathbb{Z}, +, \cdot)$ è euclideo.

Dimostrazione $(\star\star)$

Bisogna definire una funzione grado. Consideriamo la seguente:

$$gr : \mathbb{Z} - \{0\} \to \mathbb{N}$$
$$z \mapsto |z|.$$

Verifichiamo le proprietà della definizione.

• Siano x e y interi non nulli. Allora

$$gr(xy) = |xy| \geq |x| = gr(x).$$

• Possiamo limitarci al caso $y > 0$ visto che -1 è un invertibile in questo anello. Allora utilizziamo il principio del minimo sul seguente insieme:

$$A = \{q \in \mathbb{N} \mid x \leq qy\}.$$

Esso è un sottoinsieme di $\mathbb{N}$ non vuoto, dunque ammette minimo $\bar{q}$. Se $\bar{q}y = x$ abbiamo la seguente divisione euclidea:

$$x = \bar{q}y + 0.$$

Supponiamo dunque $\bar{q}y > x$, allora deve essere $(\bar{q} - 1)y < x$, altrimenti $\bar{q} - 1$ apparterrebbe ad A e sarebbe minore del minimo $\bar{q}$, assurdo. Si ha che

$$0 < r = x - (\bar{q} - 1)y < y$$

e dunque la divisione euclidea cercata è

$$x = (\bar{q} - 1)y + r.$$

56. **(Esercizio 10.15)** Gli elementi invertibili in $\mathbb{Z}[i]$ sono solo quattro: $1, -1, i, -i$.

Dimostrazione $(\star)$

Per il teorema 53. un elemento x di un anello euclideo è invertibile se e solo se $gr(x) = 1$.. Sia $x = a + ib$: allora $gr(x) = a^2 + b^2$. Ovviamente se a oppure b è maggiore di 1, allora $gr(x) > 1$ e x non è invertibile. Dunque possiamo supporre $a \leq 1 \wedge b \leq 1$. Si hanno le seguenti possibilità:

$$a = b = 1 \ (x = 1 + i) \Rightarrow gr(x) = 2 \Rightarrow x \ \textit{non} \text{ è } \textit{invertibile};$$

$$a = 0 \wedge b = 1 \ (x = i) \Rightarrow gr(x) = 1;$$
$$a = 0 \wedge b = -1 \ (x = -i) \Rightarrow gr(x) = 1;$$
$$a = 1 \wedge b = 0 \ (x = 1) \Rightarrow gr(x) = 1;$$
$$a = -1 \wedge b = 0 \ (x = -1) \Rightarrow gr(x) = 1.$$

57. **(Correttezza dell'algoritmo di Euclide)** Sia $(R, +, \cdot)$ un dominio euclideo (e dunque, per il teorema 60, a ideali principali). Sia data la seguente divisione euclidea:

$$a = bq + r,$$

con almeno uno fra a, b e b, r non nullo. Allora:

$$(a, b) = (b, r).$$

Dimostrazione $(\star\star)$

Consideriamo i seguenti due insiemi:

$$A = \{x \in \mathbb{N} \mid x \mid a \wedge x \mid b\},$$

$$B = \{x \in \mathbb{N} \mid x \mid b \wedge x \mid r\}.$$

Mostriamo che sono uguali:

$(\subseteq)$ Sia $x \in A$: allora $x \mid a \wedge x \mid b \Rightarrow x \mid a - bq = r \Rightarrow x \in B$.

$(\supseteq)$ Sia $x \in B$: allora $x \mid b \wedge x \mid r \Rightarrow x \mid bq + r = a \Rightarrow x \in A$.

Poiché i due insiemi sono uguali, in particolare il loro massimo sarà uguale. Dunque:

$$(a, b) = (b, r).$$

58. **(Esercizio 10.21)** Sia $(R, +, \cdot)$ un anello commutativo: se gli unici suoi ideali sono $\{0\}$ e R allora è un campo.

Dimostrazione $(\star)$

Per ipotesi l'ideale $\{0\} = (0)$ è massimale, e dunque per il teorema 49. $(R/(0), +, \cdot)$ è un campo. A questo punto basta notare che ovviamente

$$R/(0) \cong R.$$

La tesi è dunque immediata.

59. Sia $(R, +, \cdot)$ un dominio e sia $a \in R$. Allora

$$R[x]/(x-a) \cong R.$$

Dimostrazione $(\star)$

Usiamo il primo teorema di omomorfismo di anelli. Considero la seguente funzione:

$$\phi : R[x] \to R$$

$$p(x) \mapsto p(a)$$

Per il teorema 51. esso un omomorfismo (di valutazione). Mostriamo che $Ker(\phi) = (x-a)$, facendo vedere la doppia inclusione.

$(\subseteq)$ Sia $p(x) \in Ker(\phi)$. Allora $p(a) = 0$ e per il teorema di Ruffini svolto a Esercitazioni

$$\exists q(x) \in R[x] \mid p(x) = (x-a)q(x) \Rightarrow p(x) \in (x-a).$$

$(\supseteq)$ Sia $p(x) \in (x-a)$. Allora

$$\exists q(x) \in R[x] \mid p(x) = (x-a)q(x).$$

Ma allora $p(a) = 0$, e dunque $p(x) \in Ker(\phi)$.
Inoltre l'omomorfismo è surgettivo: per ottenere l'elemento $\gamma \in R$ basta scegliere il polinomio $p(x) = \gamma \in R[x]$. Dal primo teorema di omomorfismo si ha la tesi.

60. Sia $(R, +, \cdot)$ un anello euclideo. Allora tutti i suoi ideali sono principali.

Dimostrazione $(\star\star)$

Sia I un ideale di R. Ovviamente l'ideale $I = \{0\}$ è un ideale principale, generato da 0. Supponiamo allora che esista $d \in I,\ d \neq 0$. e consideriamo allora

$$m = \min\{gr(a) \mid a \in I - \{0\}\} = \min A.$$

A è un sottoinsieme di $\mathbb{N}$ ed è inoltre non vuoto, dunque per il principio del buon ordinamento ammette minimo m: sia $d \in I \mid gr(d) = m$. Vogliamo mostrare che $(d) = I$.

$(\supseteq)$ Ovvio, visto che $d \in I$;

$(\subseteq)$ Sia $y \in I$, allora visto che siamo in un anello euclideo esistono $q,\ r \in R \mid y = qd + r$. Poiché $y \in I$ e $d \in I$ allora $y - qd = r \in I$. Si hanno due possibilità: se fosse $r \neq 0$ allora $gr(r) < gr(d)$, che è assurdo vista la minimalità del grado di d. Dunque $r = 0$ e $y = qd \Rightarrow y \in (d)$.

61. Sia $(R, +, \cdot)$ un dominio ad ideali principali e siano $a, b \in R$ non entrambi nulli. Allora esiste un massimo comun divisore d di $a,\ b$ e inoltre $\exists \alpha, \beta \in R \mid \alpha a + \beta b = d$.

Dimostrazione $(\star\star)$

Consideriamo l'ideale $I = (a, b)$: poiché siamo in un dominio ad ideali principali esiste $d \in R \mid I = (d)$. Osserviamo che, poiché $d \in (a, b)$, è possibile scrivere per certi $\alpha, \beta \in R$

$$d = \alpha a + \beta b.$$

Osserviamo che d è un massimo comun divisore di $a,\ b$: infatti $a \in (d),\ b \in (d) \Rightarrow \exists c, c' \mid a = cd \wedge b = c'd$. Inoltre

$$p|a \ \wedge \ p|b \Rightarrow \exists M, N \in R \mid a = pM \ \wedge b = pN \Rightarrow$$
$$\Rightarrow d = \alpha a + \beta b = \alpha pM + \beta pN = p(\alpha M + \beta N) \Rightarrow p|d.$$

62. Siano $a, b \in \mathbb{Z}$ entrambi non nulli. Allora $(a, b) = c$ è il più piccolo intero positivo esprimibile come combinazione lineare intera di a e b.

Dimostrazione $(\star)$

Supponiamo che esista $\delta \in R$, tale che $\delta < (a, b) = c$ è esprimibile come combinazione lineare intera di a e b. Allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\delta = \alpha a + \beta b$. Poiché c divide sia a sia b si ricava che esistono $m, n \in \mathbb{Z}$ per cui $a = cm$ e $b = cn$, pertanto

$$\delta = \alpha(cm) + \beta(cn) = c(\alpha m + \beta n).$$

Ma allora $c|\delta$, e in particolare $c \leq \delta$, dunque $\delta = (a, b)$.

63. Siano $a, b \in \mathbb{Z}$ due interi, e sia $d = (a, b)$ il loro massimo comun divisore. Allora i due numeri interi $\frac{a}{d}$ e $\frac{b}{d}$ sono coprimi.

Dimostrazione $(\star)$

Sappiamo che esistono $\alpha, \beta \in \mathbb{Z}$ tali che

$$\alpha a + \beta b = d \Rightarrow \alpha\left(\frac{a}{d}\right) + \beta\left(\frac{b}{d}\right) = 1.$$

Per il teorema precedente allora si ha subito la tesi.

64. Siano a, b, c interi tali che $a|bc$ e $(a, b) = 1$. Allora $a|c$.

Dimostrazione $(\star)$

Sappiamo che esistono $\alpha, \beta \in \mathbb{Z}$ tali che

$$\alpha a + \beta b = 1 \Rightarrow \alpha ac + \beta bc = c.$$

Poiché banalmente $a|\alpha ac$ e per ipotesi $a|bc$ si ha anche che $a|\alpha ac + \beta bc = c$.

65. Sia $(R, +, \cdot)$ un dominio di integrità e sia $p \in R$ primo. Allora p è irriducibile.

Dimostrazione $(\star)$

Sia $p = xy$. Poiché p è primo $p|x$ oppure $p|y$. Senza perdita di generalità, supponiamo che $p|x$. Allora $\exists M \in R \mid x = pM$. Dunque $p = pMy \Rightarrow p(1 - My) = 0$. Tuttavia, poiché siamo in un dominio d'integrità e $p \neq 0$, deve essere $1 - My = 0 \Rightarrow My = 1 \Rightarrow y \in R^*$.

