Dispense di Algebra 1

Università di Pisa

Basate sugli appunti dei corsi tenuti dai professori
Ilaria Del Corso e Davide Lombardo (a.a 2023/2024)
Ilaria Del Corso e Leonardo Patimo (a.a. 2024/2025)

Daria Pasqualetti, Lorenzo Ferrari

Queste dispense sono nate dagli appunti di Daria dell'a.a. 2023/2024 e concluse l'anno successivo da Lorenzo, integrandole sulla base del corso nuovo. Il programma dei due corsi era di fatto identico, l'unica differenza sono state alcune esercitazioni. Sono inclusi tutti gli esercizi lunghi o interessanti svolti ad esercitazione, tutti i fatti di teoria e qualche fatto interessante trovato in compitini vecchi o negli esercizi del libro "Esercizi scelti di Algebra. Volume 2." di R. Chirivì, I. Del Corso, R. Dvornicich. Qualsiasi segnalazione di typo o proposta di aggiunta è chiaramente ben accetta, così come commenti al file (azzardando: e proporsi per aggiungere esempi o altri esercizi). Attualmente l'unica parte totalmente completa come esempi ed esercizi è teoria dei gruppi.

Per segnalare typo: d.pasqualetti3@studenti.unipi.it $\vee$ l.ferrari41@studenti.unipi.it.

Indice

1 Teoria dei gruppi

Dove non diversamente specificato G è un gruppo con identità e. Il simbolo dell'operazione verrà omesso.

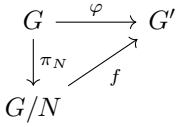
1.1 Definizioni e richiami di Aritmetica

Definizione - centro: $Z(G) = \{h \in G \mid \forall\, g \in G\ gh = hg\}$.
Proposizione - proprietà del centro: $G/Z(G)$ ciclico $\Rightarrow$ G abeliano ($Z(G) = G$).
Attenzione! $G/Z(G)$ abeliano $\Rightarrow$ G abeliano è falsa, un controesempio è Q_8.
Definizione - centralizzatore di un elemento: se $g \in G$, $Z_G(g) = \{h \in G \mid gh = hg\}$.
Definizione - centralizzatore di un sottogruppo: se $H < G$, $Z_G(H) = \bigcap_{h\in H} Z_G(h)$.
Definizione - classe di coniugio di un elemento: $Cl(g) = \{hgh^{-1} \mid h \in G\}$.
Teorema - Lagrange: sia G finito e $H < G$. Allora $\#H \mid \#G$. Corollario: $g \in G \Rightarrow \text{ord}(g) \mid \#G$.
Definizione - prodotto diretto: Dati $(H, *_H), (K, *_K)$ gruppi si può dare una struttura di gruppo al loro prodotto cartesiano $H \times K$, prendendo come operazione $*$ tale che $(h_1, k_1) * (h_2, k_2) = (h_1 *_H h_2, k_1 *_K k_2)$ (chiaramente ha tutte le proprietà richieste). Questo gruppo è detto *prodotto diretto* di H, K.
Proposizione - prodotto di sottogruppi: Siano $H, K \leq G$. HK sottogruppo $\Leftrightarrow$ $HK = KH$. Si nota che ciò è certamente verificato se almeno uno tra H e K è normale.
Proposizione - cardinalità del prodotto di sottogruppi: Siano $H, K \leq G$. A prescindere dal fatto che HK sia o no un sottogruppo si ha $\#HK = \frac{\#H\#K}{\#H\cap K} = \#KH$.

1.2 Teoremi di omomorfismo

Teorema - 1° di omomorfismo:

Sia $\varphi : G \to G'$ un omomorfismo, $N \lhd G$ tale che $N \subseteq \text{Ker}(\varphi)$. Allora $\exists! f$ che fa commutare il diagramma a lato. Inoltre $N = \text{Ker}(\varphi) \Rightarrow f$ iniettiva.



dim. Considero la funzione $f : G/N \to G'$ data da $f(gN \mapsto \varphi(g))$.

- buona def.: se scelgo due diversi rappresentanti per la classe in G/N allora si ha $g_1N = g_2N \Rightarrow g_2^{-1}g_1 \in N \Rightarrow g_2^{-1}g_1 \in \text{Ker}(\varphi) \Rightarrow \varphi(g_2)^{-1}\varphi(g_1) = e' \Rightarrow \varphi(g_1) = \varphi(g_2)$ quindi non ci sono problemi.
- è omomorfismo: usando che φ è omomorfismo si ha $gNhN = ghN \Rightarrow f(gNhN) = f(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = f(gN)f(hN)$

Dimostriamo ora che $\text{Ker}(f) = \text{Ker}(\varphi)/N$. Si nota intanto che l'espressione a destra ha senso perché N è un sottogruppo normale in G contenuto in $\text{Ker}(\varphi)$, e quindi è normale in $\text{Ker}(\varphi)$. Inoltre $f(gN) = e' \Leftrightarrow \varphi(g) = e' \Leftrightarrow g \in \text{Ker}(\varphi) \Leftrightarrow gN \in \text{Ker}(\varphi)/N$. Da ciò segue l'iniettività se $\text{Ker}(\varphi) = N$.

Teorema - 2° di omomorfismo: Siano $H, K \lhd G$, $H \leq K$. Allora $\frac{G/H}{K/H} \cong G/K$.

dim. Notiamo intanto la buona def. Infatti da $H \lhd G$ e $H \leq K$ segue che H normale anche in K. Quindi K/H è ben definito. Inoltre da $K \lhd G$ segue $K/H \lhd G/H$. Considero l'omomorfismo $f : G/H \to G/K$ tale che $f(gH \mapsto gK)$.

- buona def.: se scelgo due diversi rappresentanti per la classe in G/H allora si ha $g_1H = g_2H \Rightarrow g_2^{-1}g_1 \in H \subset K \Rightarrow g_1K = g_2K$ quindi non ci sono problemi
- è omomorfismo: chiaro per le proprietà del gruppo quoziente

Dimostriamo ora che $\mathrm{Ker}(f) = K/H$. Infatti $f(gH) = K \Leftrightarrow gK = K \Leftrightarrow g \in K$. Per il 1° teorema di omomorfismo si ha la tesi.

Teorema - 3° di omomorfismo: Siano $H, K \lhd G$. Allora $\frac{H}{H\cap K} \cong \frac{HK}{K}$.

dim. Notiamo intanto la buona def. Poiché entrambi i sottogruppi sono normali, si ha $HK = KH$ e quindi HK è sottogruppo; inoltre dalle normalità in G seguono le due normalità necessarie per definire i quozienti, quindi non abbiamo problemi. Considero ora $f : H \to HK/K$ tale che $f(h \mapsto hK)$. È chiaramente omomorfismo per le proprietà del gruppo quoziente. Dimostriamo ora che $\mathrm{Ker}(f) = H \cap K$. Si ha $f(h) = K \Leftrightarrow hK = K \Leftrightarrow h \in K$. Ma $h \in H$ per definizione, e quindi $\mathrm{Ker}(f) = H \cap K$. Per il 1° teorema di omomorfismo si ha la tesi.

1.3 Sottogruppi normali e automorfismi interni

Definizione - normalizzatore: Dato $H \leq G$ chiamiamo $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$.

- segue immediatamente dalla definizione che è un gruppo e che $H \lhd N_G(H)$
- segue dalle definizioni che $H \lhd G \Leftrightarrow N_G(H) = G$; quindi se G è abeliano tutti i gruppi sono normali e quindi $N_G(H) = G$ per ogni $H < G$
- si ha $Z_G(H) < N_G(H)$
- talvolta si chiama normalizzatore di un elemento il normalizzatore del sottogruppo generato

Esempio: per $G = S_3$ si ha $N_G((1,2)) = \langle(1,2)\rangle$, $N_G((1,2,3)) = G$ (e infatti $\langle(1,2,3)\rangle \lhd S_3$); per $G = S_4$ si ha $N_G((1,2)) = \{id, (1,2), (3,4), (1,2)(3,4)\}$.
Definizione - automorfismi interni: Sia $g \in G$; denotiamo con $\varphi_g \in \mathrm{Aut}(G)$ il coniugio $\varphi_g(x \mapsto gxg^{-1})$. $\mathrm{Inn}(G) := \{\varphi_g : g \in G\}$ viene chiamato il gruppo degli *automorfismi interni* di G.

- per definizione $H < G$ è normale se e solo se è è invariante per automorfismi interni.

buona def. $\varphi_g \in \mathrm{Aut}(G)$ perché $\varphi_g(h_1)\varphi_g(h_2) = gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1} = \varphi_g(h_1h_2)$. Inoltre è un gruppo perché $\varphi_{g_1} \circ \varphi_{g_2}(h) = g_1g_2hg_2^{-1}g_1^{-1} = g_1g_2h(g_1g_2)^{-1} = \varphi_{g_1g_2}(h)$, ovvero composizione di automorfismi interni resta automorfismo interno. L'identità è φ_e, l'inverso di φ_g è $\varphi_{g^{-1}}$ per quanto appena detto.

Proposizione - proprietà degli automorfismi interni: (1) $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$, (2) $\mathrm{Inn}(G) \cong G/Z(G)$

dim.

(1) basta notare che $\forall f \in \mathrm{Aut}(G)$ si ha $f \circ \varphi_g \circ f^{-1} = \varphi_{f(g)}$. Infatti $\forall h \in G$ si ha $f \circ \varphi_g \circ f^{-1}(h) = f(gf^{-1}(h)g^{-1}) = f(g)f(f^{-1}(h))f(g)^{-1} = f(g)hf(g)^{-1} = \varphi_{f(g)}(h)$

(2) Consideriamo l'omomorfismo di gruppi $\varphi : G \to \mathrm{Aut}(G)$, $\varphi(g \mapsto \varphi_g)$ (si vede facilmente che è omomorfismo). Notiamo che $\varphi_g(h) = h \Leftrightarrow gh = hg$ e quindi $g \in Ker\varphi \Leftrightarrow g \in Z(G)$ (l'uguaglianza di prima deve valere $\forall h \in G$). Allora per il primo teorema di omomorfismo si ha: $G/Z(G) \cong \mathrm{Inn}(G)$, come voluto.

Esempio - $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$: vale in particolare $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3) \cong S_3$.
Questo risultato si può generalizzare.

dim. Innanzitutto $\mathrm{Inn}(S_3) \cong S_3$ per il teorema appena dimostrato (il centro di S_3 è banale). Notiamo ora che $\#\mathrm{Aut}(G) \leq 6$. Infatti S_3 è generato dalle sue trasposizioni, la cui immagine può essere solo un'altra trasposizione. Quindi un automorfismo di S_3 deve permutare le trasposizioni $\Rightarrow$ ci sono (al più) 6 possibilità $\Rightarrow \#\mathrm{Aut}(G) \leq 6 \Rightarrow \mathrm{Inn}(S_3) \cong S_3 \cong \mathrm{Aut}(S_3)$.

Definizione - sottogruppo caratteristico: $H < G$ si dice *caratteristico* se $\forall \varphi \in \mathrm{Aut}(G)$ vale $\varphi(H) = H$.

- un sottogruppo caratteristico è invariante per automorfismi, quindi in particolare per automorfismi interni, ed è quindi normale;
- non vale il viceversa: poiché $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ è abeliano, tutti i suoi sottogruppi sono normali; tuttavia l'omomorfismo che scambia le componenti dimostra che $\mathbb{Z}/2\mathbb{Z} \times \{0\}$ non è caratteristico.

Proposizione - la normalità non è transitiva: Un controesempio sono i sottogruppi $D_2 < D_4 < D_8$: si ha infatti $D_2 \lhd D_4$, $D_4 \lhd D_8$ ma $D_2 \not\lhd D_8$.

dim. (si rimanda allo studio del gruppo diedrale per dettagli sulle dimostrazioni che seguono.) Si ha $D_2 \lhd D_4 \lhd D_8$ perché ciascuno ha indice 2 nel successivo, ma $D_2 \not\lhd D_8$ perché, chiamando r, s la rotazione e la simmetria standard di D_8 si ha $D_2 =< r^4, s >= \{id, r^4, s, sr^4\}$ ma $srD_2(sr)^{-1} = srD_2sr = \{id, srr^4sr, srssr, srsr^4sr\} = \{id, r^4, sr^2, sr^6\}$.

Rafforzando leggermente le ipotesi, il fatto vale.
Proposizione - fatto utile: se $C < N < G$ con C caratteristico in N e $N \lhd G$, allora $C \lhd G$.

dim. $C \lhd G \Leftrightarrow \forall \varphi \in \mathrm{Inn}(G)\ \varphi(C) = C$ ma $N \lhd G \Rightarrow \forall F \in \mathrm{Inn}(G)\ F\mid_H \in \mathrm{Aut}(H)$ e C caratteristico in $N \Rightarrow \forall f \in \mathrm{Aut}(H)\ f(C) = C$. Mettendo assieme le due cose: $\forall \varphi \in \mathrm{Inn}(G)\ \varphi(C) = \varphi\mid_H (C) = C$.

Lemma - normalizzatore-centralizzatore: Sia $H < G$. Vale che $Z_G(H) \lhd N_G(H)$ e inoltre

$$N_G(H)/Z_G(H) \hookrightarrow \mathrm{Aut}(H)$$

dim. $Z_G(H) \subset N_G(H)$ è chiaro dalla definizione. Per vedere la normalità, basta considerare $g \in N_G(H)$. Per definizione, $\forall h \in H\ \exists h' \in H\ h = gh'g^{-1}$. Quindi si ha $\forall z \in Z_G(H)\ gzg^{-1}h = gzh'g^{-1} = gh'zg^{-1} = hgzg^{-1}$, e dunque $gzg^{-1} \in Z_G(H) \Rightarrow gZ_G(H)\ g^{-1} \subseteq Z_G \Rightarrow gZ_G(H)g^{-1} = Z_G$.

Considero ora $\varphi : N_G(H) \to \mathrm{Aut}(H)$ tale che $\varphi(g \mapsto \varphi_g)$ dove $\varphi_g(h \mapsto ghg^{-1})$ è il coniugio per g. È ben definita per definizione di normalizzatore, e si è visto prima che è un omomorfismo. Inoltre è chiaro che $\mathrm{Ker}(\varphi) = Z_G(H)$, e quindi per il 1° teorema di omomorfismo $N_G(H)/Z_G(H)$ è isomorfo a $Imm(\varphi) < \mathrm{Aut}(H)$, come voluto.

1.4 Azioni di gruppo

Definizione - azione: dato X insieme, chiamiamo *azione* di G su X un omomorfismo da G in $S(X)$ (gruppo delle permutazioni degli elementi di X). La permutazione in cui viene mandato $g \in G$ si indica con φ_g, oppure semplicemente $x \mapsto g \cdot x$ o $x \mapsto x^g$.