66. Sia $(R, +, \cdot)$ un dominio a ideali principali e sia $p \in R$ irriducibile. Allora (p) è massimale.

Dimostrazione $(\star)$

Sia J un ideale tale che $(p) \subseteq J \subseteq R$. Allora poiché siamo in un dominio ad ideali principali, esiste $q \in R \mid J = (q)$. Poiché $p \in (q) \exists h \in R \mid p = qh$, ma poiché p è irriducibile q è invertibile o h è invertibile:
- Se q è invertibile allora $J = R$;
- Se h è invertibile allora $J = (p)$.

67. Sia $(R, +, \cdot)$ un dominio a ideali principali e sia $p \in R$ irriducibile. Allora p è primo.

Dimostrazione $(\star\star)$

Poiché p è irriducibile, per il teorema 60. (p) è massimale, e per il teorema 49. è anche primo. Dunque l'elemento p è primo.

68. Ogni anello euclideo $(R, +, \cdot)$ è anche a fattorizzazione unica.

Dimostrazione $(\star\star\star)$

Esistenza della fattorizzazione

Poiché siamo in un dominio euclideo, è possibile definire una funzione grado ρ. Sia $a \in R$ un elemento non invertibile e non nullo: procediamo per induzione su $\rho(a)$.

Passo base $\rho(a) = 2$.
Mostriamo che a deve essere irriducibile, infatti se fosse $a = bc$ si avrebbero due casi: se $a = b$ si avrebbe che

$$a = bc \Rightarrow 1 = c,$$

e dunque c è invertibile; se $a \neq b$ si avrebbe che $b \mid a$ ma $a \nmid b$. Allora per il teorema 52 $\rho(b) < \rho(a) = 2$, ovvero $\rho(b) = 1$, e dunque b è invertibile.
Passo induttivo $\rho(\alpha) \Rightarrow \rho(\alpha) + 1$.
Supponiamo ora che $\rho(a) = n + 1$ non sia minima, e che la tesi sia vera per tutti gli elementi con grado $\leq n$. Se a è irriducibile non c'è niente da dimostrare, allora possiamo supporre che a non sia irriducibile, e dunque per certi α, β si ha $a = \alpha\beta$. Ma allora per come è definità la funzione grado $\rho(\alpha) < \rho(a) = n + 1$ e $\rho(\beta) < \rho(a) = n + 1$. Dunque per ipotesi induttiva esiste una fattorizzazione per α e β, dunque una fattorizzazione per a si ottiene moltiplicando fra loro le fattorizzazioni di α e di β.

Unicità della fattorizzazione

Supponiamo che esistano due fattorizzazioni in elementi irriducibili distinte per a :

$$a = q_1 q_2 ... q_m,$$

$$a = r_1 r_2 ... r_n.$$

Notiamo preliminarmente che, poiché siamo in un anello euclideo e dunque in un dominio a ideali principali, un elemento irriducibile è anche primo. Allora mostriamo che $m = n$ e che

$$\forall\ 1 \leq i \leq m\ \exists\ 1 \leq k \leq m \mid q_i = r_k,$$

vale a dire la seconda fattorizzazione è uguale alla prima a meno di un riordinamento. Possiamo supporre senza perdita di generalità che $m \leq n$: proviamo la tesi per induzione su m.

Passo base $m = 1$
Allora ovviamente anche n deve essere uguale a 1, altrimenti a sarebbe contemporaneamente irriducibile e riducibile. Dunque $q_1 = a = r_1$: dunque il passo base è terminato.
Passo induttivo $m \Rightarrow m + 1$
Supponiamo che l'enunciato sia vero quando la prima fattorizzazione ha m fattori primi.
Sia ora $a = q_1 ... q_m q_{m+1} = r_1 ... r_n$. Consideriamo q_1 : ovviamente, poiché è primo, si ha che

$$q_1 | r_1 ... r_n \Rightarrow q_1 | r_1 \vee q_1 | r_2 ... r_n.$$

Nel primo caso poiché q_1 e r_1 sono entrambi primi, si ha necessariamente che $q_1 = r_1$. Dividendo entrambe le fattorizzazioni si ottiene

$$q_2 ... q_{m+1} = r_2 ... r_n,$$

poiché la fattorizzazione di sinistra ha m elementi, per ipotesi induttiva tale fattorizzazione è unica e la tesi è provata; se invece $q_1 | r_2 ... r_n$ iterando il ragionamento di prima si troverà alla fine un primo r_k tale che $q_1 = r_k$. Dividendo ambo i membri per tale elemento si ottiene

$$q_2 ... q_{m+1} = r_1 ... \hat{r_k} ... r_n.$$

Sempre per ipotesi induttiva, infine, si ha che i primi presenti nelle due fattorizzazioni sono uguali, da cui la tesi.

69. Sia $p \in \mathbb{Z}$ un numero primo dispari che sia riducibile in $\mathbb{Z}[i]$. Allora p si può scrivere come somma di due quadrati di due numeri interi.

Dimostrazione ($\star\star$)

Poiché p è riducibile esistono due non invertibili in $\mathbb{Z}[i]$ tali che $p = (a+bi)(c+di)$. In quanto non invertibili per il teorema 53.

$$a^2 + b^2 > 1$$

$$c^2 + d^2 > 1.$$

Inoltre poiché $p = \bar{p}$ si ha anche che $p = (a-bi)(c-di)$. Moltiplicando membro a membro le due relazioni otteniamo

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

Da quest'ultima si ricava immediatamente che

$$p = a^2 + b^2 = c^2 + d^2.$$

70. Sia p un primo della forma $4n+1$. Allora la congruenza

$$x^2 \equiv -1 \ (p)$$

ha soluzione in $\mathbb{Z}$.

Dimostrazione ($\star\star$)

Immediata conseguenza del teorema 17.

71. Sia p un numero primo congruo a 1 modulo 4. Allora in $\mathbb{Z}[i]$ p è riducibile ed esistono

$$a,\ b \in \mathbb{Z} \mid p = a^2 + b^2.$$

Dimostrazione ($\star$)
Dimostro che p è riducibile, il resto è immediata conseguenza del teorema 69.

Sia $x \in \mathbb{Z} \mid x^2 \equiv -1 \ (p)$, che esiste per il teorema precedente. Dunque $p | x^2 + 1 = (x+i)(x-i)$. Se p fosse irriducibile sarebbe anche primo e dunque dovrebbe dividere almeno uno fra $x+i$ e $x-i$. Ad esempio se fosse $p | x+i \Rightarrow c, d \ \in \mathbb{Z} \mid p(c+di) = x+i \Rightarrow pc = x \wedge dp = 1$ $(assurdo)$.

72. Sia p un primo congruo a 3 modulo 4. Allora p non si può scrivere come somma di due quadrati ed è dunque irriducibile in $\mathbb{Z}[i]$.

Dimostrazione ($\star$)

Supponiamo che $p = a^2 + b^2$. Poiché p è dispari, deve essere che uno fra a e b è pari e l'altro è dispari, ma in questo caso $a^2 + b^2 \equiv 1 \equiv 3 \ (4)$ (assurdo).

73. In $\mathbb{Z}[i]$ un elemento p è irriducibile (a meno di associati) se e solo se è un primo congruo a 3 modulo 4 oppure se $gr(p)$ è un primo di $\mathbb{Z}$.

Dimostrazione ($\star\star$)

($\Rightarrow$) Sia $p \in \mathbb{Z}[i]$ irriducibile (e dunque primo). Dunque $p|p\bar{p} = gr(p) = q_1...q_n$, dove $q_1...q_n$ è la fattorizzazione di $gr(p)$ (i primi possono essere ripetuti). Allora, poiché p è primo, deve essere che esiste un primo q_k tale che $p|q_k$, vale a dire $q_k = pM$ per un certo $M \in \mathbb{Z}[i]$. Se M è invertibile, q_k e p sono associati, e dunque q_k è irriducibile ed è dunque un primo congruo a 3 modulo 4. Se invece M non è invertibile si passa ai quadrati delle norme e si ottiene che

$$q_k^2 = gr(p)gr(M) \Rightarrow q_k = gr(p) \wedge q_k = gr(M).$$

($\Leftarrow$) Se p è un primo congruo a 3 modulo 4 si conclude subito grazie al teorema 72. Se invece $gr(p) = N$ con N primo

$$p = \alpha\beta \Rightarrow N = gr(\alpha)gr(\beta).$$

Dunque uno fra $gr(\alpha)$ e $gr(\beta)$ deve essere 1, ovvero p è irriducibile.

74. **(Esercizio 11.34)** Sia $(R, +, \cdot)$ un dominio a ideali principali. Allora un suo ideale $I \neq \{0\}$ è primo se e solo se è massimale.

Dimostrazione ($\star$)

($\Rightarrow$) Sia I un ideale primo. Allora, poiché siamo in un dominio a ideali principali, esso è generato da un elemento γ. Allora γ deve essere primo e dunque è irriducibile per il teorema 65: allora l'ideale (γ)=(I) è massimale per il teorema 66
($\Leftarrow$) Immediato per il teorema 50.

75. **(Esercizio 11.40)** Sia p un primo congruo a 1 modulo 4. Allora si può scrivere in modo unico come somma di due quadrati.

Dimostrazione ($\star\star$)

Supponiamo che esistano due modi di scrivere p come somma di due quadrati,

$$p = a^2 + b^2$$

$$p = c^2 + d^2.$$

Allora

$$p = (a + bi)(a - bi)$$

$$p = (c + di)(c - di).$$

Sappiamo che si tratta di fattorizzazioni in irriducibili e che $(\mathbb{Z}[i], +, \cdot)$ è un dominio a fattorizzazione unica, e dunque deve essere che $c + di$ e $c - di$ sono associati a $a + bi$ e $a - bi$.