- Notiamo ora che un'azione definisce in modo naturale una relazione d'equivalenza, in cui $(x, y \in X)$ $x\ y \Leftrightarrow \exists g \in G\ g \cdot x = y$.

buona def. È riflessiva perché $e \cdot x = x \Rightarrow x \sim x$. È simmetrica perché $x \sim y \Rightarrow \exists g \in G\ g \cdot x = y$ e $g \cdot x = y \Rightarrow g^{-1} \cdot y = x$ (l'azione è un omomorfismo, quindi la permutazione di g^{-1} è l'inversa di quella di g). È transitiva perché $x \sim y, y \sim z \Rightarrow \exists g_1, g_2 \in G\ g_1 \cdot x = y, g_2 \cdot y = z$ e quindi $g_2 g_1 \cdot x = z$ (l'azione è un omomorfismo, quindi $g_2 g_1 \cdot x = g_2 \cdot (g_1 \cdot x)$).

Esempio: Nel caso in cui $X = G$ il coniugio è un'azione di gruppo ($g \cdot x := gxg^{-1}$), così come anche la moltiplicazione a sinistra/destra ($g \cdot x := gx$ oppure xg). Un caso in cui $X \neq G$ è dato da $G = K^*$ con K campo, $X = V$ $K-$ spazio vettoriale, e l'azione di X su G è data da $\lambda \cdot \underline{v} := \lambda \underline{v}$.
Le verifiche sono lasciate per esercizio.
Definizione - orbita: data un'azione di G su X $\text{orb}(x) := \{g \cdot x \mid g \in G\} \subseteq X$.

- poiché l'azione definisce una relazione di equivalenza (visto prima) e le orbite ne sono le classi (per definizione), le orbite partizionano X
- nel caso del coniugio per $g \in G$ l'orbita di un elemento $x \in G$ è la sua classe di coniugio $Cl(x)$ (le definizioni coincidono)
- nel caso della moltiplicazione a sinistra (e a destra) l'orbita di un elemento $x \in G$ è tutto G ($\forall y \in Gy = (yx^{-1}) \cdot x$)
- nel caso $G = K^*$ $X = V$ K-spazio vettoriale e $\lambda \cdot \underline{v} = \underline{v}$, vale che se $\underline{v} \neq \underline{0}$ $\text{orb}(\underline{v}) = \text{Span}(\underline{v}) \setminus \{\underline{0}\}$, mentre $\text{orb}(\underline{0}) = \{\underline{0}\}$.

Definizione - stabilizzatore: data un'azione di G su X $\text{stab}(x) := \{g \in G \mid g \cdot x = x\}$

- si verifica facilmente che $\text{stab}(x)$ è un sottogruppo
- nel caso del coniugio per $g \in G$ lo stabilizzatore di un elemento $x \in G$ è il suo centralizzatore $Z_G(g)$ (basta notare che $gxg^{-1} = x \iff gx = xg$)
- nel caso della moltiplicazione a sinistra (e a destra) l'orbita di un elemento $x \in G$ è solo $\{e\}$ ($yx = x \Rightarrow y = e$)
- nel caso $G = K^*$ e $X = V$ K-spazio vettoriale e $\lambda \cdot \underline{v} = \underline{v}$, vale che se $\underline{v} \neq \underline{0}$ $\text{stab}(\underline{v}) = \{1\}$, mentre $\text{stab}(\underline{0}) = X$.

Lemma - orbita-stabilizzatore: se G è finito vale,

$$\forall x \in X \quad \#\text{orb}(x)\#\text{stab}(x) = \#G.$$

dim. Poiché lo stablizzatore è un sottogruppo di G, per il teorema di Lagrange si ha $\#G = [G : \text{stab}(x)]\#\text{stab}(x)$. Basta quindi dimostrare $[G : \text{stab}(x)] = \#\text{orb}(x)$. Consideriamo la mappa
$F : \text{orb}(x) \to G/\text{stab}(x)$ tale che se $y = g \cdot x$ $F(y) = g\,\text{stab}(x)$.

- buona def: se $y = g_1 \cdot x = g_2 \cdot x$ allora $g_2^{-1} g_1 \cdot x = x \Rightarrow g_2^{-1} g_1 \in \text{stab}(x) \Rightarrow g_1\text{stab}(x) = g_2\text{stab}(x)$ quindi la scelta è indipendente dal rappresentante di g.
- iniettività: si procede al contrario $g_1\text{stab}(x) = g_2\text{stab}(x) \Rightarrow g_2^{-1} g_1 \in \text{stab}(x) \Rightarrow g_2^{-1} g_1 \cdot x = x \Rightarrow g_1 \cdot x = g_2 \cdot x$
- suriettività: segue dal fatto che $\text{orb}(x)$ contiene tutti gli $g \cdot x$ al variare di $g \in G$ e quindi la sua immagine secondo F contiene tutti i $g\text{stab}(x)$ al variare di $g \in G$.

- osservazione: se si prende $H < G$ e si considera l'azione di G su G/H data sulla moltiplicazione a sinistra, si ha il teorema di Lagrange: $\#G/H = \#\text{orb}(H) = \frac{\#G}{\#\text{stab}(H)} = \frac{\#G}{\#H}$; poiché G/H è un intero, $\#H|\#G$

Esempio - cardinalità classi di coniugio: $\forall x \in G \ \ \#Cl(x) = [G : Z_G(x)]$; equivalentemente, se G finito, si ha $\forall x \in G \ \#G = \#Cl(x)\#Z_G(x)$.

dim. considerando come azione quella di coniugio (azione di G su G) si ha $\forall x \in G$ $\text{stab}(x) = Z_G(x)$, $\text{orb}(x) = Cl(x)$ e si ottiene la tesi per il lemma orbita-stabilizzatore.

Corollario - gli stabilizzatori sono tutti coniugati: se l'azione agisce transitivamente sull'insieme (ovvero $\forall x, y \in X \ \exists g \in G \ \ g \cdot x = y$).

dim. $\forall x, y \in X$ se $g_0 \cdot x = y$ si ha

$$\begin{aligned}\text{stab}(y) &= \{g \in G | g \cdot y = y\} = \\ &= \{g \in G | g g_0 \cdot x = g_0 \cdot x\} = \\ &= \left\{g \in G | g_0^{-1} g g_0 \cdot x = x\right\} = \\ &= \left\{g \in G | g_0^{-1} g g_0 \in \text{stab}(x)\right\} = \\ &= g_0 \text{stab}(x) g_0^{-1}\end{aligned}$$

Esempio - esiste azione senza punti fissi: se $\#X \geq 2$ e l'azione agisce transitivamente sull'insieme allora $\exists g \in G$ tale che la sua permutazione associata φ_g non abbia punti fissi (ovvero $g \cdot x \neq x \ \forall x \in X$).

dim.

$$\begin{aligned}g \text{ agisce senza punti fissi } &\Leftrightarrow \forall x \in X g \notin \text{stab}(x) \Leftrightarrow \\ &\Leftrightarrow g \notin \bigcup_{x \in X} \text{stab}(x) \Leftrightarrow \qquad \text{(fissiamo } x_0 \in X \text{ e usiamo transitività)} \\ &\Leftrightarrow g \notin \bigcup_{h \in G} \text{stab}(h \cdot x_0) \Leftrightarrow \qquad \text{usiamo il corollario di sopra} \\ &\Leftrightarrow g \notin \bigcup_{h \in G} h\text{stab}(x_0)h^{-1}\end{aligned}$$

Usando che G non è unione di sottogruppi coniugati si ha che un tale g esiste sempre se $\text{stab}(x_0) \neq G$. Ma $\text{stab}(x_0) = G$ e $\text{orb}(x_0) = X$ (azione transitiva) dà un assurdo per il lemma orbita-stabilizzatore, quindi $\text{stab}(x_0) \neq G$ da cui la tesi.

Teorema - formula delle classi: Sia G finito e R insieme di rappresentanti per le classi di coniugio di G. Vale allora:

$$\#G = \#Z(G) + \sum_{g \in R \setminus Z(G)} \frac{\#G}{\#Z_G(g)}$$

dim. Notiamo intanto che l'omomorfismo che manda un elemento nel coniugio per quell'elemento è un'azione di un gruppo su sé stesso (omettiamo le verifiche). Consideriamo quindi l'azione data dal coniugio. Chiaramente in questa azione l'orbita di un elemento è la sua classe di coniugio, mentre lo stabilizzatore è il centralizzatore. Per il lemma orbita-stabilizzatore allora si ha $\forall g \in G \ \#Cl(g)\#Z_G(g) = \#G$. Poiché G può essere partizionato nelle sue classi di coniugio, scegliendo un insieme R di rappresentanti per esse,

vale $\#G = \sum_{g \in R} \#Cl(g) = \sum_{g \in R} \frac{\#G}{\#Z_G(g)}$. Notiamo ora che se $g \in Z(G)$ allora $Cl(g) = \{g\}$ e $Z_G(g) = G$, e quindi $\frac{\#G}{\#Z_G(g)} = 1$. Notiamo anche che ciò implica che in R si trovano tutti gli elementi di $Z(G)$, visto che ciascuno è l'unico possibile rappresentante della propria classe di coniugio. Isolando questi termini nella sommatoria si ottiene la formula dell'enunciato.

Corollario - formula delle classi per sottogruppi normali: Se $H \lhd G$ allora vale una formula delle classi "modificata":

$$\#H = \#(Z(G) \cap H) + \sum_{g \in (R \setminus Z(G)) \cap H} \frac{\#G}{\#Z_G(g)}.$$

dim. Basta notare che $H \lhd G \Rightarrow H$ è unione di classi di coniugio e procedere come nella dimostrazione del teorema.

Alcune applicazioni interessanti della formula delle classi si trovano nella sezione "Fatti utili sui gruppi finiti".

1.5 Teoremi fondamentali

Teorema - Cauchy: Sia G finito, e sia p primo che divide $\#G$. Allora $\exists g \in G$ $\text{ord}(g) = p$.

dim. Notiamo intanto che è sufficiente dimostrare che esiste un elemento $x \in G$ tale che $p \mid \text{ord}(x)$. Infatti $y := x^{\frac{\text{ord}(x)}{p}}$ avrebbe ordine p, come voluto.

Trattiamo prima il caso in cui G è abeliano. Scriviamo $\#G = pn$ e procediamo per induzione estesa su n.

Passo base: $n = 1 \Rightarrow \#G = p \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$ e la tesi è ovvia.

Passo induttivo: prendiamo ora $x \in G \setminus \{e\}$. Poichè G è abeliano tutti i suoi sottogruppi sono normali in G e quindi $\langle x \rangle \lhd G$. Distinguiamo ora due casi:

- $p \mid \text{ord}(x)$ allora si ha già la tesi.
- $p \nmid \text{ord}(x)$ allora $p \mid \#(G/\langle x \rangle)$. $G/\langle x \rangle$ ha cardinalità minore di G perché $x \neq e$. Allora per ipotesi induttiva nel gruppo quoziente $\exists \overline{y}$ tale che $p \mid \text{ord}(\overline{y})$. Notiamo però che considerando l'omomorfismo di proiezione $\pi : G \to G/\langle x \rangle$ poiché l'ordine in arrivo è un divisore dell'ordine in partenza, si ha che, se $\overline{y} = \pi(y)$, $p \mid \text{ord}(\overline{y}) \mid \text{ord}(y)$, come voluto.

Trattiamo ora il caso generale, di nuovo per induzione. Il passo base è analogo a prima.

Passo induttivo: distinguiamo due casi:

- $\exists H < G, H \neq G,\ p \mid \#H$. Allora per ipotesi induttiva si avrebbe la tesi.
- $\forall H < G,\ p \nmid \#H$. Allora in particolare $\forall g \in G\ p \nmid Z_G(g)$. Guardiamo allora la formula delle classi modulo p. $p \mid \#G, \frac{\#G}{\#Z_G(g)}$ e quindi $p \mid \#Z(G)$. Se $Z(G) \neq G$ ci riconduciamo al caso precedente, altrimenti al caso G abeliano, entrambi già trattati.

seconda dim. Consideriamo un'azione di $\mathbb{Z}/p\mathbb{Z}$ su $X = \{(h_1, \dots, h_p) \mid h_1 \dots h_p = e\}$ (p-uple di G con prodotto e). Notiamo intanto che X è non vuoto perché $(e, \dots, e) \in X$. L'azione è da $k \mapsto f_k$ tale che $f_k(\ (h_1, \dots, h_p) \mapsto (h_{1+k}, \dots, h_{p+k})\ )$, dove nella seconda espressione gli indici sono intesi modulo p (è chiaramente ben definita).

$\forall \bar{h} = (h_1, \dots, h_p) \in X$ per il lemma orbita-stabilizzatore $\#\mathbb{Z}/p\mathbb{Z} = p = \#\text{orb}(\bar{h})\#\text{stab}(\bar{h})$, e quindi abbiamo due scelte: $\#\text{orb}(\bar{h}) = 1$ oppure p. Notiamo che se $\#\text{orb}(\bar{h}) = 1$ allora è formata da p elementi

uguali. Infatti $f_k((h_1,\dots,h_p)) = (h_1,\dots,h_p) \Rightarrow h_1 = h_{1+k}$ e quindi se vale $\forall k$ tutti gli elementi sono uguali a h_1. In particolare, o $h_1 = e$ o $\mathrm{ord}(h_1) = p$, poiché per definizione $h_1^p = e$ e p è primo. Sia Y l'insieme delle p-uple formate da p elementi uguali, ossia con orbita banale, e Z un insieme di rappresentanti per gli elementi di X con orbita di cardinalità p. Vorremmo dimostrare che $\#Y \geq 2$, perché così avremmo una p-upla di tutti elementi uguali e diversi da e.

$\#X = \sum_{x\in Y\cup Z} \#\mathrm{orb}(x) = \#Y + p\#Z \cong \#Y \pmod p$ perché X è partizionato nelle sue orbite. Studiamo ora $\#X$. Fissati in un qualunque modo i primi $p-1$ elementi della p-upla l'ultimo è univocamente determinato da $h_p = (h_1 \dots h_{p-1})^{-1}$. Quindi $\#X = (\#G)^{p-1}$. In particolare $p \mid \#G \Rightarrow p \mid \#X \Rightarrow p \mid \#Y$ e quindi, poiché abbiamo dimostrato che Y è non vuoto, $\#Y \geq p \geq 2$.

Teorema - Cayley: Sia G finito, $\#G = n$. Allora $G \hookrightarrow S_n$ (G "si immerge" in S_n, ovvero esiste una copia di G in S_n).

dim. Consideriamo l'azione $g \mapsto \psi_g \in S(G) \cong S_n$ tale che $\psi_g(h \mapsto gh)$.

- buona def.: la moltiplicazione a sinistra appartiene a $S(G)$ perché $gh_1 = gh_2 \Leftrightarrow h_1 = h_2$ (legge di cancellazione), quindi ψ_g è iniettiva $\Rightarrow$ è bigettiva (G è finito).
- è omomorfismo: si vede chiaramente $\psi_{g_1} \circ \psi_{g_2} = \psi_{g_1 g_2}$
- iniettività: guardiamo il nucleo dell'azione, corrispondente a $\{g \in G \mid \psi_g = \mathrm{id}\} = \{g \in G \mid \forall h \in G gh = h\} = \{e\}$. Questo basta per dimostrare l'iniettività.