76. Sia $(K,+,\cdot)$ un campo e $f(x) \in K[x]$ irriducibile di grado ≥ 2. Allora è sempre possibile trovare un campo $(E,+,\cdot)$ che estende il precedente e tale che il polinomio $f(x)$ ha almeno una radice in E.

Dimostrazione $(\star\star)$

Sia $f(x) = a_n x^n + ... + a_1 x + a_0$. Notiamo che poiché $f(x)$ è irriducibile, l'ideale $(f(x)) = I$ è massimale e dunque $K[x]/I = E$ è un campo. Notiamo che esiste un sottocampo di E isomorfo a K (si veda la proiezione al quoziente), e pertanto è possibile vedere $f(x)$ anche come polinomio in $E[x]$ Inoltre si verifica che una radice del polinomio $f(x)$ in E è $x + I$:

$$f(x+I) = a_n(x+I)^n + ...a_1(x+I) + a_0 = f(x) + I = 0 + I.$$

77. Sia $(K,+,\cdot)$ un campo e $f(x) \in K[x]$ irriducibile. Allora il campo $(K[x]/(f(x)),+,\cdot) = (E,+,\cdot)$ è uno spazio vettoriale su $(K,+,\cdot)$ di dimensione $deg(f(x)) = n$.

Dimostrazione $(\star)$

La prima asserzione è banale: infatti per il teorema precedente in $(E,+,\cdot)$ c'è un sottocampo isomorfo a $(K,+,\cdot)$, e dunque non solo è ben definita la somma ma anche il prodotto per gli scalari (gli elementi di K). Consideriamo il seguente insieme:

$$1 + (f(x)), x + (f(x)), x^2 + (f(x)), ..., x^{n-1} + (f(x))$$

È un insieme di generatori: un generico elemento di E è della forma

$$a_{n-1}x^{n-1} + ... + a_1 x + a_0 + (f(x)) = a_0(1 + (f(x)) + a_1(x + (f(x)) + ... + a_{n-1}(x^{n-1} + (f(x))).$$

Inoltre essi sono evidentemente linearmente indipendenti e dunque abbiamo una base di E con $n = deg(f(x))$ elementi.

78. Siano $(K, +\cdot)$ e $(L, +, \cdot)$ due campi tali che $K \subseteq L$, e sia $\alpha \in L$. Allora $(K[\alpha], +, \cdot)$ è un campo se e solo se esiste un polinomio $f(x) \in K[x]$ diverso dal polinomio nullo tale che $f(\alpha) = 0$.

Dimostrazione ($\star\star$)

Consideriamo l'omomorfismo di valutazione

$$\psi : K[x] \to L$$

$$p(x) \mapsto p(\alpha)$$

e studiamone il nucleo. Notiamo preliminarmente che $(K[x], +, \cdot)$ è un anello euclideo, e in particolare un dominio a ideali principali, pertanto, visto che $Ker(\psi)$ è un ideale, esso sarà generato da un unico elemento. Si hanno due possibilità:

- $Ker(\psi) = \{0\}$
  Ciò vuol dire che non esiste un polinomio in $K[x]$ diverso da quello nullo che si annulli in α. Per il primo teorema di omomorfismo si ha allora

  $$K[x] \cong K[\alpha].$$

  Poiché $K[x]$ non è un campo, non lo è nemmeno $K[\alpha]$;
- $Ker(\psi) = (f(x)),\ f(x) \neq 0$
  Ciò vuol dire che esiste un polinomio in $K[x]$ diverso da quello nullo che si annulla in α.
  Allora $f(x)$ è irriducibile: infatti se $f(x) = p(x)q(x)$ allora si avrebbe che $f(\alpha) = p(\alpha)q(\alpha) = 0$. Allora deve essere $p(\alpha) = 0$ o $q(\alpha) = 0$. Se tale fattorizzazione fosse non banale i gradi di $p(x),\ q(x)$ sarebbero minori di quello di $f(x)$, il che è assurdo in quanto $f(x)$ è generatore dell'ideale, dunque abbiamo la tesi. Ma allora per il teorema 66. l'ideale $(f(x)) = Ker(\psi)$ è massimale e per il teorema 49.

  $$K[x]/(f(x)) = K[x]/Ker(\psi)$$

  è un campo.
  Inoltre per il primo teorema di omomorfismo $K[x]/(f(x)) \cong Im(\psi) = K[\alpha]$, e dunque $(K[\alpha], +, \cdot)$ è un campo. $K \subseteq K[\alpha]$ e $\alpha \in K[\alpha]$ e dunque $K(\alpha) \subseteq K[\alpha]$, inoltre è immediato notare che tutti i polinomi in α appartengono a $K(\alpha)$, e dunque vale anche $K[\alpha] \subseteq K(\alpha)$: ciò implica

  $$K[\alpha] = K(\alpha).$$

79. Siano $(K,+,\cdot)$ e $(L,+,\cdot)$ due campi tali che $K \subseteq L$ e sia $f(x)$ un polinomio irriducibile in $K[x]$ che ammette due radici distinte in L, α e β. Allora esiste un isomorfismo

$$\theta : K[\alpha] \to K[\beta]$$

fra i campi $K[\alpha]$ e $K[\beta]$ tale che

$$\theta(\alpha) = \beta$$
$$\theta|_K = Id_K.$$

Dimostrazione $(\star\star)$

Per il teorema 78. abbiamo che

$$K[x]/(f(x)) \cong K[\alpha] \quad e \quad K[x]/(f(x)) \cong K[\beta].$$

Dunque

$$K[\alpha] \cong K[x]/(f(x)) \cong K[\beta]$$

Abbiamo i due seguenti isomorfismi:

$$\psi_\alpha^{-1} : K[\alpha] \to K[x]/(f(x))$$
$$p(\alpha) \mapsto p(x) + (f(x))$$
$$\psi_\beta : K[x]/(f(x)) \to K[\beta]$$
$$p(x) + (f(x)) \mapsto p(\alpha)$$

che sono rispettivamente l'inverso dell'omomorfismo di valutazione in α e l'omomorfismo di valutazione in β. Osserviamo che

$$\psi_\beta \circ \psi_\alpha^{-1} : \ K[\alpha] \to K[\beta]$$
$$p(\alpha) \mapsto p(\beta)$$

verifica le condizioni richieste:

$$(\psi_\beta \circ \psi_\alpha^{-1})(\alpha) = \psi_\beta(x + (f(x))) = \beta$$

Inoltre sia $m \in K$.

$$(\psi_\beta \circ \psi_\alpha^{-1})(m) = \psi_\beta(m + (f(x))) = m.$$

80. Sia $(K, +, \cdot)$ un campo e sia $f(x) \in K[x]$ un polinomio di grado $n \geq 0$. Allora esiste un campo $(E, +, \cdot)$ tale che $K \subseteq E$ ed esistono n elementi $a_1, ..., a_n \in E$ tali che $f(x)$ si fattorizza in $E[x]$ nel seguente modo:

$$f(x) = \lambda(x - a_1)...(x - a_n),$$

dove $\lambda \in E$ è una costante.

Dimostrazione $(\star)$

Si procede per induzione sul grado del polinomio.
Passo base $deg(f) = 0$
Ovvio.
Passo induttivo $deg(f) \Rightarrow deg(f) + 1$
Supponiamo che
$deg(f) = n + 1$ e sia $f_1(x)$ un suo fattore irriducibile. Allora, per il teorema 76. in $K[x]/(f_1(x)) = F$ il polinomio $f(x)$ ha una radice, $x + (f_1(x))$. Chiamiamola a_1. Allora abbiamo in F una fattorizzazione non banale:

$$f(x) = (x - a_1)g(x),$$

dove $g(x)$ è un polinomio di grado n. Ma allora per ipotesi induttiva esiste un campo $(E, +, \cdot)$ che estende i precedenti ed esistono $a_2, ..., a_n$ in E per cui $g(x)$ ha la seguente fattorizzazione:

$$g(x) = \lambda(x - a_2)...(x - a_n),$$

da cui si rimonta la fattorizzazione di $f(x)$:

$$f(x) = \lambda(x - a_1)(x - a_2)...(x - a_n).$$

81. **(Teorema delle torri d'estensione)** Siano $K \subseteq L,\ F \subseteq K$ estensioni finite di campi. Allora:

$$[L : F] = [L : K][K : F].$$

Dimostrazione ($\star\star$)

Supponiamo che $[L : K] = m,\ [K : F] = n$. Allora una base di L come spazio vettoriale su K è composta da m elementi $\mathbf{B} = \{\mathbf{v_1}, ...\mathbf{v_m}\}$, mentre una base di K come spazio vettoriale su F è composta da n elementi $\mathbf{C} = \{\mathbf{w_1}, ..., \mathbf{w_n}\}$.. Consideriamo un generico elemento v di L, esso si potrà dunque esprimere come combinazione lineare degli elementi della base $\mathbf{B}$:

$$v = a_1v_1 + ...a_mv_m.$$

I coefficienti $a_1, ..., a_m$ sono elementi di K, e in quanto tali essi si potrano scrivere come combinazione lineare degli elementi della base $\mathbf{C}$.

$$a_i = b_{i1}w_1 + ... + b_{im}w_m.$$

In definitiva:

$$v = \sum_{\substack{i=1,...,n \\ j=1,...,m}} b_{ij}w_jv_i.$$

E' dunque evidente che gli elementi della forma v_iw_j generano tutto L come spazio vettoriale su F. In tutto sono mn: per avere la tesi basta provare che sono linearmente indipendenti. Dalla relazione

$$\sum_{\substack{i=1,...,n \\ j=1,...,m}} b_{ij}w_jv_i = 0 \Rightarrow \sum_{\substack{i=1,...,n \\ j=1,...,m}} (b_{ij}w_j)v_i = 0,$$

poiché $v_1, ..., v_n$ è una base, si ricava che, per ogni i:

$$\sum_{j=1}^{m} b_{ij}w_j = 0.$$

Ma poiché anche $w_1, ..., w_m$ è una base si ricava che per ogni i, j

$$b_{ij} = 0,$$

da cui la tesi.

82. Sia L estensione finita di F e $F \subseteq K \subseteq L$. Allora K è estensione finita di F, L è estensione finita di K e

$$[L : F] = [L : K][K : F].$$

Dimostrazione ($\star\star$)

Poiché per ipotesi L è un'estensione finita di F e K è un suo sottospazio, allora anche quest'ultimo sarà un'estensione finita di F. Inoltre poiché una base di L come spazio vettoriale su F è un insieme finito di generatori di L su K, anche la seconda asserzione è dimostrata. L'ultima è diretta conseguenza del teorema precedente.

83. Sia $F \subseteq K$ un'estensione di campi e sia $\alpha \in K$. Allora α è algebrico su F se e solo se $F(\alpha)$ è un'estensione finita di F.

Dimostrazione ($\star\star$)

($\Rightarrow$) Se α è algebrico su F con polinomio minimo $f(x)$ su F, allora

$$F[x]/(f(x)) \cong F[\alpha] = F(\alpha)$$

e per il teorema 77. $F(\alpha)$ è un estensione finita di F.

($\Leftarrow$) Se $[F(\alpha) : F] = p$, gli elementi

$$1, \alpha, ..., \alpha^p,$$

sono linearmente dipendenti (sono infatti $p+1$), dunque esistono $a_0, ..., a_p$ non tutti nulli per cui:

$$a_0 + a_1\alpha + ... + a_p\alpha^p = 0$$

e allora α è radice del polinomio $p(x) = a_0 + a_1x + ... + a_px^p$ e dunque α è algebrico su F.

84. Sia $F \subseteq L$ un'estensione di campi e siano $\alpha, \beta \in L$ algebrici su F di grado m e n, rispettivamente. Allora sono algebrici su F anche $a \pm b, ab, \frac{a}{b} (se\ b \neq 0)$, di grado $\leq mn$.

Dimostrazione ($\star\star$)

Abbiamo che $[F(a) : F] = m$ e $[F(b) : F] = n$. Notiamo che, poiché b è algebrico su F, lo sarà anche su $F(a)$.
Tuttavia può darsi che il suo polinomio minimo $f(x)$ su F sia riducibile su $F(a)$: in tal caso il suo polinomio minimo su $F(a)$ sarebbe uno dei fattori irriducibili di $f(x)$. Dunque $[F(a)(b) : F(a)] \leq n$. Abbiamo che $F \subseteq F(a) \subseteq F(a)(b)$ sono estensioni finite. Per il teorema delle torri d'estensione allora:

$$[F(a)(b) : F] = [F(a)(b) : F(a)][F(a) : F] \leq mn.$$

Infine notiamo che $F(a)(b)$ è un campo che contiene a e b, e dunque anche $a \pm b, ab, \frac{a}{b} (se\ b \neq 0)$, e dunque tali elementi devono essere algebrici in base al teorema 83. poiché ad esempio,

$$F \subseteq F(a \pm b),\ F(ab),\ F\left(\frac{a}{b}\right) \subseteq F(a)(b).$$

85. **(Esercizio 13.14)** Sia $(\mathbf{A}, +, \cdot)$ il campo dei numeri algebrici su $\mathbb{Q}$. Allora $[\mathbf{A} : \mathbb{Q}] = \infty$.

Dimostrazione ($\star$)

Supponiamo per assurdo che tale estensione sia finita di grado n. Consideriamo il numero $2^{\frac{1}{n+1}}$. Esso è algebrico su $\mathbb{Q}$, in quanto radice del polinomio $x^{n+1} - 2 \in \mathbb{Q}[x]$. Tale polinomio è irriducibile su Q per il criterio di Eisenstein fatto ad Esercitazioni, e dunque $\mathbb{Q}[x]/(x^{n+1} - 2)$ è un'estensione di $\mathbb{Q}$ di grado $n+1$. Poiché abbiamo che $\mathbb{Q} \subseteq \mathbb{Q}(2^{\frac{1}{n+1}}) \subseteq \mathbf{A}$ sono estensioni finite dovrebbe valere, per il teorema delle torri d'estensione:

$$n = [\mathbf{A} : \mathbb{Q}] = [\mathbf{A} : \mathbb{Q}(2^{\frac{1}{n+1}})][\mathbb{Q}(2^{\frac{1}{n+1}}) : \mathbb{Q}] = [\mathbf{A} : \mathbb{Q}(2^{\frac{1}{n+1}})](n+1) \Rightarrow n+1 \mid n,$$

assurdo.

86. Sia $(F, +, \cdot)$ un campo e sia $f(x) \in F[x]$ un polinomio non nullo di grado n. Sia $(E, +, \cdot)$ un campo di spezzamento di $f(x)$ su F. Allora $[E : F] \leq n!$.

Dimostrazione $(\star)$

Siano $a_1, ..., a_m$ le radici distinte di $f(x)$ in E $(m \leq n)$. Dunque $E = F(a_1, ..., a_m)$.

Consideriamo $F \subseteq F(a_1)$: abbiamo che

$$[F(a_1) : F] \leq n,$$

poiché il polinomio minimo di a_1 in $F[x]$ è uno dei fattori irriducibili di $f(x)$ e pertanto ha grado $\leq n$. Consideriamo ora $F \subseteq F(a_1) \subseteq F(a_1, a_2)$: per il teorema delle torri d'estensione

$$[F(a_1, a_2) : F] = [F(a_1, a_2) : F(a_1)][F(a_1) : F] \leq (n-1)n.$$

Infatti abbiamo che in $F(a_1)$ il polinomio f(x) si fattorizza sicuramente come $f(x) = (x - a_1)g(x)$, dunque il polinomio minimo di a_2 su $F(a_1)$ è uno degli irriducibili con cui si scompone $g(x)$, che ha grado $n - 1$. In n passi si ottiene la tesi.

87. Siano $(F, +\cdot)$ e $(F', \star, \times)$ due campi, e siano $\phi : F \to F'$ un isomorfismo e $\tilde{\phi} : F[x] \to F'[x]$ l'isomorfismo di anelli associato così definito:

$$\tilde{\phi}(a_n x^n + ...a_1 x + a_0) = \phi(a_n)x^n + ... + \phi(a_1)x + \phi(a_0).$$

Siano $F \subseteq L$ e $F' \subseteq L'$ due estensioni di campi e sia $\alpha \in L$ algebrico su F con polinomio minimo $p(x)$. Supponiamo che esista in L' una radice α' di $\tilde{\phi}f(x)$. Allora esiste un isomorfismo $\phi' : F(\alpha) \to F'(\alpha')$ tale che $\phi(\alpha) = \alpha'$ e $\phi'|_F = \phi$.

Dimostrazione $(\star\star\star)$

Visto che $p(x)$ è irriducibile e $\tilde{\phi}$ un isomorfismo, sarà irriducibile anche $\tilde{\phi}(p(x))$. Dunque $(F'[x]/(\tilde{\phi}(p(x))), +, \cdot)$ è un campo. Per il teorema 79. abbiamo i due seguenti isomorfismi:

$$\psi_\alpha^{-1} : F[\alpha] \to F[x]/(p(x))$$
$$f(\alpha) \mapsto f(x) + (p(x))$$
$$\psi_{\alpha'} : F'[x]/(\tilde{\phi}(p(x))) \to F'[\alpha']$$
$$f(x) + (\tilde{\phi}(p(x))) \mapsto f(\alpha')$$

Cerco un isomorfismo fra $F[x]/(p(x))$ e $F'[x]/(\tilde{\phi}(p(x))$, una volta trovato basterà comporre isomorfismi per trovare quello cercato.
Sfruttiamo il primo teorema di omomorfismo: dato

$$F[x] \to^{\tilde{\phi}} F'[x] \to^{\pi} F'[x]/(\tilde{\phi}(p(x)),$$

dove π è l'omomorfismo di proiezione, consideriamo l'omomorfismo

$$\theta = \pi \circ \tilde{\phi}.$$

Si nota immediatamente che $Ker(\theta) = (p(x))$. Dunque per il primo teorema di omomorfismo esiste un isomorfismo θ',

$$\theta' : \ F[x]/(p(x)) \to F'[x]/(\tilde{\phi}(p(x))$$
$$x + (p(x)) \mapsto \phi(x) + (\tilde{\phi}(p(x)).$$

Riassumendo abbiamo:

$$F[\alpha] \to^{\psi_\alpha^{-1}} F[x]/(p(x)) \to^{\theta'} F'[x]/(\tilde{\phi}(p(x)) \to^{\psi_{\alpha'}} F'[\alpha'].$$

L'isomorfismo cercato è dunque:

$$\phi' = \psi_{\alpha'} \circ \theta' \circ \psi_\alpha^{-1},$$

infatti:

$$\psi_{\alpha'} \circ \theta' \circ \psi_\alpha^{-1}(\alpha) = \psi_{\alpha'} \circ \theta'(x + (p(x))) = \psi_{\alpha'}(x\phi(x) + (\tilde{\phi}(p(x)))) = \alpha',$$

e preso $k \in F$

$$\psi_{\alpha'} \circ \theta' \circ \psi_\alpha^{-1}(k) = \psi_{\alpha'} \circ \theta'(k + (p(x))) = \psi_{\alpha'}(\phi(k) + (\tilde{\phi}(p(x)))) = \phi(k).$$