Osservazione - embedding di Cayley: guardiamo l'immagine di un elemento di g secondo quell'omomorfismo. Se $\mathrm{ord}(g) = d$ (divisore di n) allora "seguendo" un elemento $h_0 \in G$ otteniamo $h_0,\ gh_0 = h_1,\ g^2h_0 = gh_1 = h_2,\ \dots,\ g^{d-1}h_0 = h_{d-1},\ g^dh_0 = h_0$ (e da qui in poi si ripete il ciclo). Gli h_i sono necessariamente tutti distinti ($h_i = h_j \Leftrightarrow g^ih_0 = g^jh_0 \Leftrightarrow g^{i-j} = e \Leftrightarrow i-j \cong 0 \pmod d \Leftrightarrow i-j = 0$ visto che $1 \leq i,j \leq d-1$). Quindi ψ_g nell'isomorfismo con S_n è una permutazione con $\frac{n}{d}$ d-cicli (abbiamo appena dimostrato che ogni elemento che viene permutato sta in un d-ciclo).

Teorema - di corrispondenza: Sia $N \lhd G$ e consideriamo $\pi : G \to G/N = G'$ la proiezione al quoziente. Allora c'è una corrispondenza biunivoca tra i sottogruppi di G che contengono N e i sottogruppi di G'. Inoltre tale corrispondenza preserva ordinamento, indice e normalità.

dim. Siano $\pi_N : G \to G/N$ la proiezione al quoziente, $X = \{H \leq G \mid N \subseteq H\}$, $Y = \{\overline{H} \leq G/N\}$. Consideriamo le due funzioni $\alpha : X \to Y$ tale che $\alpha(H \mapsto \pi_N(H))$ e $\beta : Y \to X$ tale che $\beta(\overline{H} \mapsto \pi_N^{-1}(\overline{H}))$.

- buona def. di α: $N \lhd G, N \subseteq H \Rightarrow N \lhd H$ e quindi è ben definito $H/N = \pi_N(H)$, che è chiaramente un sottogruppo
- buona def. di β: $\pi_N^{-1}(\overline{H})$ è un sottogruppo perché controimmagine di sottogruppo. Inoltre da $N \in \overline{H}$ segue $N \subseteq \pi_N^{-1}(\overline{H})$

Notiamo ora che: $\alpha \circ \beta$ manda $H \mapsto \pi_N(\pi_N^{-1}(\overline{H})) = H$ dove l'ultima uguaglianza segue dal fatto che π_N è suriettiva. Invece $\beta \circ \alpha$ manda $H \mapsto \pi_N(\pi_N(H))^{-1} = \pi_N(H/N)^{-1} = \{g \in G \mid gN \in H/N\} = H$ dove l'ultima uguaglianza segue da $N \subseteq H$ (quindi $\exists h \in H\ gN = hN \Leftrightarrow \exists h \in H, n \in N\ g = hn \Leftrightarrow g \in H$ dove $\Rightarrow$ segue da $N \subseteq H$, mentre per $\Leftarrow$ basta scegliere, per ogni $g \in H$, $h = g, n = e$).

Quindi α e β sono entrambe bigezioni, una inversa dell'altra. Dimostriamo le proprietà della tesi per α.

- Preserva il contenimento: segue dalla definizione

- Preserva la normalità: segue dal fatto che π_N è un omomorfismo, e quindi controimmagine di sottogruppi normali è normale, e inoltre è suriettiva, e quindi manda sottogruppi normali in sottogruppi normali
- Preserva gli indici: occorre dimostrare che $\forall H \leq G, N \subseteq H\ [G : H] = [G' : \alpha(H)] = [G' : H/N]$. Consideriamo la funzione $T : G/H \to \frac{G'/N}{H/N}$ (nota: poiché non è assunta la normalità, non stiamo intendendo il gruppo quoziente ma solo l'insieme delle classi laterali) data da $T(xH \mapsto (xN)H/N)$. T è ben definita perché $xH = yH \Rightarrow \exists h \in H\ x = yh \Rightarrow (xN)H/N = (yhN)H/N = (yNh)H/N = (yN)H/N$ dove la penultima uguaglianza segue dalla normalità di N. Inoltre T è suriettiva per definizione ed è iniettiva perché se si ha $(xN)H/N = (yN)H/N$ allora $\exists h \in H\ xN = (yN)(hN) \Rightarrow x \in yNh \Rightarrow$ (usando che $N \subseteq H$) $\exists h' \in H\ x = yh' \Rightarrow xH = yH$.

  (Si noti che se il sottogruppo in questione fosse stato abeliano, per dimostrare che l'indice viene preservato sarebbe bastato il 2° teorema di omomorfismo.)

Teorema - decomposizione in prodotto diretto: Siano $H, K \lhd G$ tali che $H \cap K = \{e\}$ e $HK = G$. Allora $G \cong H \times K$.

dim. Mostriamo prima un lemma, ossia che nelle ipotesi del teorema si ha $hk = kh \forall h \in H, k \in K$. Fissiamo tali h, k. Per normalità di H in G si ha $khk^{-1} = \tilde{h} \in H$. Quindi $khk^{-1}h^{-1} = \tilde{h}h^{-1} \in H$. In modo analogo si mostra $khk^{-1}h^{-1} \in K$. Quindi $khk^{-1}h^{-1} \in H \cap H = \{e\} \Rightarrow kh = hk$.
Consideriamo ora $\varphi : H \times K \to G\ \varphi(\ (h, k) \mapsto hk)$. φ è omomorfismo perché per il lemma appena dimostrato $h_1h_2k_1k_2 = h_1k_1h_2k_2 \Rightarrow \varphi((h_1h_2, k_1k_2)) = \varphi((h_1, k_1))\varphi((h_2k_2))$. Da $HK = G$ segue φ suriettiva. Inoltre φ è iniettiva perché $(h, k) \in \mathrm{Ker}(\varphi) \Leftrightarrow hk = e \Leftrightarrow H \ni h = k^{-1} \in K \Rightarrow h, k \in H \cap K \Rightarrow h = k = e$.

Definizione - prodotto semidiretto: Siano H, K due gruppi, e $\psi : K \to \mathrm{Aut}(H)$ un omomorfismo. Indichiamo con ψ_g l'immagine di $g \in K$ secondo ψ e definiamo l'operazione $*$ sul prodotto cartesiano $H \times K$ data da $(h_1, k_1) * (h_2, k_2) = (h_1\psi_{k_1}(h_2), k_1k_2)$. Indichiamo con $H \rtimes_\psi K$ questo nuovo gruppo, che chiamiamo un *prodotto semidiretto* di H e K.

- $\psi \equiv id_K$ si ottiene il prodotto diretto (e viceversa);
- *Nota:* d'ora in poi il segno "$*$" sarà omesso come nelle altre operazioni.

buona def. Verifichiamo che è un gruppo:

- elemento neutro: $(h, k) * (h', k') = (h', k') \Leftrightarrow (h\phi_k(h'), kk') = (h', k') \Leftrightarrow h\phi_k(h') = h'$ e $k' = e_K \Leftrightarrow h\phi_{e_K}(h') = hh' = h'$ e $k' = e_K \Leftrightarrow (h, k) = (e_H, e_K)$ e analogamente $(h', k') * (h, k) = (h', k') \Leftrightarrow (h'\phi_{k'}(h), k'k) = (h', k') \Leftrightarrow \phi_{k'}(h) = e_H$ e $k' = e_k \Leftrightarrow (h, k) = (e_H, e_K)$.
- associatività: siano $h, h', h'' \in H$, $k, k', k'' \in K$.

$$\begin{aligned}((h, k) * (h', k')) * (h'', k'') &= (h\phi_k(h'), kk') * (h'', k'') = \\ &= (h\phi_k(h')\phi_{kk'}(h''), kk'k'') = \\ &= (h\phi_k(h')\phi_h(h'')\phi_{k'}(h''), kk'k'');\end{aligned}$$

$$\begin{aligned}(h, k) * ((h', k') * (h'', k'')) &= (h, k) * (h'\phi_{k'}(h''), k'k'') = \\ &= (h\phi_k(h'\phi_{k'}(h'')), kk'k'') = \\ &= (h\phi_k(h')\phi_k \circ \phi_{k'}(h'')), kk'k'').\end{aligned}$$

Quindi le due espressioni sono uguali e si ha associatività.

- inverso: detto $(h,k)^{-1} = (\phi_{k^{-1}}(h^{-1}), k^{-1})$, vale $(h,k)(h,k)^{-1} = (h,k)^{-1}(h,k) = e$.

Osservazione - asimmetria del prodotto semidiretto: $H \times \{e_K\} \lhd H \rtimes K$; **non** vale con $\{e_H\} \times K$.

dim. Basta considerare la proiezione sul secondo fattore, e notare che $H \times \{e_K\}$ ne è il nucleo. Non si può fare lo stesso con la proiezione sul primo fattore per quella che è la definizione del gruppo, e dopo il teorema successivo sarà chiaro come costruire un controesempio.

Teorema - decomposizione in prodotto semidiretto: Siano $H, K \leq G$ tali che $H \lhd G$, $H \cap K = \{e\}$ e $HK = G$. Allora $G \cong H \rtimes_\varphi K$, dove $\varphi(k \mapsto \varphi_k)$ è la mappa che manda $k \in K$ nel coniugio per k ristretto ad H.

dim. Si nota intanto che $\forall k \in K\ \varphi_k \in \mathrm{Aut}(H)$ per normalità di H.

Consideriamo $F : H \rtimes_\varphi K \to G$ tale che $F((h,k) \mapsto hk)$.

- è omomorfismo: $F((h,k)(h',k')) = F(hkh'k^{-1}, kk') = hkh'k^{-1}kk' = hkh'k' = F((h,k))F((h',k'))$
- è bigettiva: il ragionamento è analogo a quello per i prodotti diretti

Proposizione - isomorfismo di prodotti semidiretti: siano H, K gruppi, $\varphi, \psi : K \to \mathrm{Aut}(H)$ omomorfismi. Se $\exists \alpha \in \mathrm{Aut}(H),\ \beta \in \mathrm{Aut}(K)$ tali che $\forall k \in K\ \alpha \circ \varphi_k \circ \alpha^{-1} = \psi_{\beta(k)}$ allora $H \rtimes_\varphi K \cong H \rtimes_\psi K$.

dim. Consideriamo $F : H \rtimes_\varphi K \to H \rtimes_\psi K$ tale che $F((h,k) \mapsto (\alpha(k), \beta(h))$.

- è omomorfismo: $F((h,k) *_\varphi (h',k')) = F(h\varphi_k(h'), kk') = (\alpha(h)\alpha\circ\varphi_k(h'), \beta(k)\beta(k')) = (\alpha(h)\psi_{\beta(k)}(\alpha(h')), \beta(k)\beta(k')) = (\alpha(h), \beta(k)) *_\psi (\alpha(h'), \beta(k')) = F((h,k)) *_\psi F((h',k'))$
- è bigettiva perché lo sono α, β

Definizione - p-Sylow: Sia G un gruppo finito, $\#G = p^n m$ con p primo, $n \geq 1$, $p \nmid m$. Chiamiamo p-Sylow un sottogruppo di G di cardinalità p^n.
Teorema - Sylow: Sia G come prima. Valgono i seguenti quattro enunciati:

- **esistenza**: $\forall \alpha \in \mathbb{N},\ 1 \leq \alpha \leq n\ \exists H \leq G, \#H = p^\alpha$;
- **inclusione**: $\forall \alpha \in \mathbb{N},\ 1 \leq \alpha \leq n-1\ \forall H \leq G$ tali che $\#H = p^\alpha\ \exists K \leq G, \#K = p^{\alpha+1}$ e $H \leq K$;
- **coniugio**: i p-Sylow sono tutti coniugati;
- **numero**: detto n_p il numero di p-Sylow, valgono $n_p \equiv 1 \pmod p$ e $n_p | \#G$, da cui $n_p | m$.

dim. Sia $M = \{X \subseteq G \mid \#X = p^\alpha\}$. Calcoliamo innanzitutto la potenza di p che divide $\#M = \binom{\#G}{p^\alpha} = \frac{p^n m \cdot (p^n m - 1) \cdot \dots \cdot (p^n m - p^\alpha + 1)}{p^\alpha \cdot (p^\alpha - 1) \cdot \dots \cdot 1} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$. Da $p^n \geq p^\alpha > i$ segue che nella produttoria la valutazione p-adica di numeratore e denominatore è sempre la stessa, e quindi non sopravvive nessun fattore p nel prodotto. Quindi la valutazione p-adica di $\#M$ è $n - \alpha$.

Consideriamo l'azione di G su M data da $g \mapsto \psi_g(X \mapsto gX)$ (chiaramente è ben definita). Poiché $p^{n-\alpha+1} \nmid \#M$ e $\#M$ è somma delle cardinalità delle orbite dell'azione, deve necessariamente esistere $Y \in M$ tale che $p^{n-\alpha+1} \nmid \#\mathrm{orb}(Y) = \frac{p^n m}{\#\mathrm{stab}(Y)}$ per il lemma orbita-stabilizzatore. Ma allora necessariamente $p^\alpha \mid \#\mathrm{stab}(Y)$.

Fissiamo ora $y_0 \in Y$ e consideriamo $j : \text{stab}(Y) \to Y$ data da $j(x \mapsto y_0 x)$. È ben definita per definizione di stabilizzatore ed è iniettiva per la legge di cancellazione, e quindi $p^\alpha = \#Y \geq \text{stab}(Y)$, da cui segue $\#\text{stab}(Y) = p^\alpha$. Abbiamo così **esistenza**.

Sia ora S un p-Sylow di G e $H \leq G$ tale che $\#H = p^\alpha$, $0 \leq \alpha \leq n$. Consideriamo l'insieme G/S delle classi laterali di S e consideriamo l'azione (di moltiplicazione a sinistra) di H su G/S che manda $h \in H$ in $\theta_h(gS \mapsto (hg)S)$ (chiaramente è ben definita). Per il lemma orbita-stabilizzatore e usando che le orbite partizionano G/S si ha che, scelto un insieme R di rappresentanti per le orbite $m = \#(G/S) = \sum_{g\in R} \text{orb}(gS) = \sum_{g\in R} \frac{\#H}{\#\text{stab}(gS)} = \sum_{g\in R} \frac{p^\alpha}{\#\text{stab}(gS)}$. Da ciò segue, poiché $p \nmid m$, che $\exists g_0 \in R$ tale che $p^\alpha = \#\text{stab}(g_0 S)$ e quindi $H = \text{stab}(g_0 S)$. Ma allora si ha $\forall h \in H\ hg_0 S = g_0 S \Rightarrow h \in g_0 S g_0^{-1}$ e quindi $H \subseteq g_0 S g_0^{-1}$, che è un p-Sylow. Ciò prova **coniugio** se si pone $\alpha = n$ (l'uguaglianza segue per cardinalità). Se $\alpha < n$ si ha solo che H è contenuto in un p-Sylow, ma tanto basta per restringerci al caso di un p-gruppo.
lemma: in un p-gruppo G, $\forall H \lneq G\ H \lneq N_G(H)$.

> dim. Procediamo per induzione su $n = v_p(\#G)$. Il passo base $n = 1$ è ovvio perché il gruppo è isomorfo a $\mathbb{Z}/p\mathbb{Z}$, che ha solo i due sottogruppi banali per cui la tesi è ovvia. Nel passo induttivo distinguiamo due casi:
>
> - $Z(G) \nsubseteq H$: basta allora notare $Z(G) \subseteq N_G(H)$
> - $Z(G) \subseteq H$: allora quozientiamo per $Z(G)$ e concludiamo usiamo l'ipotesi induttiva, unita al teorema di corrispondenza.