88. Siano $(K,+,\cdot)$ e $(K',\star,\times)$ due campi, e sia $\phi : K \to K'$ un isomorfismo. Sia $\tilde{\phi} : K[x] \to K'[x]$ l'isomorfismo di anelli associato, definito esattamente come nel teorema precedente. Dato un polinomio non nullo $f(x) \in K[x]$ sia $(E,+,\cdot)$ un suo campo di spezzamento su $(F,+,\cdot)$, e sia $(E',\star,\times)$ un campo di spezzamento su $(F',\star,\times)$ di $\tilde{\phi}(f(x))$. Allora esiste un isomorfismo

$$\phi' : E \to E'$$

tale che

$$\phi'|_F = \phi.$$

Dimostrazione $(\star\star\star)$

Procediamo per induzione sul grado di $f(x)$.
Il caso $deg(f) = 0$ è banalmente vero. scegliamo come base $deg(f) = 1$.
Passo base $deg(f) = 1$
In tal caso si ha che $E = K$, $E' = K'$ e basta porre $\phi' = \phi$ per avere la tesi.
Passo induttivo $deg(f) \Rightarrow deg(f) + 1$
Sia $g(x)$ un fattore irriducibile di $f(x)$. Sia dunque $a \in E$ una radice di $g(x)$ e sia $a' \in E'$ una radice di $\tilde{\phi}(g(x))$ (che è ancora un irriducibile). Allora per il teorema precedente esiste un isomorfismo

$$\theta : K(a) \to K(a')$$

tale che $\theta(a) = a'$ e $\theta|_K = \phi$.
A tale isomorfismo è associato il seguente omomorfismo di anelli

$$\tilde{\theta} : K(a)[x] \to K(a')[x].$$

Poiché $\tilde{\theta}(x-a) = x - a'$ il polinomio $f(x) = (x-a)\bar{f}(x) \in K(a)[x]$ viene mandato da $\tilde{\theta}$ in $\tilde{\theta}(f(x)) = (x-a')\tilde{\theta}(\bar{f}(x)) \in K'(a')[x]$. Sappiamo che:

- C'è un isomorfismo $\phi : K(a) \to K'(a')$;
- Il polinomio $\bar{f}(x)$ ha grado $deg(f)$;
- $(E,+,\cdot)$ è un campo di spezzamento per $\bar{f}(x)$ su $K(a)$;
- $(E',\star,\times)$ è un campo di spezzamento per $\tilde{\theta}(\bar{f}(x))$ su $K'(a')$. Per ipotesi induttiva allora esiste un isomorfismo $\phi' : E \to E'$ tale che $\phi'|_{K(a)} = \theta = \phi$.

89. Sia p un numero primo, e sia $(K,+,\cdot)$ un campo di caratteristica p. La funzione

$$F : K \to K$$

$$a \mapsto a^p$$

è un omomorfismo iniettivo.

Dimostrazione $(\star)$

Verifichiamolo direttamente:

- $F(1) = 1^p = 1$;

- $F(ab) = (ab)^p = (a^p)(b^p) = F(a)F(b)$;

- $F(a+b) = (a+b)^p = a^p + b^p = F(a) + F(b)$.

Inoltre notiamo che il nucleo di questo omomorfismo è proprio, essendo $F(1) = 1$. Ma allora, poiché K è un campo, l'unica possibilità è che $Ker(F) = (0) = \{0\}$.

90. Sia $(K, +, \cdot)$ un campo, e sia $\psi : K \to K$ un omomorfismo. Allora, detto

$$Fix_\psi = \{k \in K \mid \psi(k) = k\},$$

$(Fix_\psi, +, \cdot)$ é un sottocampo di $(K, +, \cdot)$.

Dimostrazione $(\star)$

Mostro prima che è un sottoanello e poi che è un sottocampo.

- $\psi(0) = 0 \Rightarrow 0 \in Fix_\psi$;
- $\forall x \in Fix_\psi,\ \psi(-x) = -\psi(x) = -x \Rightarrow -x \in Fix_\psi$;
- $\forall x, y \in Fix_\psi,\ \psi(x + y) = \psi(x) + \psi(y) = x + y \Rightarrow x + y \in Fix_\psi$;
- $\forall x, y \in Fix_\psi,\ \psi(xy) = \psi(x)\psi(y) = xy \Rightarrow xy \in Fix_\psi$;
- $\psi(1) = 1 \Rightarrow 1 \in Fix_\psi$;
- $\forall x \in Fix_\psi,\ \psi(x^{-1}) = \psi(x)^{-1} = x^{-1} \Rightarrow x^{-1} \in Fix_\psi$.

91. Sia $(K, +, \cdot)$ un campo finito. Allora la sua caratteristica è un numero primo p.

Dimostrazione $(\star\star)$

Consideriamo l' (unico) omomorfismo di anelli con unità

$$\phi : \mathbb{Z} \to K.$$

In particolare per il primo teorema di omomorfismo

$$\mathbb{Z}/Ker(\phi) \cong Im(\phi).$$

Poiché $(\mathbb{Z}, +, \cdot)$ è un dominio a ideali principali, esiste $d \in \mathbb{Z} \mid Ker(\phi) = (d)$. Inoltre $Im(\phi)$ è un sottoanello di K, e in particolare un dominio: allora per il teorema 48. l'ideale (d) è primo, vale a dire d è primo oppure $d = 0$. Se si avesse $Ker(\phi) = (0)$, avremmo che $\mathbb{Z} \cong Im(\phi)$ che è assurdo in quanto abbiamo supposto K finito, e dunque un suo sottoanello non può essere infinito. Dunque la caratteristica di K è necessariamente un numero primo.

92. **Teorema di classificazione dei campi finiti** Ogni campo finito ha cardinalità p^n, dove p è un numero primo e n è un intero positivo. Inoltre per ogni scelta di un numero primo p e per ogni intero positivo n esiste un campo finito di cardinalità p^n unico a meno di isomorfismi.

Dimostrazione $(\star\star\star)$

Per il teorema precedente, ogni campo finito $(K+,\cdot)$ ha caratteristica p, dove p è un numero primo, dunque ha un sottocampo isomorfo a $(\mathbb{Z}_p,+,\cdot)$. E' immediato notare che K è un'estensione finita di tale sottocampo, per cui è possibile vederlo come spazio vettoriale su $\mathbb{Z}_p$. Sia n il grado di tale estensione, ciò vuol dire che esiste una base di n elementi e ogni vettore di K si può scrivere nella forma:

$$v = a_1x_1 + ...a_nx_n.$$

con i coefficienti $a_1, ..., a_n \in \mathbb{Z}_p$. Poiché per ogni coefficiente abbiamo in tutto p scelte le possibili combinazioni sono allora p^n.

Siano fissati p numero primo e n intero positivo e consideriamo un campo di spezzamento R del polinomio $f(x) = x^{p^n} - x$ su $\mathbb{Z}_p$ (in particolare allora il campo di spezzamento considerato ha caratteristica p). Consideriamo la sua derivata $f'(x)$: si ha che

$$f'(x) = p^m x^{p^n-1} - 1 = -1,$$

dunque per un teorema fatto ad Esercitazioni poiché non ha radici in comune con $f(x)$ se ne deduce che le radici di $f(x)$ devono essere tutte distinte.Poiché $deg(f) = p^n$, tale polinomio ha p^n radici. Sia ora $L = \{x \in R \mid F^n(x) = x\}$, dove $F(x)$ è l'omomorfismo di Frobenius. E' immediato notare che i suoi elementi sono proprio le radici di $f(x)$. Infine per il teorema 90. questo è un sottocampo di R con p^n elementi.

93. Sia $(\mathbb{F}_{p^n}, +, \cdot)$ un campo finito. Allora il gruppo $(\mathbb{F}^*_{p^n}, \cdot)$ è ciclico.

Dimostrazione $(\star\star\star\star)$

Ovviamente $|\mathbb{F}^*_{p^n}| = p^n - 1$. Bisogna dunque trovare un elemento di ordine $p^n - 1$.

— **Lemma 1** — Sia d un divisore di $p^n - 1$. Allora esistono d radici distinte del polinomio $x^d - 1$ in $\mathbb{F}^*_{p^n}$.

Sia $p^n - 1 = dm$. Allora

$$x^{p^n-1} - 1 = x^{dm} - 1 = (x^d)^m - 1 = (x^d - 1)(x^{d(m-1)} + ... + x^d + 1).$$

Dunque tutte le radici di $x^d - 1$ sono anche radici di $x^{p^n-1} - 1$, che sono tutti gli elementi di $\mathbb{F}^*_{p^n}$. Poiché in $\mathbb{F}_{p^n}$ il polinomio $x^{p^n-1} - 1$ si spezza in fattori lineari, lo stesso vale per $x^d - 1$.

— Lemma 2 — Siano q un numero primo e r un intero positivo tali che $q^r \mid p^n - 1$. Allora esiste in $\mathbb{F}^*_{p^n}$ un elemento di ordine q^r.

Per il punto precedente, esistono in $\mathbb{F}^*_{p^n}$ esattamente q^r radici distinte del polinomio $x^{q^r} - 1$. Sempre per il punto precedente, esistono in $\mathbb{F}^*_{p^n}$ esattamente q^{r-1} radici distinte del polinomio $x^{q^{r-1}} - 1$. Allora esiste sicuramente una radice β del primo polinomio che non è radice del secondo polinomio con ordine uguale a q^r. Se infatti l'ordine fosse minore di q^r avremmo che deve dividere q^r, e dunque è del tipo q^s, con $s < r$. Ma allora si avrebbe che β è radice del polinomio $x^{q^{r-1}} - 1$, assurdo.

— Lemma 3 — Sia $(G, \star)$ un gruppo abeliano e siano $\beta_1, ..., \beta_m$ dei suoi elementi, di ordine rispettivamente $a_1, ..., a_m$ a due a due primi fra loro. Allora l'ordine del prodotto $\beta_1...\beta_m$ è $a_1...a_m$.

Sicuramente si ha che

$$(\beta_1...\beta_m)^{a_1...a_m} = 1.$$

Se per assurdo l'ordine fosse un divisore proprio di $a_1...a_m$, ovvero un elemento $\nu < a_1...a_m$, avremmo che, visto che gli a_i sono primi fra loro, esiste un a_i che non divide ν. Supponiamo senza perdita di generalità che tale elemento sia β_1. Dunque $\beta_1^\nu \neq 1$. Sfruttiamo la seguente relazione:

$$(\beta_1...\beta_m)^\nu = 1 = \beta_1^\nu(\beta_2...\beta_m)^\nu \Rightarrow \beta_1^\nu = (\beta_2...\beta_m)^{-\nu}.$$

Ora, poiché β_1 ha ordine a_1, l'elemento β_1^ν ha ordine che è un divisore di a_1. Per motivi analoghi l'elemento $\beta_2...\beta_m$ ha ordine che è divisore di $a_2...a_m$. Per l'uguaglianza ottenuta i due ordini devono essere uguali, e dunque si sta cercando un divisore comune a a_1 e a $a_2...a_m$. Ma poiché a_1 e $a_2...a_m$ sono primi fra loro, necessariamente tale ordine deve essere 1, da cui si ricava

$$(\beta^\nu)^1 = \beta^\nu = 1,$$

assurdo.

Sia ora $p^n - 1 = q_1^{r_1}...q_m^{r_m}$ la fattorizzazione in primi di $p^n - 1$: allora per il secondo lemma per ogni $1 \leq i \leq m$ esiste un elemento $\beta_i \in \mathbb{F}_{p^n}$ di ordine $q_i^{r_i}$. Dunque per il lemma 3 l'elemento $\beta_1...\beta_m$ ha ordine $q_1^{r_1}...q_m^{r_m} = p^n - 1$. Ciò conclude la dimostrazione del teorema.

94. Consideriamo il campo finito $(\mathbb{F}_{p^n}, +, \cdot)$ e sia α un generatore del gruppo $(\mathbb{F}^*_{p^n}, \cdot)$. Sia $p(x)$ il polinomio minimo di α su $\mathbb{Z}_p[x]$. Allora

$$\mathbb{F}_{p^n} \cong \mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[x]/(p(x)).$$

Dimostrazione ($\star\star$)

Il secondo isomorfismo è vero per un teorema precedente. Per il primo basta notare che $\mathbb{Z}_p[\alpha]$ è un sottoinsieme di $\mathbb{F}_{p^n}$ che contiene lo 0 e tutte le potenze di α, dunque coincide con $\mathbb{F}_{p^n}$.

95. Per ogni primo p e ogni intero positivo n esiste un polinomio irriducibile di grado n in $\mathbb{Z}_p[x]$.

Dimostrazione ($\star\star$)

Consideriamo un generatore α di $\mathbb{F}^*_{p^n}$ e sia $f(x)$ il suo polinomio minimo. Per il teorema precedente, si ha che

$$\mathbb{F}_{p^n} \cong \mathbb{Z}_p[x]/(f(x)).$$

Si ha che $|\mathbb{F}_{p^n}| = p^n$, dunque $deg(f) = n$.

96. Dato un numero primo p e un intero positivo n, il polinomio $x^{p^n} - x$ è il prodotto di tutti i polinomi monici irriducibili in $\mathbb{Z}_p[x]$ di grado $d|n$.

Dimostrazione ($\star\star\star\star$)

Consideriamo un polinomio $g(x)$ irriducibile di grado d divisore di n, mostriamo che allora $g(x)$ divide $x^{p^n} - x$. Consideriamo il campo

$$\mathbb{Z}_p[x]/(g(x)),$$

esso è un campo con p^d elementi, dunque è isomorfo a $(\mathbb{F}_{p^d}, +, \cdot)$ i cui elementi sono tutte le radici del polinomio $x^{p^d} - x$. Inoltre in tale campo c'è, per il teorema 69, almeno una radice α di $g(x)$. Poiché $d \mid n$ esiste un intero s tale che $n = ds$. Allora

$$\alpha^{p^n} = \alpha^{p^{ds}} = (\alpha^{p^d})^{p^{(s-1)d}} = \alpha^{p^{(s-1)d}}.$$

Per induzione su s si prova che

$$\alpha^{p^n} = \alpha.$$

Poiché $g(x)$ e $x^{p^n} - x$ hanno una radice in comune $\alpha \in \mathbb{Z}_p[x]/(g(x))$ sicuramente il loro massimo comun divisore non può essere 1, in quanto per il teorema di Ruffini fatto ad Esercitazioni sono entrambi divisi da $x - \alpha$. Ma allora, poiché $g(x)$ è irriducibile, deve essere

$$(g(x), x^{p^n} - x) = g(x),$$

dunque $g(x) \mid x^{p^n} - x$.

Ora sappiamo che nella fattorizzazione di $x^{p^n} - x$ compaiono tutti i polinomi $q(x)$ di grado $d|n$. Tuttavia, vogliamo dimostrare che non ci sono altri fattori, dunque quanto detto finora non basta: se dimostriamo anche il viceversa del passo precedente si ha la tesi. Dunque vogliamo dimostrare che se un polinomio irriducibile r(x) divide $x^{p^n} - x$, il suo grado d divide n.
Considero il campo $(\mathbb{Z}_p[x]/(r(x)), +, \cdot)$. Esso è un campo con p^d elementi, e dunque isomorfo a $(\mathbb{F}_{p^d}, +, \cdot)$. Prendiamo il campo $(\mathbb{F}_{p^n}, +, \cdot)$: i suoi elementi sono tutte e sole le radici del polinomio $x^{p^n} - x$; poiché per ipotesi $r(x)$ divide tale polinomio, tra questi elementi ci sono tutte le radici di $r(x)$, sia β una di queste. Il polinomio minimo di β su $(\mathbb{Z}_p, +, \cdot)$ è proprio $r(x)$, in quanto irriducibile, e dunque esiste un isomorfismo

$$\phi : (\mathbb{Z}_p(\beta) \to (\mathbb{Z}_p[x]/(r(x)), +, \cdot).$$

Se ne deduce che

$$(\mathbb{Z}_p(\beta), +, \cdot)$$

è un sottocampo di $(\mathbb{F}_{p^n}, +, \cdot)$ isomorfo a $(\mathbb{F}_{p^d}, +, \cdot)$. Consideriamo un generatore γ del gruppo ciclico $(\mathbb{F}_{p^n}, \cdot)$ e il sottocampo $(\mathbb{Z}_p(\beta, \gamma), +, \cdot)$. Visto e considerato che l'insieme delle potenze di γ è proprio $\mathbb{F}^*_{p^n}$, si ha che i campi

$$(\mathbb{F}_{p^n}, +, \cdot)$$

$$(\mathbb{Z}_p(\beta, \gamma), +, \cdot)$$

coincidono. Sia $g(x)$ il polinomio minimo di γ su $(\mathbb{Z}_p(\beta), +, \cdot)$ di grado s e consideriamo la seguente catena di estensioni finite:

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p(\beta) \subseteq \mathbb{Z}_p(\beta, \gamma).$$

Per il teorema delle torri d'estensione si ha allora:

$$n = [\mathbb{F}_{p^n} : \mathbb{Z}_p] = [\mathbb{Z}_p(\beta, \gamma) : \mathbb{Z}_p] = [\mathbb{Z}_p(\beta, \gamma) : \mathbb{Z}_p(\beta)][\mathbb{Z}_p(\beta) : \mathbb{Z}_p] = sd,$$

da cui la tesi.

Teoremi fatti a Esercitazioni

1. **(Formula di Stiefel)** Siano $k \leq n$ interi positivi. Allora

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

Dimostrazione ($\star$)

Per verifica diretta si ha che

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \Rightarrow \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} = \frac{k \cdot n! + (n-k+1) \cdot n!}{k!(n-k+1)!} =$$

$$= \frac{(n+1)n!}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n-k+1)!} = \binom{n+1}{k}.$$

2. **(Teorema del binomio)** Sia n un intero positivo e siano $a,\ b$ due numeri reali, allora:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Dimostrazione ($\star$)

Procediamo per induzione su n.
Passo base $n = 1$
E' una semplice verifica.
Passo induttivo $n \Rightarrow n+1$

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} =$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1} b^k = a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1} b^k + b^{n+1} =$$

$$= a^{n+1} + b^{n+1} + \sum_{k=0}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) a^{n-k+1} b^k = a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n-k+1} b^k =$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n-k+1} b^k.$$

3. **Teorema del multinomio** Sia n un intero positivo e siano $a_1,\ ..., a_m$ numeri reali ($m \geq 1$), allora:

$$(a_1 + ... + a_m)^n = \sum_{h_1+...+h_m=n} \binom{n}{h_1, ..., h_m} a_1^{h_1} ... a_m^{h_m}$$

Dimostrazione ($\star\star$)

Procediamo per induzione su m.
Passo base $m = 1$
Ovvio.
Passo induttivo $m \Rightarrow m + 1$

$$(a_1 + ... + a_m + a_{m+1})^n = (a_1 + ... + (a_m + a_{m+1}))^n =$$

$$= \sum_{h_1+...+h_{m-1}+K=n} \binom{n}{h_1, ..., h_{m-1}, K} a_1^{h_1} ... a_{m-1}^{h_{m-1}} (a_m + a_{m+1})^K =$$

$$= \sum_{h_1+...+h_{m-1}+K=n} \left[\binom{n}{h_1, ..., h_{m-1}, K} a_1^{h_1} ... a_{m-1}^{h_{m-1}} \sum_{h_m+h_{m+1}=K} \binom{K}{k_m, k_{m+1}} a_m^{h_m} a_{m+1}^{h_{m+1}} \right] =$$

$$= \sum_{h_1+...+h_{m+1}=n} \binom{n}{h_1, ..., h_{m-1}, K} \binom{K}{h_m, h_{m+1}} a_1^{k_1} ... a_{m+1}^{k+1} = \sum_{h_1+...+h_{m+1}=n} \binom{n}{h_1, ..., h_{m+1}} a_1^{k_1} ... a_{m+1}^{k+1}.$$

4. Sia $(G, \cdot)$ un gruppo tale che $\forall a, b \in G\ (ab)^2 = a^2b^2$. Allora il gruppo è abeliano.

Dimostrazione ($\star$)

$$(ab)^2 = abab = a^2b^2 \Rightarrow bab = ab^2 \Rightarrow ba = ab.$$

5. Sia $(G, \cdot)$ un gruppo e $n \in \mathbb{N}$. Allora $a^n = e \Rightarrow o(a)|n$.

Dimostrazione ($\star$)

Svolgiamo la divisione euclidea fra n e $o(a)$. Allora

$$n = o(a)q + r \Rightarrow a^n = a^{o(a)q+r} = a^{o(a)q} a^r = a^r = e$$

Per la minimalità di $o(a)$ non può che essere $r = 0$, da cui la tesi.