Consideriamo la proiezione: $\pi : N_G(H) \to N_G(H)/H$. Poiché $N_G(H)/H$ è un p-gruppo non banale, per il teorema di Cauchy $\exists \overline{x} \in N_G(H)/H$ $\text{ord}(\overline{x}) = p$. Allora $H \subseteq \pi^{-1}(\langle \overline{x} \rangle)$ e $\#\pi^{-1}(\langle \overline{x} \rangle) = p^{\alpha+1}$. Infatti se $\overline{x} = xH$, si ha $\pi(H) \cup \pi(xH) \cup \cdots \cup \pi(x^{p-1}H) = \langle \overline{x} \rangle$ e per costruzione sono tutti disgiunti ($\overline{x} = xH$ ha ordine p). Allora, poiché le classi laterali hanno tutte la stessa cardinalità, pari a $\#H = p^\alpha$, si ha $\#\pi^{-1}(\langle \overline{x} \rangle) = \#\bigcup_{i=0}^{p-1} x^i H = p \cdot p^\alpha$. Questo dimostra **inclusione**.

Passiamo ora al numero di p-Sylow. Sia $X = \{p\text{-Sylow}\}$ e come prima fissiamo S un p-Sylow. Il coniugato di un p-Sylow, avendo la stessa cardinalità, è a sua volta un p-Sylow e abbiamo precedentemente dimostrato che i p-Sylow sono tutti coniugati, quindi $n_p = \#X$ è la cardinalità della classe di coniugio di S. Consideriamo l'azione di G per coniugio sull'insieme X, ben definita per quanto detto. Chiaramente $\text{orb}(S) = X$, quindi per il lemma orbita-stabilizzatore $n_p = \#\text{orb}(S) \mid \#G$. Restringiamo ora questa azione a S (ossia, consideriamo solo il coniugio per elementi di S, come azione di S su X). Notiamo che S è l'unico elemento con orbita banale: per ogni p-Sylow S' con orbita banale si ha $S \subseteq \text{stab}(S') = N_G(S') \Rightarrow SS'$ sottogruppo e $\#(SS') = \frac{\#S\#S'}{\#(S\cap S')} = \frac{p^n \cdot p^n}{\#(S\cap S')}$, ma SS' sottogruppo di G e p-gruppo $\Rightarrow \#(SS') = p^k$ con $k \leq n \Rightarrow \#(S \cap S') \geq p^n \Rightarrow \#(S \cap S') = p^n$ e quindi $S = S'$. Poiché le orbite partizionano l'insieme che subisce l'azione, dato R insieme di rappresentanti, si ha $n_p = \sum_{S'\in R} \#\text{orb}(S') = 1 + \sum_{S'\in R\setminus\{S\}} \#\text{orb}(S') \equiv 1 \pmod p$. Questo conclude **numero**.

1.6 Teorema di struttura dei gruppi abeliani finiti

La sezione tratta gruppi abeliani, quindi si userà principalmente la notazione additiva (vale a dire $g + h$ invece di gh e 0 invece di e).
. . . in generale: I seguenti risultati sono conseguenze del teorema di decomposizione ciclica primaria dei moduli di torsione su PID (Capitolo 6 di Advanced Linear Algebra, Roman)! In particolare, ogni gruppo

abeliano è uno $\mathbb{Z}$-modulo di torsione (per $n = G$ si ha $nG = \{e\}$) e $\mathbb{Z}$ è un PID. Il teorema di struttura dei gruppi abeliani finiti corrisponde alla più generale "decomposizione in fattori invarianti". Queste generalizzazioni non fanno parte del programma di Algebra 1.

Definizione - componente di p-torsione: Dato p primo e G abeliano, chiamiamo così il gruppo $G(p) = \{g \in G \mid \exists k \in \mathbb{N} \ \text{ord}(x) = p^k\}$. (Se G non è abeliano, in generale $G(p)$ non è un sottogruppo: un 3-ciclo è prodotto di due trasposizioni.)

Teorema - 1: Se G abeliano finito, $\#G = \prod_{i=1}^{s} p_i^{\alpha_i}$ con p_i primi, $G \cong G(p_1) \times \cdots \times G(p_s)$.

dim. Procediamo per induzione su s. Nel passo base la tesi è ovvia. Scriviamo ora $\#G = n = mm'$ con $m, m' \neq 1$ e coprimi. Consideriamo i sottogruppi mG e $m'G$. Essi sono chiaramente sottogruppi di G e inoltre si ha:

- $mG + m'G = G$: il contenimento $\subseteq$ è ovvio, mentre $\supseteq$ utilizza il teorema di Bezout: poiché m, m' sono coprimi, esistono $a, b \in \mathbb{Z}$ tali che $am + bm' = 1$ e quindi vale $\forall g \in G \ m(ag) + m'(bg) = g$
- $mG \cap m'G = \{0\}$: infatti se g appartiene all'intersezione, allora necessariamente si ha $g = mx = m'y$ per degli opportuni $x, y \in G$. Allora $m'g = m'mx = nx = 0$, $mg = mm'y = ny = 0 \Rightarrow \text{ord}(g)|m, m'$, e poiché m, m' coprimi, $\text{ord}(g) = 1 \Rightarrow g = 0$.

Quindi per il teorema di decomposizione in prodotto diretto $G \cong mG \times m'G$. Noto ora che $mG = G_{m'} = \{x \in G \mid m'x = 0\}$. Infatti il contenimento $\subseteq$ è ovvio, mentre $\supseteq$ utilizza ancora a, b dati da Bezout: se $x \in G_{m'}$ $x = amx + bm'x = amx = m(ax)$. Analogamente $m'G = G_m$.

Da $G \cong mG \times m'G = G_{m'} \times G_m$ segue allora $\#G_m \#G_{m'} = mm'$. Poiché l'ordine di un elemento deve dividere l'ordine del sottogruppo, guardando i primi che possono dividere $\#G_m, \#G_{m'}$, necessariamente si deve avere $\#G_m = m, \#G_{m'} = m'$. Per lo stesso motivo e usando le cardinalità $\forall p_i$ divisore di m si ha anche $G(p_i) = G_m(p_i)$ e analogamente con m'. Quindi le componenti di p-torsione si partizionano tra $G_m, G_{m'}$. Poiché $m, m' < \#G$, usiamo l'ipotesi induttiva e concludiamo:

$G \cong G_{m'} \times G_m \cong \prod_{p_i|m'} G_{m'}(p_i) \times \prod_{p_i|m} G_m(p_i) = \prod_{p_i|m'} G(p_i) \times \prod_{p_i|m} G(p_i)$.

Corollario - 1: Sia G abeliano finito, allora $\forall p$ primo $\#G(p) = p^r$ con $r = v_p(\#G)$.

dim. Basta guardare le cardinalità dei fattori nella scomposizione data dal teorema, notando che in $\#G(p)$ può e deve comparire solo p.

Corollario - 2: Sia G abeliano finito, allora la decomposizione di G come prodotto diretto di p-gruppi esiste ed è unica (ed è quella data dall'enunciato del teorema).

dim. Le cardinalità dei p-gruppi sono fissate dal fatto che il loro prodotto deve essere $\#G$. A questo punto l'unica possibilità nel caso di due diverse scomposizioni (isomorfe, perché isomorfe a G) è che i p-gruppi corrispondenti allo stesso primo siano a due a due isomorfi, il che implica che sono la stessa composizione. Siano infatti H_1, H_2 i due p-gruppi in questione, relativi al primo p, e sia $n = \#G = p^k m$ con $(m, p) = 1$. Allora $H_1 \cong mG \cong H_2$ (moltiplicando ogni elementi del prodotto diretto per m tutte le componenti relative ai primi divisori di m diventano 0).

Teorema - 2: Sia G p-gruppo abeliano. Allora esistono $r_1 \geq \cdots \geq r_t$ univocamente determinati tali che $G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$.

dim. Sia $\#G = p^n$ e procediamo per induzione su n. Il passo base è chiaro. Per il passo induttivo, sia $x_1 \in G$ di ordine massimo, $\text{ord}(x_1) = p^{r_1}$. Se $r_1 = n$ $G \cong \mathbb{Z}/p^n\mathbb{Z}$ e si ha la tesi. Altrimenti consideriamo

$G/\langle x_1\rangle$. Esso è un p-gruppo non banale di cardinalità strettamente inferiore a p^n, e posso dunque applicargli l'ipotesi induttiva, ottenendo (prendo i generatori dei gruppi ciclici) $\mathbb{Z}/p^{r_2}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{r_t}\mathbb{Z}\cong G/\langle x_1\rangle = \langle\overline{x}_2\rangle\langle\overline{x}_3\rangle\ldots\langle\overline{x}_t\rangle$ con $\mathrm{ord}(x_i)=p^{r_i}$ e $r_2\geq r_3\geq\cdots\geq r_t$.

lemma: $\forall\overline{x}\in G/\langle x_1\rangle\ \exists x\in\pi^{-1}(\overline{x})$ tale che $\mathrm{ord}(x)=\mathrm{ord}(\overline{x})$.

dim. Sia $y\in\pi^{-1}(\overline{x})$: cerchiamo tale elemento in $y+\langle x_1\rangle=\{y+ax_1\mid a\in\mathbb{Z}\}=\pi^{-1}(\overline{x})$. Sia $p^r=\mathrm{ord}(\overline{x})$, $r\leq r_1$ perché per omomorfismo e per massimalità di r_1 si ha $p^r=\mathrm{ord}(\overline{x})\mid\mathrm{ord}(y)\mid p^{r_1}$. Analogamente anche $\forall a\in\mathbb{Z}\ p^r=\mathrm{ord}(\overline{x})\mid\mathrm{ord}(y+ax_1)$, dunque $\mathrm{ord}(y+ax_1)=p^r\Leftrightarrow p^r(y+ax_1)=0$. Abbiamo $0=\pi(p^ry)\Rightarrow p^ry\in\mathrm{Ker}(\pi)=\langle\overline{x}_1\rangle$, dunque $\exists b\in\mathbb{Z}\ p^ry=bx_1$. Sappiamo inoltre $0=p^{r_1}y=p^{r_1-r}(p^ry)=p^{r_1-r}(bx_1)\Rightarrow p^{r_1}=\mathrm{ord}(x_1)\mid p^{r_1-r}b\Rightarrow\exists c\in\mathbb{Z}\ b=p^rc$. Allora $y-cx_1$ è l'elemento cercato, infatti $p^r(y-cx_1)=p^ry-p^rcx_1=bx_1-bx_1=0$.

Consideriamo $x_2,\ldots,x_t$ dati dal lemma per $\overline{x}_2,\ldots,\overline{x}_t$. Sia $H=\langle x_2,\ldots,x_t\rangle$. Dimostriamo $\pi|_H$ isomorfismo. È chiaramente suriettiva perché $\pi|_H(x_i)=\overline{x}_i$ per $i=2,\ldots,t$. Inoltre:

$$\begin{aligned}\mathrm{Ker}(\pi|_H)&=\{h\in H\ \mid\ \pi(h)=0\}=\\&=\{a_2x_2+\cdots+a_tx_t\in H\ \mid\ \overline{0}=\pi(h)=a_2\overline{x}_2+\cdots+a_t\overline{x}_t\}=\\&=\{a_2x_2+\cdots+a_tx_t\in H\ \mid\ a_i\overline{x}_i=\overline{0}\ \forall i=2,\ldots,t\}=\\&=\{a_2x_2+\cdots+a_tx_t\in H\ \mid\ p^{r_i}\mid a_i\ \forall i=2,\ldots,t\}=\\&=\{a_2x_2+\cdots+a_tx_t\in H\ \mid\ a_ix_i=0\ \forall i=2,\ldots,t\}=\{0\}.\end{aligned}$$

Quindi $H\cong\langle\overline{x}_2\rangle\ldots\langle\overline{x}_t\rangle\cong\langle x_2\rangle\ldots\langle x_t\rangle$. Se dimostriamo $G\cong\langle x_1\rangle\times H$, segue la tesi. Verifichiamo che sono soddisfatte le ipotesi del teorema di decomposizione in prodotto diretto:

- $\langle x_1\rangle+H=G$: $\forall x\in G$ vale che $\pi(x)=a_2\overline{x}_2+\cdots+a_t\overline{x}_t\Rightarrow\pi(x-(a_2x_2+\cdots+a_tx_t))=0\Rightarrow x-(a_2x_2+\cdots+a_tx_t)\in\langle x_1\rangle$;
- $\langle x_1\rangle\cap H=\{e\}$: basta notare che $\{0\}=\mathrm{Ker}(\pi|_H)=\mathrm{Ker}(\pi)\cap H=\langle x_1\rangle\cap H$.

Dunque $G\cong\langle x_1\rangle\times\ldots\langle x_t\rangle$.

Per l'unicità procediamo sempre per induzione. Nel passo base è chiaramente ovvia, perché può essere solo isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Per il passo induttivo supponiamo che esistano due scritture $\mathbb{Z}/p^{r_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{r_t}\cong\mathbb{Z}/p^{q_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{q_s}$,($r_i$ e q_i crescenti). Poiché i campi sono isomorfi l'ordine massimo di un loro elemento deve essere lo stesso, e quindi $p^{r_t}=p^{q_s}\Rightarrow r_t=q_s$. Quozientiamo allora i due gruppi per $\mathbb{Z}/p^{r_t}$. Otteniamo due scritture $\mathbb{Z}/p^{r_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{r_{t-1}}\cong\mathbb{Z}/p^{q_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{q_{s-1}}$ che per ipotesi induttiva sono la stessa, e quindi $t=s$ e $r_i=q_i\forall i=1,\ldots,t$.

Teorema - struttura dei gruppi abeliani finiti: Sia G abeliano finito. Allora esistono univocamente determinati $n_1,\ldots,n_t$ tali che $G\cong\mathbb{Z}/n_1\mathbb{Z}\times\cdots\times\mathbb{Z}/n_t\mathbb{Z}$ e $n_t\mid n_{t-1}\mid\cdots\mid n_1$.

dim. Sia $\#G=\prod_{i=1}^s p_i^{\alpha_i}$ con p_i primi. Mettiamo insieme i due teoremi appena visti.

$$\begin{aligned}G&\cong G(p_1)\times\cdots\times G(p_s)\cong&(1)\\&\cong\mathbb{Z}/p_1^{r_{1,1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_1^{r_{1,t_1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{r_{s,1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{r_{s,t_s}}\mathbb{Z}\cong&(2)\\&\cong\mathbb{Z}/p_1^{r_{1,1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_1^{r_{1,t}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{r_{s,1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{r_{s,t}}\mathbb{Z}\cong&(3)\\&\cong\mathbb{Z}/p_1^{r_{1,1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{r_{s,1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_1^{r_{1,t}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{r_{s,t}}\mathbb{Z}\cong&(4)\\&\cong\mathbb{Z}/n_1\mathbb{Z}\times\times\cdots\times\mathbb{Z}/n_t\mathbb{Z}&(5)\end{aligned}$$

Motivazioni dei vari passaggi:

(1) applichiamo il teorema 1

(2) applichiamo il teorema 2, e chiamiamo $r_{i,j}$ gli esponenti ottenuti per il primo p_i, $1 \leq j \leq t_i$; si ha quindi $r_{i,1} \geq \cdots \geq r_{i,t_i} \forall i = 1, \ldots, s$

(3) imponiamo wlog che le scritture abbiano tutte la stessa lunghezza, estendendole eventualmente alla massima, che indichiamo con t, con dei gruppi banali ($\forall i = 1, \ldots, s \; r_{i,j} = 0 \; \forall j > t_i$)

(4) riarrangiamo i termini

(5) applichiamo TCR raggruppando blocchi di termini coprimi: $n_k = \prod_{i=1}^{s} p_i^{r_{i,k}}$ e quindi, dal fatto che gli $r_{i,k}$ sono ordinati (rispetto a k) in senso decrescente, si ha $n_t \mid n_{t-1}, \ldots, n_2 \mid n_1$

Per l'unicità ripercorriamo i passaggi al contrario, sfruttando il fatto che si ha unicità nei teoremi 1 e 2.

1.7 Fatti utili sui gruppi finiti

Proposizione - gruppo finito non è unione di sottogruppi coniugati: Sia G finito e $H < G$ sottogruppo. Allora $\bigcup_{g \in G} gHg^{-1} = G \Leftrightarrow H = G$

dim. La freccia "$\Leftarrow$" è ovvia. Si nota che l'unione è un'unione di $\#G$ gruppi, che però non sono necessariamente tutti distinti. In particolare:

$$g_1 H g_1^{-1} = g_2 H g_2^{-1} \Leftrightarrow g_2^{-1} g_1 H g_1^{-1} g_2 = H \Leftrightarrow g_2^{-1} g_1 \in N_G(H).$$

Quindi ogni gruppo compare $\#N_G(H)$ volte, da cui segue che i gruppi distinti sono $n = \#G/\#N_G(H)$. Potremmo notare che se vale $N_G(H) \gneq H$ abbiamo già chiuso per cardinalità. Tuttavia, possiamo raffinare la stima: ciascun gruppo gHg^{-1} è in bigezione naturale con H e quindi ha $\#H$ elementi. Ma essendo gruppi, certamente tutti contengono l'identità. Quindi gli elementi distinti nell'unione $\bigcup_{g \in G} gHg^{-1}$ sono al più $n \cdot (\#H - 1) + 1$, ovvero:

$$\# \bigcup_{g \in G} gHg^{-1} \leq \#G/\#N_G(H) \cdot (\#H - 1) + 1 \leq \#G/\#H \cdot (\#H - 1) + 1 = \#G - \#G/\#H + 1,$$

che è minore di $\#G$ se $H \neq G$.

Proposizione - centro di un p-gruppo: Sia G tale che $\#G = p^n$, con p primo. Allora $Z(G) \neq \{e\}$.

dim. Consideriamo la formula delle classi modulo p. Se fosse $\#Z(G) = 1$ allora $\sum \frac{\#G}{\#Z_G(g)} = \sum \frac{p^n}{\#Z_G(g)}$ non sarebbe divisibile per p, e quindi almeno uno dei termini dovrebbe non essere divisibile per p. L'unica possibilità è che si abbia $\frac{\#G}{\#Z_G(g)} = 1$ per un qualche g, ossia $Z_G(g) = G$, assurdo perché $g \notin Z(G)$.

Proposizione - gruppi di ordine p^2: Sia G con $\#G = p^2$, con p primo. Allora $G \cong \mathbb{Z}/p^2\mathbb{Z}$ oppure $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In particolare G è abeliano.

dim. Dimostriamo innanzitutto che G è abeliano. Le possibili cardinalità di $Z(G)$ sono solo $1, p, p^2$. $\#Z(G) = 1$ è esclusa dalla proposizione precedente. Non può essere neanche $\#Z(G) = p$, infatti si avrebbe $[G : Z(G)] = p \Rightarrow G/Z(G)$ ciclico $\Rightarrow G$ abeliano $\Rightarrow \#Z(G) = p^2$, contro l'ipotesi $\#Z(G) = p$. Necessariamente allora $\#Z(G) = p^2$, i.e. G è abeliano.

Distinguiamo ora due casi: se esiste un elemento di ordine p^2 allora G è ciclico, se invece un tale elemento non esiste, per il teorema di Lagrange tutti gli elementi eccetto il neutro hanno ordine p. Sia x un tale

elemento e $y \in G \setminus \langle x \rangle$. $\langle x \rangle \cap \langle y \rangle = \{e\}$ perché se avessero in comune un elemento $z \neq e$ di ordine p si avrebbe l'assurdo $\langle x \rangle = \langle z \rangle = \langle y \rangle$. Poiché G è abeliano, sia $\langle x \rangle$ che $\langle y \rangle$ sono normali in G. Dal teorema di decomposizione in prodotto diretto segue $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proposizione - gruppi di ordine pq: Sia G tale che $\#G = pq$, con $p < q$ primi. Se $p \nmid q-1$ allora necessariamente $G \cong \mathbb{Z}/pq\mathbb{Z}$, altrimenti a questa possibilità si aggiunge $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

dim. Per il teorema di Cauchy $\exists x, y \in G$ $\mathrm{ord}(x) = q, \mathrm{ord}(y) = p$. Se per assurdo esistesse $z \in G \setminus \langle x \rangle$ di ordine q, allora avrei $\langle x \rangle \cap \langle z \rangle = \{e\}$ e quindi l'assurdo $\#\langle x \rangle\langle z \rangle = q^2 > pq$. Dunque $\langle x \rangle$ è l'unico sottogruppo di ordine q, quindi è caratteristico e in particolare normale. $\langle x \rangle \cap \langle y \rangle = \{e\}$ perché l'ordine di un elemento nell'intersezione divide sia p che q, che sono coprimi. Segue $\#\langle x \rangle\langle y \rangle = pq$, cioè $G = \langle x \rangle\langle y \rangle$. Per il teorema di decomposizione in prodotto semidiretto si ha allora $G \cong \langle x \rangle \rtimes_\varphi \langle y \rangle$ dove φ è l'azione per coniugio di $\langle y \rangle$ su $\langle x \rangle$, quindi un omomorfismo $\varphi : \langle y \rangle \to \mathrm{Aut}(\langle x \rangle)$ che corrisponde a un omomorfismo $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ ($\cong \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$). Le possibili cardinalità dell'immagine di φ sono 1 o p, ma per Lagrange l'immagine può avere cardinalità p solo se $p \mid q-1$. Quindi:

- se $p \nmid q-1$ l'unica possibilità è l'omomorfismo banale, nel cui caso il prodotto è diretto;
- se $p \mid q-1$ esistono anche omomorfismi f non banali, ognuno univocamente determinato dall'immagine di 1. $\mathrm{ord} f(1) = p \Rightarrow f(1) = k^{\frac{q-1}{p}}$ per un $k \in \{1, \dots, p-1\}$. Quindi, detta $f^{(k)}$ la funzione $f^{(k)}(1 \mapsto k^{\frac{q-1}{p}})$, vale $f = f^{(k)}$ per qualche k. Data $\beta \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ definita da $\beta(1 \mapsto k^{-1})$ vale $\forall i \in \mathbb{Z}/p\mathbb{Z}$ $(f^{(k)} \circ \beta)(i) = f^{(k)}(i\beta(1)) = i\beta(1)f^{(k)}(1) = i\beta(1)k^{\frac{q-1}{p}} = i(ap+1)^{\frac{q-1}{p}} = i^{\frac{q-1}{q}} = f^{(1)}(i)$, dunque $f^{(k)} \circ \beta = f^{(1)}$. Per il lemma sull'isomorfismo di prodotti semidiretti si ha $\mathbb{Z}/q\mathbb{Z} \rtimes_{f^{(1)}} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{f^{(k)}} \mathbb{Z}/p\mathbb{Z}$, dunque il prodotto semidiretto non banale $\langle x \rangle \rtimes_\varphi \langle y \rangle$ è unico a meno di isomorfismo.

Proposizione - gruppi di ordine $2d$: Sia G tale che $\#G = 2d$, con d dispari. Allora G ha un sottogruppo di indice 2 (che quindi è normale in G).

dim. Per il teorema di Cauchy $\exists x \in G$ $\mathrm{ord}(x) = 2$. Consideriamo l'immersione del teorema di Cayley, $f : G \hookrightarrow S_{2d}$. Sia $H = f^{-1}(A_{2d}) = f^{-1}(A_{2d} \cap f(G))$. Per teorema di corrispondenza, $[G : H] = [f(G) : A_{2d} \cap f(G)]$, dove il secondo termine può essere solo 1 o 2. Infatti $A_{2d} \cap f(G) = \mathrm{Ker}(\mathrm{sgn}\mid_{f(G)})$ e quindi $f(G)/(A_{2d} \cap f(G)) \cong Imm(\mathrm{sgn}\mid_{f(G)}) \subseteq \{\pm 1\}$, da cui segue $[f(G) : A_{2d} \cap f(G)] \leq 2$. Segue dalle proprietà viste dell'embedding di Cayley che se $\mathrm{ord}(x) = 2$ allora $f(x)$ è una permutazione formata da d 2-cicli, quindi in particolare $f(x)$ ha segno dispari e $f(x) \notin A_{2d}$. Quindi $H \neq G \Rightarrow [G : H] = 2$. Alternativamente, per ogni $H < S_n$ se esiste $\sigma \in H$ $\mathrm{sgn}(\sigma) = -1$, allora $\tau \mapsto \sigma \circ \tau$ è una bigezione tra gli elementi pari e gli elementi dispari di H.

Proposizione - condizione sufficiente per normalità: Sia G finito. Se $H < G$ ha indice il più piccolo primo che divide $\#G$, allora H è normale.

dim. Considero l'azione φ di G sull'insieme $X = \{gH | g \in G\}$ data dalla moltiplicazione a sinistra. Per definizione si ha $\#X = p$. Ricordiamo che un'azione è definita come un omomorfismo $\varphi : G \to S(X) \cong S_p$. Sia K il suo nucleo, voglio dire $K = H$. Per il primo teorema di omomorfismo, $G/K \cong \mathrm{Imm}(\phi) < S_p$, quindi $\#(G/K) | p!$ e chiaramente $\#(G/K) | \#G$. Segue $\#(G/K) | MCD(\#G, p!) = p$, dove l'ultima uguaglianza segue dal fatto che p è il *minimo* primo che divide $\#G$. Non può essere $K = G$ poiché $\forall g \in G$ $gH = H \Rightarrow H = G$, contro l'ipotesi. Necessariamente allora $\#(G/K) = p$. $H \leq K$ implica $p = \#(G/K) \leq \#(G/H) = p$, da cui $K = H$.

seconda dim: Vale $H \lhd G \Leftrightarrow \forall g \in G, h \in H$ $hgH = gH$. Considero l'azione φ di G sull'insieme $X = \{gH | g \in G\} \setminus \{eH\}$ data dalla moltiplicazione a sinistra, per definizione si ha $\#X = p-1$. L'azione

è ben definita. Ricordiamo che un'azione è definita come un omomorfismo $\varphi : G \to S(X) \cong S_{p-1}$. Per quanto detto, $H \lhd G \Leftrightarrow \text{Imm}(\varphi) = \{id_X\}$. Si ha $\#\text{Imm}(\varphi) \mid \#S_{p-1} = (p-1)!$ e $\#\text{Imm}(\varphi) \mid \#G$, ma allora $\#\text{Imm}(\varphi) | MCD(\#G, (p-1)!) = 1$, cioè $\text{Imm}(\varphi) = \{id_X\}$.

Proposizione - sottogruppo normale contenuto nel centro: Sia G finito. Se $H \lhd G$ ha ordine p il più piccolo primo che divide $\#G$, allora H è contenuto nel centro.

dim. Nello stesso spirito della dimostrazione precedente, considero l'azione per coniugio di G su $X = H \setminus \{e\}$, ben definita per normalità di H e poiché $ghg^{-1} = e \Leftrightarrow h = e$. L'azione è un omomorfismo $\varphi : G \to S(X) \cong S_{p-1}$. $H \subset Z(G)$ se e solo se l'immagine di φ è banale, ma ciò è sicuramente verificato poiché $\#\text{Imm}(\varphi) \mid MCD(\#G, \#S_{p-1}) = 1$.

Definizione - sottogruppo derivato/dei commutatori: il commutatore di due elementi $x, y \in G$ si indica con $[x, y] := xyx^{-1}y^{-1}$. Il sottogruppo generato da tutti i commutatori si indica con G'.

Proposizione - proprietà del sottogruppo derivato:

- è caratteristico (e quindi anche normale)

  dim. Basta osservare che per ogni omomorfismo f con dominio G si ha $f([x, y]) = [f(x), f(y)]\ \forall x, y \in G$. Quindi un qualsiasi automorfismo manda l'insieme dei commutatori in sé stesso, e di conseguenza G' in sé stesso.

- G/G' è abeliano (tale gruppo è detto l'*abelianizzato* di G).

  dim. $\forall g, h \in G$ si ha $gG' \cdot hG' = hG' \cdot gG' \Leftrightarrow ghG' = hgG' \Leftrightarrow ghg^{-1}h^{-1} \in G'$ che è chiaro perché è un commutatore.

- $\varphi : G \to H$ omomorfismo con H abeliano $\Rightarrow G' \subset \text{Ker}(\varphi)$

  dim. Basta osservare che se H abeliano

  $$f([x, y]) = [f(x), f(y)] = f(x)f(y)f(x)^{-1}f(y)^{-1} = f(x)f(x)^{-1}f(y)f(y)^{-1} = e_H \quad \forall x, y \in G$$

  . Quindi i commutatori sono tutti nel nucleo e di conseguenza anche G'.

- H abeliano $\Rightarrow Hom(G, H)$ e $Hom(G/G', H)$ sono in bigezione.

  dim. Costruiamo le sue corrispondenze come segue.

  - $\varphi \in Hom(G, H)$ la mandiamo in $\tilde{\varphi} \in Hom(G/G', H)$ data dal 1° teorema di omomorfismo (visto che $G' \subseteq \text{Ker}(\varphi)$). Segue dall'unicità nel teorema che sono tutte distinte e quindi questa mappa è iniettiva.
  - $\varphi \in Hom(G, H)$ la mandiamo in $\varphi \circ \pi \in Hom(G/G', H)$ dove π è la proiezione $\pi : G \to G/G'$. Anche questa mappa è chiaramente iniettiva, visto che $G' \subseteq \text{Ker}(\varphi)$ e quindi se due mappe vengono mandate nella stessa allora coincidono anche su tutto G.

Proposizione - prodotti diretti "belli": Se $G \cong H \times K$ con H, K finiti tali che $(\#H, \#K) = 1$ allora $\{e_H\} \times K$ e $H \times \{e_K\}$ sono caratteristici in G.

dim. Dimostriamo che $\{e_H\} \times K$ e $H \times \{e_K\}$ sono gli unici sottogruppi delle rispettive cardinalità, quindi caratteristici. Basta dire che nelle ipotesi per ogni sottogruppo $L \leq G$ vale $L = \langle \pi_H(L) \times \{e_K\}, \{e_H\} \times \pi_K(L) \rangle$ e quindi $\#L = \#\pi_H(L)\#\pi_K(L)$. Vale sempre $L \subseteq \langle \pi_H(L) \times \{e_K\}, \{e_H\} \times \pi_K(L) \rangle$. L'altro contenimento segue da $(\#H, \#K) = 1$, infatti per Bezout $\forall (h,k) \in L \ \exists a, b \in \mathbb{N} \ (h,k)^a = (h, e_K)$ e $(h,k)^b = (e_H, k)$.