6. Siano $(G, \cdot)$ e $(H, \star)$ due gruppi e $(x, y) \in G \times H$: allora

$$o((x, y)) = [o(x), o(y)].$$

Dimostrazione $(\star\star)$

$$(x, y)^{[o(x),o(y)]} = (x^{[o(x),o(y)]}, y^{[o(x),o(y)]}) = ((x^{o(x)})^m, (y^{o(y)})^n) = (e_1, e_2) \Rightarrow$$
$$\Rightarrow o((x, y))|[o(x), o(y)];$$
$$(e_1, e_2) = (x, y)^{o((x,y))} = (x^{o((x,y))}, y^{o((x,y))}) \Rightarrow o(x)|o((x, y)) \wedge o(y)|o((x, y)) \Rightarrow$$
$$\Rightarrow [o(x), o(y)]|o((x, y)).$$

7. Sia $g \in \mathbb{Z}_n^*$ e $x, y \in \mathbb{Z}$. Allora

$$g^a \equiv g^b \ (n) \Leftrightarrow a \equiv b \ (o(g)).$$

Dimostrazione $(\star)$

Visto che g è invertibile

$$g^a \equiv g^b \ (n) \Leftrightarrow g^{a-b} \equiv 1 \ (n) \Leftrightarrow o(g)|(a - b) \Leftrightarrow a - b \equiv 0 \ (o(g)) \Leftrightarrow a \equiv b \ (o(g)).$$

8. **(Teorema di Ruffini)** Sia $(K, +\cdot)$ un campo, $\alpha \in K$ è radice di un polinomio $f(x) \in K[x]$ se e solo se il fattore $x - a$ divide $f(x)$.

Dimostrazione $(\star)$

$(\Rightarrow)$ Se α è radice di $f(x)$, allora $f(\alpha) = 0$, inoltre svolgendo la divisione euclidea di $f(x)$ con $x - a$ (che è possibile fare perché se K è un campo $K[x]$ è euclideo) si ha che esistono $q(x), r(x)$ tali che

$$f(x) = q(x)(x - a) + r(x).$$

Notiamo che $r(x)$ è una costante $r(x) = r$, in quanto o $r(x) = 0$ o $deg(r) < deg(x - a) = 1$. Valutando in α si ha $0 = f(\alpha) = r$ e dunque $x - a$ divide $f(x)$.

$(\Leftarrow)$ Se $x - a$ divide $f(x)$ allora esiste $g(x)$ tale che $f(x) = (x - a)g(x)$. Allora valutando in α si ricava $f(\alpha) = 0$ e dunque α è una radice di $f(x)$.

9. Sia $(K, +\cdot)$ un campo e $f(x) \in K[x] - 0$ un polinomio di grado n. Allora in K $f(x)$ ha al più n radici distinte.

   Dimostrazione $(\star)$

   Procediamo per induzione sul grado di $f(x)$.

   Passo base $deg(f) = 0$ In tal caso il polinomio è una costante non nulla, e pertanto non ha radici.

   Passo induttivo $deg(f) \Rightarrow deg(f) + 1$ Se $f(x)$ non ha radici in K, abbiamo finito. Se invece ha almeno una radice α per il teorema di Ruffini esiste $g(x)$ per cui $f(x)$ si fattorizza nel modo seguente:

   $$f(x) = g(x)(x - \alpha).$$

   Il polinomio $g(x)$ ha grado n, e dunque per ipotesi induttiva ha al più n radici, e poiché ogni radice di $g(x)$ è anche radice di $f(x)$ e viceversa, $f(x)$ ha al più $n + 1$ radici, per cui si ha la tesi.

10. **(Principio d'identità dei polinomi)** Sia $(K, +, \cdot)$ un campo infinito e siano $f(x),\ g(x)\ \in K[x]$. Allora $f(x) = g(x)$ se e solo se le due funzioni polinomiali associate

    $$\begin{aligned} \tilde{f} : K &\to K \\ a &\mapsto f(a) \end{aligned}$$

    e

    $$\begin{aligned} \tilde{g} : K &\to K \\ a &\mapsto g(a) \end{aligned}$$

    coincidono.

    Dimostrazione $(\star\star)$

    $(\Rightarrow)$ Ovvio.

    $(\Leftarrow)$ Se le due funzioni polinomiali associate coincidono, allora $\tilde{f} - \tilde{g}$ è la funzione identicamente nulla, vale a dire, ogni $k \in K$ è radice del polinomio $(f - g)(x)$. Se tale polinomio fosse il polinomio nullo, si avrebbe la tesi, in quanto ciò implicherebbe che i coefficienti dei due polinomi $f(x)$ e $g(x)$ coincidono. Se per assurdo tale polinomio non avesse tutti i coefficienti nulli, esso ha un grado n, e per il teorema precedente dovrebbe avere al più n radici, contro il fatto che ne ha infinite.

11. Sia $(K, +, \cdot)$ un campo, e siano $f(x) \in K[x]$ e α una radice di $f(x)$. Allora α è una radice multipla di $f(x)$ se e solo se α è una radice anche del polinomio derivata $f'(x)$.

Dimostrazione $(\star)$

($\Rightarrow$) Se α è una radice multipla, $\exists m \in \mathbb{N},\ m > 1$ e $\exists g(x) \in K[x] \mid g(\alpha) \neq 0$ tali che

$$f(x) = (x - \alpha)^m g(x).$$

Allora

$$f'(x) = m(x - \alpha)^{m-1} g(x) + (x - \alpha)^m g'(x) = (x - \alpha)^{m-1}[g(x) + (x - \alpha)g'(x)],$$

e dunque è immediato notare che $f'(\alpha) = 0$.

($\Leftarrow$) Se per assurdo α non fosse una radice multipla avremmo che $\exists g(x) \in K[x] \mid g(\alpha) \neq 0$ tale che

$$f(x) = (x - \alpha)g(x).$$

Allora

$$f'(x) = g(x) + (x - \alpha)g'(x),$$

che però non si annulla in α.

12. Sia $(K, +, \cdot)$ un campo, e sia $f(x) \in K[x]$ di grado 2, o 3. Allora $f(x)$ è irriducibile se e solo se non ha radici in K.

Dimostrazione $(\star\star)$

($\Rightarrow$) Immediato per il teorema di Ruffini.

($\Leftarrow$) Se per assurdo il polinomio $f(x)$ fosse riducibile, esisterebbero $g(x), h(x) \in K[x]$ di grado rispettivamente m e n tali che

$$f(x) = g(x)h(x).$$

Per come è definito il prodotto, il polinomio $f(x)$ ha grado $m + n$: sia nel caso $m + n = 2$ sia nel caso $m + n = 3$ uno fra m e n deve essere uguale a 1, ovvero per il teorema di Ruffini il polinomio dovrebbe avere una radice, assurdo.

13. Ogni polinomio $p(x) \in \mathbb{Q}[x]$ è associato a un polinomio primitivo $q(x) \in \mathbb{Z}[x]$.

Dimostrazione $(\star)$

Siano $\frac{a_0}{b_0}, ..., \frac{a_n}{b_n}$ i coefficienti del polinomio $p(x)$. Allora moltiplicando $p(x)$ per $\frac{[b_0,...,b_n]}{(a_0,...,a_n)}$ si ottiene un polinomio a coefficienti interi primitivo.

14. Sia $(R, +, \cdot)$ un anello euclideo. Allora il prodotto di due polinomi $q(x), r(x) \in R[x]$ primitivi è primitivo.

Dimostrazione $(\star)$

Supponiamo per assurdo che $p(x) = q(x)r(x)$ prodotto di polinomi primitivi non sia primitivo: allora esisterà un primo p che ne divide tutti i coefficienti. Allora nell'anello $((\mathbb{Z}_p[x], +, \cdot)$ si ha che

$$q(x)r(x) = 0.$$

Poiché siamo in un dominio d'integrità, deve essere allora che o $q(x) = 0$ o $r(x) = 0$. Ma in tal caso tutti i coefficienti di uno dei due polinomi dovrebbero essere divisibili per p il che è assurdo perché essi sono primitivi. Dunque $p(x)$ è primitivo.

15. **(Lemma di Gauss)** Sia $f(x) \in \mathbb{Z}[x]$ e sia $f(x) = g(x)h(x)$ una sua fattorizzazione in $\mathbb{Q}[x]$. Allora esiste $q \in \mathbb{Q}$ tale che $g_1(x) = q \cdot g(x) \in \mathbb{Z}[x]$ e $h_1(x) = q^{-1} \cdot h(x) \in \mathbb{Z}[x]$ e

$$f(x) = g_1(x)h_1(x)$$

è una fattorizzazione valida in $\mathbb{Z}[x]$.