Proposizione - automorfismi in un prodotto diretto: Se $G \cong H \times K$ e $\{e_H\} \times K$ e $H \times \{e_K\}$ sono caratteristici in G, allora $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

dim. Per ogni $\varphi \in \mathrm{Aut}(G)$ sia $\varphi_H \in \mathrm{Aut}(H)$ definito mediante $\varphi_H(x) := \pi_H \circ \varphi(x, e_K)$ (chiaramente è un automorfismo) e analogamente $\varphi_K \in \mathrm{Aut}(K)$.
Consideriamo allora $\Phi : \mathrm{Aut}(G) \to \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ dato da $\Phi(\varphi) = (\varphi_H, \varphi_K)$.

- è omomorfismo: basta notare che $(\psi \circ \varphi)_H = \psi_H \circ \varphi_H$;
- è iniettivo: $\Phi(\varphi) = (id_H, id_K) \Rightarrow \forall (h,k) \in G \ \varphi((h,k)) = (h,k) \Rightarrow \varphi = id_G$.

Proposizione - (*) centro di un prodotto semidiretto: Sia $G \cong H \rtimes_\varphi K$ con H abeliano. Allora

$$Z(G) \cong \left(\bigcap_{k \in K} Fix(\varphi_k) \right) \times (\mathrm{Ker}(\varphi) \cap Z(K)).$$

dim. Un elemento (a,b) sta nel centro di G se e solo se commuta con gli elementi dell'insieme di generatori $H \times \{e_K\} \cup \{e_H\} \times K$:

- $(a,b)(e_H, b') = (a\varphi_b(e_H), bb') = (a, bb')$ e $(e_H, b')(a,b) = (\varphi_{b'}(a), b'b)$ coincidono per ogni $b' \in K$ se e solo se $b \in Z(K)$ e $a \in Fix(\varphi_{b'})$;
- $(a,b)(a', e_K) = (a\varphi_b(a'), b)$ e $(a', e_K)(a,b) = (a'a, b) = (aa', b)$ coincidono per ogni $a' \in H$ se e solo se $b \in \mathrm{Ker}(\varphi)$.

Quindi $(h,k) \in Z(G) \Leftrightarrow h \in \bigcap_{k \in K} Fix(\varphi_k) \wedge k \in \mathrm{Ker}(\varphi) \cap Z(K)$, come voluto.

Proposizione - (*) intersezione dei p-Sylow con il centro: L'intersezione di un p-Sylow con il centro non dipende dal p-Sylow scelto.

dim. Sia S un fissato p-Sylow. Ricordiamo che i p-Sylow sono tutti coniugati, quindi dato Q un qualsiasi p-Sylow $\exists g \in G \ Q = gSg^{-1}$. Poiché ogni elemento del centro è invariante per qualsiasi coniugio si ha: $Q \cap Z(G) = gSg^{-1} \cap Z(G) = gSg^{-1} \cap gZ(G)g^{-1} = g(S \cap Z(G))g^{-1} = S \cap Z(G)$.

1.8 Il gruppo diedrale

Il gruppo diedrale D_n è il gruppo delle isometrie di un fissato n-agono regolare, diciamo quello inscritto nella circonferenza unitaria e con un vertice in $(1,0)$, con l'operazione di composizione. Chiamiamo r la rotazione di $2\pi/n$ in senso antiorario, s la simmetria rispetto all'asse x. Chiaramente tutte le rotazioni, che sono n contando l'identità (rotazione banale) e sono multiple di r per come è stata scelta, sono ancora in D_n, così come ci sono in realtà n simmetrie (quelle relative all'asse origine-vertice al variare dei vertici se n è dispari, e quelle relative agli assi passanti per vertici opposti o per i punti medi di lati opposti se n è pari). Questi sono chiaramente $2n$ elementi distinti, quindi $\#D_n \geq 2n$. Dimostriamo che sono gli unici elementi mostrando che $\#D_n = 2n$.

dim. Chiamiamo i vertici, in senso antiorario a partire da $(1,0)$, $V_1, V_2, \dots, V_n$ e sia $\sigma \in D_n$. Poiché σ é isometria, manda vertici in vertici, e inoltre una volta fissata l'immagine di V_1, V_2, è tutto univocamente determinato. Per V_1 abbiamo n scelte (tutti i vertici), mentre per V_2 ne abbiamo 2 (i due vicini di $\sigma(V_1)$). Quindi $\#D_n = 2n$.

Notiamo ora che sr^k è un'altra simmetria.

dim. Un'isometria è in particolare un'applicazione lineare. Consideriamo le matrice 2×2: R relativa a r e S relativa a s. Si nota che un'isometria in D_n è una simmetria assiale se e solo se la sua matrice ha determinante -1, è una rotazione se e solo se la sua matrice ha determinante 1. Si ha allora la tesi usando la moltiplicatività del determinante.

Quindi $s, sr, sr^2, \dots sr^{n-1}$ sono le n simmetrie descritte prima, in quanto tutte distinte. Si ha quindi

$$D_n = \langle r, s \rangle$$

Per lavorare con il diedrale, è allora fondamentale la seguente relazione: $srs = r^{-1}$

dim. r manda V_i in V_{i+1}, s manda V_i in V_{n+1-i} (guardando gli indici modulo n) e quindi srs manda $V_1 \mapsto V_1 \mapsto V_2 \mapsto V_{n-1}$, $V_2 \mapsto V_{n-1} \mapsto V_1 \mapsto V_1$, da cui segue la tesi.

La presentazione di D_n è $\langle x, y \mid x^n = id, y^2 = id, yxyx = id \rangle$.
Da quella relazione, con manipolazioni algebriche, si ricava

$$s^a r^b s^c r^d = s^{a+c} r^{(-1)^c b + d}.$$

Questa relazione ci fa già intuire la struttura di prodotto semidiretto. Si dimostra infatti

$$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

dim. Il sottogruppo delle rotazioni $R = \langle r \rangle$ è normale perché ha indice 2, è chiaramente disgiunto da $\langle s \rangle$ per quanto detto precedentemente sui determinanti, e si è visto prima che $\langle r \rangle \langle s \rangle = \langle r, s \rangle = D_n$. Dal teorema di decomposizione in prodotti semidiretti si ha allora la tesi: $D_n \cong \langle r \rangle \rtimes \langle s \rangle \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Infine studiamone i sottogruppi. Come detto sopra, il sottogruppo delle rotazioni $R = \langle r \rangle$ è normale perché ha indice 2. Inoltre è ciclico, quindi ha esattamente un sottogruppo di ordine d, $\forall d \mid n$. Tutti questi sottogruppi sono caratteristici in R perché sono gli unici del proprio ordine, quindi sono normali in D_n. Perciò i sottogruppi generati da un qualsiasi multiplo della rotazione r sono tutti normali.
Notiamo ora che se in un gruppo H ci sono due simmetrie distinte, allora c'è anche una rotazione: $sr^a, sr^b \in H \Rightarrow sr^a sr^b = r^{b-a} \in H$. Tutti i gruppi restanti sono allora quelli generati da una rotazione (quella di ordine massimo nel sottogruppo) e una simmetria. Sia $H = \langle r^d, sr^h \rangle$. Senza perdita di generalità possiamo supporre:

- $0 \leq h < d$: se $h = md + x$ con $0 \leq x < d$ (resto) e $r^d \in H$ si ha $sr^x \in H \Leftrightarrow sr^h = sr^x (r^d)^m \in H$;
- $0 \leq d < n$, $d|n$: basta notare che $\langle r^d \rangle = \langle r^{xd} \rangle$ per ogni x coprimo con n e d divisore.

Imponendo queste condizioni su d, h notiamo che i gruppi trovati sono tutti distinti. In altre parole, $\langle r^{d_1}, sr^{h_1} \rangle = \langle r^{d_2}, sr^{h_2} \rangle \Leftrightarrow (d_1, h_1) = (d_2, h_2)$ (se d_1, h_1 sono come su e anche d_2, h_2).

dim. Sia $H_i = \langle r^{d_i}, sr^{h_i} \rangle$ per $i = 1, 2$. Notiamo che $H_1 = H_2 \Rightarrow \langle r^{d_1} \rangle = H_1 \cap R = H_2 \cap R = \langle r^{d_2} \rangle$. Per quanto osservato prima, ciò implica $d_1 = d_2$. Si può ora notare che $H_i = \langle sr^{h_i} \rangle \langle r^{d_i} \rangle$ (basta osservare che $r^{d_i} sr^{h_i} = sr^{h_i - d} \in \langle sr^{h_i} \rangle \langle r^{d_i} \rangle$). Allora $sr^{h_2} \in H_1 \Rightarrow sr^{h_2} = (sr^{h_1})^a (r^{d_1})^b = s^a r^{ah_1 + d_1}$ da cui segue che a è dispari (o il membro di destra non sarebbe una simmetria) e quindi senza perdita di generalità $a = 1$ (le simmetrie hanno ordine 2). Ma allora $h_1 + d_1 = ah_1 + d_1 \equiv h_2 \pmod{n}$. In particolare $h_1 \equiv h_2 \pmod{d_1}$. Ma $d_1 = d_2$ e l'ipotesi implicano che sono entrambi ridotti modulo d_1 e quindi non si ha solo congruenza ma uguaglianza.

Notiamo che questi sottogruppi non sono normali $s\langle r^d, sr^h \rangle s = \langle sr^d s, r^h s \rangle = \langle r^{-d}, sr^{-h} \rangle = \langle r^d, sr^{d-h} \rangle \neq \langle r^d, sr^h \rangle$ per quanto detto prima.
Riassumendo, abbiamo tutti e soli i sottogruppi:

- $R = \langle r \rangle$ delle rotazioni, che è normale e caratteristico (non ci elementi di ordine n fuori da $R \cong \mathbb{Z}/n\mathbb{Z}$)
- $\langle r^d \rangle$ con $d|n$, che sono caratteristici in R e dunque normali in D_n
- $\langle r^d, sr^h \rangle$ con $d|n, 0 \leq h < n$, che non sono normali in D_n

1.9 Il gruppo simmetrico

Proposizione - le trasposizioni generano S_n: Ogni permutazione σ di S_n si può scrivere come composizione di trasposizioni

dim. Un ciclo è composizione di trasposizioni, infatti $(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_1, a_3) \ldots (a_1, a_k)$. Ciascuna permutazione può essere rappresentata come prodotto di cicli disgiunti, quindi abbiamo finito.

Proposizione - classi di coniugio: $\forall \sigma \in S_n$ $Cl(\sigma)$ contiene tutte le permutazioni di S_n che hanno la stessa struttura in cicli di σ.
Ad esempio, $Cl((1,2)) = \{\text{trasposizioni}\}$, in S_5 $Cl((1,2)(3,4,5)) = \{\text{2+3-cicli}\}$.

dim. Fissiamo $\sigma = (a_1^1, \ldots, a_{k_1}^1)(a_1^2, \ldots, a_{k_2}^2) \ldots (a_1^c, \ldots, a_{k_c}^c) \in S_n$ e X insieme delle permutazioni di S_n con la stessa struttura in cicli di σ.
Si mostra facilmente che $\forall \tau \in S_n$, $\tau \circ \sigma \tau^{-1} = (\tau a_1^1, \ldots, \tau a_{k_1}^1)(\tau a_1^2, \ldots, \tau a_{k_2}^2) \ldots (\tau a_1^c, \ldots, \tau a_{k_c}^c) \in X$. Quindi $Cl(\sigma) \subseteq X$.
Sia $\sigma' = (b_1^1, \ldots, b_{k_1}^1)(b_1^2, \ldots, b_{k_2}^2) \ldots (b_1^c, \ldots, b_{k_c}^c) \in X$; notiamo che $\tau = (a_1^1, b_1^1) \circ \cdots \circ (a_{k_c}^c, b_{k_c}^c)$ è tale che $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. Quindi $\sigma' \subseteq Cl(\sigma)$. Facendo variare σ', $X \subseteq Cl(\sigma)$.

Proposizione - cardinalità di un centralizzatore: Se $\sigma \in S_n$ è formata da $a_i \geq 0$ i-cicli $\forall i = 1, \ldots, n$, vale che

$$\#Z_{S_n}(\sigma) = \prod_{i=1}^{n} (a_i! \cdot i^{a_i}).$$

Ciò ci può aiutare a capire come sono fatti dei centralizzatori semplici oppure, combinato con il lemma normalizzatore-centralizzatore, dei centralizzatori.
Generalmente si cerca di costruire "indovinando" il centralizzatore e poi si dice che è quello per cardinalità. Ad esempio il centralizzatore di un k-ciclo ($a_i = 1$ se $i = k$, $a_i = n - k$ se $i = 1$, $a_i = 0$ altrimenti) secondo la formula ha cardinalità $k \cdot (n-k)!$. Poiché sia il sottogruppo generato dal k-ciclo che il sottogruppo di S_n che permuta gli elementi che non compaiono nel k-ciclo sono banalmente nel centralizzatore (e l'intersezione di questi due sottogruppi è banale) per cardinalità si conclude che il centralizzatore del ciclo è proprio il prodotto di questi due sottogruppi.

dim. Abbiamo infatti visto che per il lemma orbita-stabilizzatore vale $\#Z_{S_n} = \frac{\#S_n}{Cl(\sigma)}$. Sappiamo che $Cl(\sigma)$ è l'insieme di tutte e sole le permutazioni con a_i (fissato da σ) i-cicli. Dobbiamo contare quante sono tali permutazioni. Il conto è puramente combinatorico e si può fare in vari modi, eccone uno:

1. mettiamo in fila in ordine: il primo blocco da 1 casella, il secondo blocco da 1 casella, ... il a_1-esimo blocco da 1 casella, il primo blocco da 2 caselle, ..., il a_2-esimo blocco da 2 caselle, ..., il a_k-esimo blocco da k-caselle; chiaramente in totale ci sono in fila n caselle;
2. riempiamo tali caselle con i numeri da 1 a n in qualche ordine ; questa operazione ci dà una permutazione in $Cl(\sigma)$ se trasformiamo i blocchi di caselle in cicli;
3. ci sono delle ripetizioni, che si manifestano in 2 modi:
   - possiamo scambiare due blocchi da i caselle ottenendo la stessa scrittura in cicli; essendoci a_i i-cicli per ogni i per togliere queste ripetizioni dobbiamo dividere per $\prod_{i=1}^{n} a_i!$;
   - possiamo far ciclare (attenzione: non permutare!) il contenuto di un blocco da i fissato; per tale blocco i modi di ciclare sono i quindi per togliere queste ripetizioni dobbiamo dividere per $\prod_{i=1}^{n} i^{a_i}$ (per ciascun blocco divido per i).

Si ha allora la tesi in quanto

$$\#Cl(\sigma) = \frac{n!}{\prod_{i=1}^{n}(a_i! \cdot i^{a_i})}.$$

Definizione - segno di una permutazione: $\forall \sigma \in S_n$ definiamo

$$\operatorname{sgn}(\sigma) := \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

- le permutazioni con segno 1 sono dette pari, le altre dispari
- si mostra facilmente che se τ trasposizione, $\operatorname{sgn}(\tau) = -1$ e se σ è un k-ciclo, $\operatorname{sgn}(\sigma) = (-1)^{k+1}$
- $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$

  dim.

$$\begin{aligned}
\operatorname{sgn}(\sigma \circ \tau) &= \prod_{1 \le i < j \le n} \frac{\sigma \circ \tau(j) - \sigma \circ \tau(i)}{j - i} = && \text{applicando } \tau^{-1} \\
&= \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{\tau^{-1}(j) - \tau^{-1}(i)} = \\
&= \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} \cdot \frac{j - i}{\tau^{-1}(j) - \tau^{-1}(i)} = \\
&= \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} \prod_{1 \le i < j \le n} \frac{j - i}{\tau^{-1}(j) - \tau^{-1}(i)} = && \text{applicando } \tau \text{ nel secondo fattore} \\
&= \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} \prod_{1 \le i < j \le n} \frac{\tau(j) - \tau(i)}{j - i} = \\
&= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)
\end{aligned}$$

- rifrasando quello appena mostrato, $\operatorname{sgn} : S_n \to \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ è un omomorfismo

Definizione - il sottogruppo alternante: $A_n = \{\sigma \in S_n | \text{sgn}(\sigma) = 1\}$
Proposizione - A_n è normale: A_n è un sottogruppo normale di S_n

dim. Per definizione è il nucleo di sgn come omomorfismo, quindi è un sottogruppo normale. Notare che ciò dimostra anche che è un sottogruppo.

Proposizione - intersezioni con A_n: Se $H < S_n$ vale $[H : H \cap A_n] = 1$ oppure 2

dim. Se $H \subseteq A_n$ è chiaro che $[H : H \cap A_n] = 1$. Supponiamo allora che H contenga un ciclo dispari σ. Considero l'azione per moltiplicazione a sinistra di H sulle classi laterali di $H \cap A_n$. Per quanto già visto $[H : H \cap A_n] = \#\text{orb}(H \cap A_n) = \#\{g(H \cap A_n) | g \in H\}$.

Per ciascuna permutazione dispari $\sigma \in H$ $\sigma(H \cap A_n)$ contiene solo permutazioni dispari ed è quindi disgiunta da $H \cap A_n$, da cui segue che l'orbita ha cardinalità almeno 2. Ma due permutazione σ_1, σ_2 con lo stesso segno sono tali che $\sigma_1(H \cap A_n) = \sigma_2(H \cap A_n)$. Infatti ciò vale $\Leftrightarrow \sigma_2^{-1}\sigma_1 \in H \cap A_n$ banalmente vero. Quindi l'orbita ha cardinalità 2 da cui la tesi.

Proposizione - classi di coniugio in A_n: Sia $\sigma \in A_n$ e $Cl_{A_n}(\sigma)$ la sua classe di coniugio in A_n. Allora $\#Cl_{A_n}(\sigma)$ è uguale a $\#Cl_{S_n}(\sigma)$ oppure a $\frac{1}{2}\#Cl_{S_n}(\sigma)$. Vale inoltre $\#Cl_{S_n}(\sigma) = \#Cl_{A_n}(\sigma) \Leftrightarrow \sigma$ ha almeno un ciclo pari oppure 2 cicli dispari di uguale lunghezza (gli elementi fissati sono cicli di lunghezza 1).

dim. Sia $j = [Z_{S_n}(\sigma) : (Z_{S_n}(\sigma) \cap A_n)] \in \{1, 2\}$. Un'applicazione diretta del lemma orbita-stabilizzatore mostra $\#Cl_{A_n}(\sigma) = \#Cl_{S_n}(\sigma)$ se $j = 2$, $\#Cl_{A_n}(\sigma) = \frac{1}{2}\#Cl_{S_n}(\sigma)$ altrimenti. La seconda parte dell'enunciato è lasciata come esercizio.

Proposizione - generatori di A_n: se $n \geq 3$ i 3-cicli generano A_n; se $n \geq 5$ i $2+2$-cicli generano A_n.

dim. Mostriamo la prima parte dell'enunciato. Tutte le permutazioni sono esprimibili come prodotto di trasposizioni. Ma se $\sigma \in A_n$ allora necessariamente è esprimibile come prodotto di *un numero pari di* trasposizioni (per le proprietà del segno). Basta allora mostrare che i 3-cicli generano $\{(i, j)(k, l) | i \neq j, k \neq l, 1 \leq i, j, k, l \leq n\}$ (visto che ciascuna permutazione si scrive come composizione di un certo numero di elementi di questo tipo). Ma ciò è chiaro perché $(k, j, l)(i, k, j) = (i, j)(k, l)$.

Mostriamo la seconda parte dell'enunciato. Per il punto precedente, basta mostrare che i 2+2-cicli generano i 3-cicli. Ma ciò è vero perché prendendo $i, j, k, l, h \in \{1, \ldots, n\}$ *tutti distinti* (o quelle di dopo non sarebbero 2+2-cicli ma altro), $(h, i)(k, l) \circ (i, j)(h, k) = (i, j, k)$.

Con tutti i lemmi appena visti, possiamo caratterizzare i sottogruppi normali di S_n.
Esempio - sottogruppi normali di S_3: In S_3 i sottogruppi normali sono $\{id\}, A_3 = \langle(1, 2, 3)\rangle, S_3$.

dim. In S_3 la cardinalità di un sottogruppo H può essere solo $1, 2, 3, 6$. Se $\#H = 1$ il sottogruppo è banale e se $\#H = 6$ allora $H = S_3$. Se $\#H = 2$ o 3, essendo primi, il gruppo è ciclico (generato da un 2-ciclo oppure 3-ciclo). Se $H \cong \mathbb{Z}/3\mathbb{Z}$ allora H è normale perché ha indice 2 (minimo primo che divide 6). $H \cong \mathbb{Z}/3\mathbb{Z}$ non può essere normale perché altrimenti S_3 sarebbe abeliano. Quindi l'unico sottogruppo normale non banale è $\langle(1, 2, 3)\rangle = A_3$
Nota: si poteva anche usare che $\#S_3 = pq$ con p, q primi, per dire che $S_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Definizione - sottogruppo di Klein: $K_4 := \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. Si verifica facilmente che è sottogruppo normale di S_4 e che $K_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Esempio - sottogruppi normali di S_4: In S_4 gli unici sottogruppi normali sono $\{id\}, K_4, A_4, S_4$, dove

dim. Abbiamo già visto che tutti quei sottogruppi sono normali. Sia $H \neq \{id\}$ un sottogruppo normale di S_4. Facciamo i casi. Si ricorda che per normalità H è unione di classi di coniugio, e che le classi di coniugio in S_4 sono: trasposizioni, 3-cicli, 2+2-cicli, 4-cicli.

1. H contiene una trasposizione: allora contiene tutte le trasposizioni che però sono generatori di $S_4 \Rightarrow H = S_4$.
2. H contiene un 3-ciclo: allora contiene tutti i 3-cicli, che però sono generatori di A_4, quindi $A_4 \leq H \leq S_4$. Ma A_4 ha indice $2 \Rightarrow H = A_4$ oppure S_4 (non esistono possibilità intermedie).
3. H contiene un 2+2-ciclo: allora contiene il sottogruppo di Klein K_4. Se H contiene un 4-ciclo allora li contiene tutti e si ha in particolare $(1,2)(3,4) \in H$, $(1,2,3,4) \in H \Rightarrow (1,2)(3,4) \circ (1,2,3,4) = (2,4) \in H$ e quindi siamo nel primo caso. Se H non contiene 4-cicli allora o $H = K_4$ o comunque ci riconduciamo a uno dei casi precedenti.
4. H contiene un 4-ciclo: sia esso (a_1, a_2, a_3, a_4). Ma allora contiene anche $(a_1, a_2, a_3, a_4)^2 = (a_1, a_3)(a_2, a_4)$ e ci riconduciamo al caso precedente.

Proposizione - sottogruppi normali di S_n: se $n \geq 5$ gli unici sottogruppi normali di S_n sono $\{id\}, A_n, S_n$.

dim. Sia $H \neq \{id\}$ un sottogruppo normale. Allora H è unione di classi di coniugio e quindi $\forall \sigma \in H$ tutte le permutazioni con la stessa struttura in cicli di σ sono in H. Sia $\sigma \in H, \sigma \neq \{id\}$ e distinguiamo i casi.

- σ è una trasposizione: allora H contiene tutte le trasposizioni (classe di coniugio), ma le trasposizioni generano S_n, quindi si ha $H = S_n$;
- σ è un $(2+2)$-ciclo: allora poiché i $2+2$ cicli generano A_n, si ha $A_n \subseteq H$;
- σ è formata da $k \geq 3$ 2-cicli disgiunti: $\sigma = (a_1, b_1)(a_2, b_2) \dots (a_k, b_k)$ dove i numeri considerati sono tutti distinti. Per la normalità di H l'intera classe di coniugio di σ sta in H e quindi $\tau = (a_1, a_2)(b_1, b_2)(a_3, b_3) \dots (a_k, b_k) \in H$. Ma allora $\sigma\tau = (a_1, b_2)(a_2, b_1) \in H$ e ci riconduciamo al caso precedente;
- σ contiene almeno un ciclo di lunghezza $k \geq 3$: $\sigma = (a_1, \dots, a_k)\sigma'$ dove σ' permuta elementi disgiunti da $a_1, \dots, a_k$. Allora sempre per classe di coniugio $\tau = (a_1, a_2, a_k, \dots, a_3)(\sigma')^{-1} \in H$ (notiamo che l'inversa di una permutazione ha la stessa scrittura in cicli), e quindi $\sigma\tau = (a_1, a_3, a_2)$. Poiché i 3-cicli generano A_n, si ha $A_n \subseteq H$.

Quindi in ogni caso $A_n \subseteq H$. Ma A_n ha indice 2 in S_n, quindi le uniche possibilità per H sono $H = A_n$ oppure $H = S_n$, che sappiamo essere normali.

Proposizione - A_n è semplice: se $n \geq 5$ A_n è semplice, ossia i suoi unici sottogruppi normali sono $\{id\}, A_n$.

dim. Useremo come lemma che se $H \lhd A_n$ contiene un 3-ciclo allora $H = A_n$. Poiché i 3-cicli generano ciò è dimostrato se si mostra che $Cl_{A_n}(\text{3-ciclo}) = Cl_{S_n}(\text{3-ciclo}) = \{\text{3-cicli}\}$. Il centralizzatore di un 3-ciclo in S_n è il sottogruppo da esso generato. Essendo contenuto in A_n è anche il suo centralizzatore in A_n. Ma allora per quanto visto sulle classi di coniugio in A_n si ha la tesi.

Mostriamo ora la semplicità per induzione su n. I passi base $n = 5, 6$ si trattano vedendo le cardinalità delle classi di coniugio delle permutazioni pari e provando a farle sommare ad $\#A_n$ (occhio all'identità).

Per il passo induttivo supponiamo la tesi dimostrata per $n-1$ e mostriamola per n. Sia $H \lhd A_n$. Sia per ogni $i = 1, \dots, n$ $K_i := \{\sigma \in A_n | \sigma(i) = i\} \cong A_{n-1}$. Poiché H è normale in A_n, $H \cap K_i$ è normale in K_i per ogni i. Ma $K_i \cong A_{n-1}$ è semplice, quindi $\forall i$ si ha $K_i \cap H = \{id\}$ oppure K_i.

Notiamo che ciascun K_i contiene un 3-ciclo (basta $n \geq 4$), quindi se per qualche i_0 $K_{i_0} \cap H = K_{i_0} \Rightarrow K_{i_0} \subseteq H$ si ha necessariamente $H = A_n$ per il lemma iniziale.

Si allora $H \cap K_i = \{id\}$ per ogni i e per assurdo $id \neq \sigma \in H$. Prendiamo un qualsiasi 3-ciclo $\tau \in A_n$. Per normalità di H $\tau\sigma^{-1}\tau^{-1} \in H$, e quindi $H \ni \sigma\tau\sigma^{-1}\tau^{-1} = (\sigma\tau\sigma^{-1})\tau^{-1}$ dove i due fattori sono 3-cicli. Questa permutazione muove allora al più 6 elementi, e quindi o è l'identità o ci dà un assurdo se $n \geq 7$ perché si dovrebbe trovare in uno dei K_i. Facendo variare τ possiamo sceglierla in modo che non sia l'identità e ottenere l'assurdo (basta ad esempio che τ muova $\sigma(1)$).

Proposizione - derivato di S_n: $S_n' = A_n$ per ogni n.

dim. Notiamo intanto che per omomorfismo $\text{sgn}([\sigma, \tau]) = \text{sgn}(\sigma)^2\text{sgn}(\tau)^2 = 1$ e quindi $S_n' \subseteq A_n$.
Inoltre il sottogruppo S_n' è caratteristico, e dunque normale, da cui segue $S_n' = \{id\}$ oppure A_n. La prima si esclude perché S_n non è abeliano.

Proposizione - derivato di A_n: se $n \geq 5$ $A_n' = A_n$.
Domanda: chi è A_4'?

dim. Il sottogruppo derivato è caratteristico, e quindi normale. Ma A_n è semplice per n, quindi restano solo le possibilità $A_n' = A_n$ e $A_n' = \{id\}$. Ma quest'ultima implicherebbe che A_n sia abeliano, assurdo.

Proposizione - (*) automorfismi interni: $\forall n$ vale $Z(S_n) = \{id\}$, da cui segue $\text{Inn}(S_n) \cong S_n$.

dim. I casi $n = 2, 3$ si trattano a mano. Sia $id \neq \sigma \in S_n$. Costruiamo $\tau \in S_n$ che non commuti con σ. $\sigma \neq id \Rightarrow \exists k \in \{1, \dots, n\}$ $\sigma(k) \neq k$. Se prendo $j \neq k, \sigma(k), \sigma(\sigma(k))$ e considero $\tau = (k, \sigma(k), j)$ si ha per costruzione $\tau \circ \sigma(k) = j \neq \sigma(\sigma(k)) = \sigma \circ \tau(k)$, e quindi $\tau\sigma \neq \sigma\tau$ come voluto.

Proposizione - (*) automorfismi: $\text{Aut}(S_n) = S_n$ $\forall n \in \mathbb{N} \setminus \{2, 6\}$.

dim. La dimostrazione si divide in due parti:

1. se un automorfismo manda trasposizioni in trasposizioni, allora è interno;
2. un automorfismo manda trasposizioni in trasposizioni se $n \neq 6$;

Per la prima parte, TODO.