Dimostrazione $(\star\star)$

Possiamo limitarci al caso che che il polinomio sia primitivo.
Per il teorema 13, esistono $\alpha, \beta \in \mathbb{Q}[x]$ tali che $\alpha g(x)$ e $\beta h(x)$ siano polinomi a coefficienti interi primitivi. Il loro prodotto è

$$\alpha\beta g(x)h(x),$$

che è a sua volta a coefficienti interi e primitivo per il teorema precedente. Ma allora $\alpha\beta = \pm 1$ (se così non fosse ogni coefficiente di tale polinomio sarebbe divisibile per $\alpha\beta$ e dunque non sarebbe primitivo). A meno del segno negativo, che può essere inglobato nel polinomio $g(x)h(x)$ si ha che $\alpha\beta = 1$, da cui si ha la tesi.

16. Sia $f(x)$ un polinomio a coefficienti interi e siano a_n e a_0 rispettivamente il coefficiente direttivo e il termine noto del polinomio. Se q è una radice razionale di $f(x)$ allora è della forma $\frac{r}{s}$, dove r è un divisore del termine noto e s un divisore del coefficiente direttivo.

Dimostrazione $(\star)$

Sia $\frac{r}{s}$ una radice razionale di $f(x) = \sum_{k=0}^{n} a_k x^k$ ridotta ai minimi termini. Allora si ha che

$$\sum_{k=0}^{n} a_k \left(\frac{r}{s}\right)^k = 0 \Rightarrow s^n \sum_{k=0}^{n} a_k \left(\frac{r}{s}\right)^k = 0 \Rightarrow \sum_{k=0}^{n} a_k r^k s^{n-k} = 0 \Rightarrow$$

$$\Rightarrow a_0 s^n = -\sum_{k=1}^{n} a_k r^k s^{n-k} = -r \sum_{k=1}^{n} a_k r^{k-1} s^{n-k} \ \wedge \ a_n r^n = -\sum_{k=0}^{n-1} a_k r^k s^{n-k} = -s \sum_{k=0}^{n-1} a_k r^k s^{n-k-1}.$$

Poiché per ipotesi $\frac{r}{s}$ è ridotta ai minimi termini si ha che $(r, s) = 1$, e dunque dalle ultime due relazioni si ricava che $r \mid a_0$ e $s \mid a_n$.

17. Sia $(K, +, \cdot)$ un campo e sia $\phi : K[x] \to K[x]$ un omomorfismo di anelli tale che per ogni $q(x)$ di grado maggiore di 0 anche $\phi(q(x))$ ha grado maggiore di 0. Allora se $g(x)$ è riducibile, anche $\phi(g(x))$ lo è.

Dimostrazione $(\star)$

Poiché $q(x)$ è riducibile esistono $r(x), s(x)$ tali che $q(x) = r(x)s(x)$. Allora si ha che

$$\phi(q(x)) = \phi(r(x)s(x)) = \phi(r(x))\phi(s(x)).$$

Poiché per ipotesi i gradi di $\phi(r(x))$ e $\phi(s(x))$ sono maggiori di 0 questa è una fattorizzazione non banale di $\phi(q(x))$.

18. Sia $(K, +, \cdot)$ un campo e sia $p(x) \in K[x]$ riducibile. Allora anche $p(x^k)$ è riducibile in $K[x]$ per ogni $k \in \mathbb{N}^+$.

Dimostrazione $(\star\star)$

L'omomorfismo di anelli

$$\phi : K[x] \to K[x]$$

che lascia fisse le costanti e manda x in x^k soddisfa le condizioni del teorema precedente, dunque per quest'ultimo anche $f(x^k)$ è riducibile in $K[x]$.

19. Sia $(K, +, \cdot)$ un campo. $p(x) \in K[x]$ è riducibile se e solo se per ogni $a, b \in K, a \neq 0$ anche $p(ax + b)$ è riducibile in $K[x]$.

Dimostrazione $(\star\star)$

$(\Rightarrow)$ E' sufficiente considerare l'omomorfismo

$$\phi : K[x] \to K[x]$$

$$x \mapsto ax + b.$$

Tale omomorfismo soddisfa le condizioni del teorema 17. per ogni possibile scelta di a e b in K, con $a \neq 0$, pertanto anche $f(ax + b)$ è riducibile in $K[x]$.

$(\Leftarrow)$ Basta scegliere $a = 1$ e $b = 0$ e si ha immediatamente la tesi.

20. Sia $f(x) \in \mathbb{Z}[x]$ un polinomio e sia p un numero primo che non divide il coefficiente direttivo di $f(x)$ allora se $f_p[x] \in \mathbb{Z}_p[x]$ è irriducibile anche $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

Dimostrazione ($\star\star$)

Dimostriamo la contronominale. Se $f(x) \in \mathbb{Z}[x]$ è riducibile in $\mathbb{Q}[x]$ allora esistono $g(x), h(x) \in \mathbb{Z}[x]$ tali che

$$f(x) = g(x)h(x).$$

Allora considero l'omomorfismo

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$
$$f(x) \mapsto f_p[x].$$

Si ha che

$$f(x) = g(x)h(x) \Rightarrow \phi(f(x)) = \phi(g(x)h(x)) = \phi(g(x))\phi(h(x)).$$

L'omomorfismo ϕ non altera il grado di $g(x)$ e $h(x)$, proprio perché p non divide il loro coefficiente direttivo (se ne dividesse almeno uno allora anche il coefficiente direttivo di $f(x)$ sarebbe divisibile per p, contro l'ipotesi), e dunque il teorema 17. ci garantisce che $\phi(g(x))\phi(h(x))$ è una fattorizzazione non banale di $f(x)$ che è dunque riducibile in $\mathbb{Z}_p[x]$.

21. **(Criterio di Eisenstein)** Sia $p(x) = \sum_{k=0}^{n} c_k x^k \in \mathbb{Z}[x]$: se esiste un primo p tale che

- $p \nmid c_n$;
- $p \mid c_i \ \forall 0 \leq i < n$;
- $p^2 \nmid c_0$,

allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$, e dunque in $\mathbb{Q}[x]$.

Dimostrazione ($\star\star$)

Supponiamo per assurdo che $f(x)$ sia riducibile, allora esistono

$$a(x) = \sum_{k=0}^{\alpha} a_k x^k,$$

$$b(x) = \sum_{k=0}^{\beta} b_k x^k$$

a coefficienti interi tali che

$$f(x) = a(x)b(x).$$

Poiché p non divide il coefficiente direttivo del polinomio $f(x)$, si può applicare il teorema 20. Dunque $f_p[x] = a_n x^n = a_p[x]b_p[x]$. Si ha che anche $a_p[x]$ e $b_p[x]$ devono essere monomi, e in particolare allora p divide sia il termine noto di a_0 sia il termine noto di b_0. Dunque $p^2 \mid c_0 = a_0 b_0$, assurdo.

22. Sia p un numero primo. Allora il polinomio $p(x) = \sum_{k=0}^{p-1} x^k$ è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione ($\star\star$)

Si ha la relazione

$$\sum_{k=0}^{p-1} x^k = \frac{x^p - 1}{x - 1}.$$

Supponiamo che $p(x)$ sia riducibile. Allora siamo nelle condizioni di applicare il teorema 19. Scegliamo $a = b = 1$, allora $p(x+1)$ dovrebbe essere riducibile.

$$p(x+1) = \frac{(x+1)^p - 1}{x} = \frac{1}{x}\left(\sum_{k=0}^{p} \binom{p}{k} x^k - 1\right) = \frac{1}{x}\sum_{k=1}^{p} \binom{p}{k} x^k = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}.$$

Sappiamo che

$$p \nmid \binom{p}{p} = 1;$$

$$p \mid \binom{p}{k} \; \forall 1 \leq k < p;$$

$$p^2 \nmid \binom{p}{1} = p.$$

Ma allora per il criterio di Eisenstein $p(x+1)$ è irriducibile. Dunque per il teorema 19 anche $p(x)$ è irriducibile.

23. Sia $(K, +, \cdot)$ un campo. $f(x) \in K[x]$ ha fattori di grado maggiore di 0 multipli se e solo se il grado di $(f(x), f'(x))$ è maggiore di 0.

Dimostrazione ($\star\star$)

($\Rightarrow$) Se ha fattori di grado maggiore 0 multipli allora in particolare ne ha almeno uno, $p(x)$. Sia $m > 1$ la sua molteplicità. Allora esiste $g(x)$ tale che

$$f(x) = p(x)^m g(x),$$

$$f'(x) = mp(x)^{m-1}p'(x)g(x) + p(x)^m g'(x) = p(x)^{m-1}(mg(x)p'(x) + p(x)g'(x).$$

Sicuramente $p(x)^{m-1} \mid (f(x), f'(x))$, dunque il grado di $(f(x), f'(x))$ è sicuramente $\geq m - 1 > 0$.

($\Leftarrow$) Se un polinomio e la sua derivata hanno fattori in comune, in particolare ne hanno almeno uno, $p(x)$, supponiamo rispettivamente con molteplicità $\alpha \geq 1$ e $\beta \geq 1$. Se si dimostra che $\alpha \geq 2$ abbiamo finito. Si ha che

$$f(x) = p(x)^\alpha q(x),$$
$$f'(x) = p(x)^\beta r(x).$$

Deriviamo $f(x)$:

$$f'(x) = \alpha p(x)^{\alpha-1}p'(x)q(x) + p(x)^\alpha q'(x) = p(x)^{\alpha-1}\Big(\alpha p'(x)q(x) + p(x)q'(x)\Big).$$

Ma allora deve essere:

$$\begin{cases} p(x)^{\alpha-1} = p(x)^\beta \\ \alpha p'(x)q(x) + p(x)q'(x) = r(x) \end{cases}$$

In particolare allora si ha che

$$\alpha - 1 = \beta \Rightarrow \alpha = \beta + 1 \geq 2.$$