Per la seconda, notiamo che un automorfismo preserva gli ordini degli elementi e le classi di coniugio. Quindi, preso $f \in \text{Aut}(S_n)$, si ha che $f((1,2))$ ha ordine 2 (quindi è il prodotto di k 2-cicli) e che $f(Cl((1,2))) = Cl(f((1,2)) \Rightarrow \#Cl((1,2)) = \#Cl(f((1,2))$. Usando la formula per la cardinalità delle classi di coniugio vista a inizio paragrafo, si ha:

$$\#Cl((1,2)) = \frac{n!}{2 \cdot (n-2)!} \qquad \#Cl(f((1,2)) = \frac{n!}{2^k \cdot k!(n-2k)!}$$

Uguagliando le due espressioni, $(n-2)! = 2^{k-1} \cdot k!(n-2k)!$. Da qua si mostra che le uniche soluzioni per (n,k) sono $(n,1)$, $(6,3)$. Quindi a meno che $n = 6$, si ha che $k = 1$ e quindi una trasposizione viene mandata in trasposizione.

1.10 Presentazione di gruppo

Definizione - gruppo libero: chiamiamo gruppo libero su n generatori l'insieme

$$F_n = \langle x_1, \dots, x_n \rangle = \left\{ s = x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \dots x_{i_k}^{\alpha_k} | k \in \mathbb{N}, i_j \in \{1, \dots, n\} \text{ e } \alpha_j \in \pm 1 \ \ \forall\, 1 \leq j \leq k, \ s \text{ ridotta} \right\}$$

Ignorando l'ultima condizione esso è l'insieme delle stringhe (scritture formali) di lunghezza finita ottenute concatenando come caratteri degli x_i oppure dei loro inversi (definizione solo formale). Diciamo che una tale stringa è *ridotta* se non esiste i tale che esistano un x_i e un x_i^{-1} consecutivi. Chiaramente per ciascuna scritta esiste la stringa ridotta, ottenibile in un numero finito di passi. Talvolta si dice che due stringhe a cui è associata la stessa stringa ridotta sono *equivalenti*.
Ciò ci permette di dare a F_n struttura di gruppo: l'operazione è quella di concatenare le stringhe una accanto all'altra, l'elemento neutro è la stringa vuota e l'inverso di s è la stringa ottenuta riscrivendo s da destra a sinistra al contrario e cambiando segno agli esponenti (è già ridotta e chiaramente concatenandola a s e riducendo si cancella tutto).
Notare che la definizione funziona ugualmente anche se il gruppo dei generatori è infinito (continuiamo a considerare le stringhe finite). In tal caso chiameremo $\langle X \rangle$ il gruppo libero generato da X.
Esempio: $F_1 = \langle x \rangle = \left\{ x^k | k \in \mathbb{Z} \right\} \cong \mathbb{Z}$.
Proposizione - proprietà universale del gruppo libero: per ogni gruppo G si ha

$$\forall 1 \leq i \leq n \ Hom(F_n, G) \leftrightarrow G^n \cong (g_1, \dots, g_n) | g_i \in G,$$

ovvero sono in bigezione.

dim. basta fare delle verifiche formali (lasciate per esercizio), la bigezione è quella naturale.

Definizione - presentazione di gruppo: Dato G gruppo diciamo che $\langle S|R \rangle$ è una presentazione di G se:

- $S \subseteq G$ è un insieme di *generatori* di G
- $R \subseteq \langle S \rangle$ (gruppo libero generato da S) è un insieme di *relazioni*, tale che $\exists \varphi : \langle S \rangle \to G$ surgettivo con $\text{Ker}(\varphi) = N_R$ più piccolo sottogruppo normale di $\langle S \rangle$ che contiene $\langle R \rangle$.

  Intuitivamente, sono scritture formali tali che una volta valutate nel gruppo G siano l'elemento neutro. Ciò sarà chiarito dall'esempio.

Notare che, nella notazione della definizione e usando φ vale $G \cong \langle S \rangle / N_R$.

- la presentazione è un invariante per isomorfismo
- non tutti i gruppi ammettono presentazione finita (sia come generatori che come relazioni)
- la presentazione non è unica (ci possono essere vari insiemi di generatori o varie relazioni ammissibili)
- a ogni presentazione è associato un unico gruppo (a meno di isomorfismo)

Esempio: $\mathbb{Z}/n\mathbb{Z} = \langle x | x^n = 1 \rangle$ (di solito invece di indicare le relazioni si scrive "stringa" = el. neutro).
Esempio: il gruppo libero generato da S ha presentazione $\langle S \rangle = \langle S | \emptyset \rangle$.
Esempio: Per dire che due elementi commutano basta scrivere $[a, b] = 1$ (si ricorda che $[a, b] = aba^{-1}b^{-1}$ è il commutatore). Quindi ad esempio $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle x, y | x^2 = y^2 = xyx^-1y^-1 = 1 \rangle$ e l'informazione "il gruppo è abeliano" può essere espressa mediante le relazioni $\{[g, h] = 1 | g, h \in G\}$.

È un utile esercizio mostrare che le seguenti due sono presentazioni usando la definizione data sopra:
Esempio: $D_n = \langle r, s | r^n = id, s^2 = id, srsr = id \rangle$ (da queste relazioni si ricava $s^a r^b s^c r^d = s^{a+c} r^{(-1)^c b + d}$).
Esempio: $Q_8 = \langle i, j | i^4 = 1, i^2 j^{-2} = 1, j^{-1} iji = 1 \rangle = \langle i, j | i^4 = 1, i^2 = j^2, ji = i^{-1} j \rangle$.
A cosa ci serve una presentazione? Intuitivamente, è l'insieme dei check minimali da fare quando si costruisce un omomorfismo definendolo prima sui generatori e poi volendolo estendere. Nella pratica, è molto difficile lavorarci e costruirle, nel corso si usano principalmente per "riconoscere" D_n oppure Q_8 mentre si studia un gruppo.

1.11 Esercizi di classificazione

Esempio - classificazione dei gruppi di ordine 12: Gli unici gruppi di ordine 12 sono, a meno di isomorfismo: $\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, D_6, A_4, \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

dim. Notiamo $12 = 2^2 \cdot 3$. Siano P_2, P_3 rispettivamente un 2-Sylow e un 3-Sylow di 12. Notiamo che $P_2 \cap P_3 = \{e\}$ (le cardinalità sono coprime) e quindi $P_2 P_3 = G$ (per cardinalità). Dal teorema di Sylow si vede che $n_2 = 1, 3$ e $n_3 = 1, 4$. Guardando le possibilità e le cardinalità, necessariamente uno tra P_2 e P_3 è normale in G (due 3-Sylow distinti devono necessariamente avere intersezione banale, quindi se $n_3 = 4$ si ha che i tre 3-Sylow hanno unione di cardinalità $4 \cdot (3-1) + 1 = 9$; un 2-Sylow ha chiaramente intersezione banale con questa unione, quindi deve essere contenuto nei $12 - 9 + 1 = 4$ elementi rimanenti, da cui segue che ce ne può essere uno solo) , quindi $G \cong P_2 \rtimes P_3$ oppure $G \cong P_2 \rtimes P_3$. Poiché $P_3 \cong \mathbb{Z}/3\mathbb{Z}$ e $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ oppure $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ facciamo i casi:

- $G \cong P_2 \rtimes P_3$, $P_2 \cong \mathbb{Z}/4\mathbb{Z}$. Quindi $G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ e quindi l'unica scelta per φ è l'identità (i due gruppi hanno ordini coprimi). Quindi $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$.
- $G \cong P_2 \rtimes P_3$, $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Quindi $G \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \cong S_3$ e quindi abbiamo due scelte.
  - $\varphi = id$ e quindi $G \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
  - $\varphi \neq id$ che ci dà $G \cong A_4$, con l'isomorfismo che manda $(\mathbb{Z}/2\mathbb{Z})^2$ nel Klein e $\mathbb{Z}/3\mathbb{Z}$ nel gruppo generato da un tre ciclo.
- $G \cong P_3 \rtimes P_2$, $P_2 \cong \mathbb{Z}/4\mathbb{Z}$. Quindi $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$. $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ e quindi abbiamo due scelte:
  - $\varphi = id$ e quindi $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$ (già visto)
  - $\varphi \neq id$ che non dà "gruppi noti"; scriviamo solo $G \cong \mathbb{Z}/3 \rtimes \mathbb{Z}/4\mathbb{Z}$
- $G \cong P_3 \rtimes P_2$, $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Quindi $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})^2$. $\varphi : (\mathbb{Z}/2\mathbb{Z})^2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ e quindi abbiamo due scelte (in realtà le scelte sono 4, se consideriamo i due generatori canonici, ma tre di esse sono chiaramente isomorfe):
  - $\varphi = id$ e quindi $G \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ già visto.
  - $\varphi \neq id$, e quindi $\mathrm{Ker}(\varphi) \cong \mathbb{Z}/2\mathbb{Z}$. Sia $\mathrm{Ker}(\varphi) = \langle x \rangle$ con $x \in G$, e siano $y, z \in G$ tali che $\langle z \rangle \cong \mathbb{Z}/3\mathbb{Z}$ e $\langle x \rangle \langle y \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2 \Rightarrow G \cong \langle z \rangle \rtimes \langle x \rangle \langle y \rangle$. Allora per definizione (essendo φ_z il coniugio per z) si ha $zxz^{-1} = x, zyz^{-1} = xy = yx \Rightarrow$ Si può allora mostrare che $Z(G) \cong \mathbb{Z}/6\mathbb{Z}$. Poiché

Esempio - classificazione dei gruppi di ordine 8: gli unici gruppi di ordine 8 sono, a meno di isomorfismo: $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3, D_4, Q_8$.

dim. Facciamo qualche considerazione sugli ordini degli elementi. Detto G un gruppo di ordine 8 e preso $g \in G$ per Lagrange $\text{ord}(g) \in \{1, 2, 4, 8\}$.

- se tutti gli elementi hanno ordine 2 G è abeliano; basta infatti notare che in tal caso si ha $g^2 = e$ e quindi $g^{-1} = g \ \forall g \in G$. Da ciò segue $gh = g^{-1}h^{-1} = (hg)^{-1} = hg \ \forall g, h \in G$. Usando il teorema di struttura, questo caso ci dà $G \cong (\mathbb{Z}/2\mathbb{Z})^3$
- se un elemento ha ordine 8 allora G è ciclico e $G \cong \mathbb{Z}/8\mathbb{Z}$
- se nessuna delle precedenti condizioni è verificata $\exists a \in G$ tale che $\text{ord}(a) = 4$. $[G : \langle a \rangle] = 2 \Rightarrow \langle a \rangle \lhd G \Rightarrow$ preso $b \in G \setminus \langle a \rangle$ si ha $G = \langle a \rangle \cup b\langle a \rangle$ (G è unione delle classi laterali), ovvero $G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$. Notiamo che, essendo $\langle a \rangle$ normale, necessariamente $bab^{-1} \in \langle a \rangle$. Facciamo i casi:
  - $bab^{-1} = e \Rightarrow a = e$ assurdo
  - $bab^{-1} = a^2 \Rightarrow (bab^{-1})^2 = a^4 = e \Rightarrow ba^2b^{-1} = e \Rightarrow a^2 = e$ assurdo
  - $bab^{-1} = a \Rightarrow ab = ba$ da cui si verifica facilmente che G è abeliano. I casi con G abeliano sono dati dal teorema di struttura, e sono quelli nel testo.
  - $bab^{-1} = a^3 = a^{-1}$. In questo caso distinguiamo due casi in base a $\text{ord}(b)$, notando che le possibilità (per come abbiamo fatto i casi) sono solo 2 e 4:
    * se $\text{ord}(b) = 2$ si può verificare che $G \cong D_4$, mediante l'isomorfismo che manda $a \mapsto r$, $b \mapsto s$; la presentazione di gruppo in questo caso è $\langle a, b | a^4 = 1, b^2 = 1, ba = a^3b \rangle$ (notare che è la stessa di D_4)
    * se $\text{ord}(b) = 4$ si può verificare che $G \cong Q_8$, mediante l'isomorfismo che manda $a \mapsto i$, $b \mapsto j$; la presentazione di gruppo in questo caso è $\langle a, b | a^4 = 1, b^4 = 1, ba = a^3b \rangle$ (notare che è la stessa di Q_8)

Esempio - classificazione dei gruppi di ordine 30: Gli unici gruppi di ordine 30 sono, a meno di isomorfismo: $\mathbb{Z}/30\mathbb{Z}, D_{15}, D_5 \times \mathbb{Z}/3\mathbb{Z}, D_3 \times \mathbb{Z}/5\mathbb{Z}$.

dim. Notiamo innanzitutto che $30 = 2 \cdot 15$ e quindi è della forma $2d$ con d dispari. Pertanto, detto G un generico gruppo di ordine 30, esiste $H \lhd G$ con $\#H = 15$. $15 = 3 \cdot 5$, quindi è della forma pq con p, q primi. Per quanto visto a teoria, poiché $3 \nmid 5 - 1 = 4$ si ha $H \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ e quindi $H = \langle x \rangle$ (è ciclico). Sia ora $y \in G$ di ordine 2, che esiste per Cauchy. Chiaramente $y \notin H$ per una questione di ordini. Quindi $\langle x \rangle \cap \langle y \rangle = \{e\}$ e per cardinalità $\langle x \rangle \langle y \rangle = G$, da cui segue dal teorema di decomposizione in prodotto semidiretto (ricordando che $\langle x \rangle$ è normale) che $G \cong \langle x \rangle \rtimes_\varphi \langle y \rangle \cong \mathbb{Z}/15\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$. Sempre dal teorema segue che $\varphi : \langle y \rangle \to \text{Aut}(\langle x \rangle)$ è il coniugio, ossia $\varphi_y(x) = yxy^{-1}$.

Notiamo che $\text{Aut}(\langle x \rangle) \cong \text{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong (\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Poiché y ha ordine 2 necessariamente φ_y ha ordine 1 (quindi è id) oppure 2. In entrambi i casi $\varphi_y(\varphi_y(x)) = x$.

Notiamo intanto che per normalità di $\langle x \rangle$ si ha $\varphi_y(x) \in \langle x \rangle$ e quindi $yxy^{-1} = \varphi_y(x) = x^\ell$. $(\ell, 15) = 1$, perché altrimenti φ_y non sarebbe automorfismo, e che $x = \varphi_y(\varphi_y(x)) = x^{2\ell} \Rightarrow 2\ell \equiv 1 \pmod{15}$. Ciò implica $\begin{cases} \ell \equiv \pm 1 \pmod 3 \\ \ell \equiv \pm 1 \pmod 5 \end{cases}$ e ci dà perciò quattro casi:

- $\begin{cases} \ell \equiv 1 \pmod 3 \\ \ell \equiv 1 \pmod 5 \end{cases} \Rightarrow \ell \cong 1 \pmod{15} \Rightarrow yxy^{-1} = x \Rightarrow yx = xy.$

  Quindi il gruppo è abeliano, ovvero $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z}$.

- $\begin{cases} \ell \equiv 1 \pmod 3 \\ \ell \equiv -1 \pmod 5 \end{cases} \Rightarrow \ell \cong 4 \pmod{15} \Rightarrow yxy^{-1} = x^4$

  Si può osservare che ciò implica $yx^5y^{-1} = x^5 \Rightarrow x^5 \in Z_G$. A questo punto si verifica manualmente $G \cong D_5 \times \mathbb{Z}/3\mathbb{Z}$ con l'isomorfismo che manda $x \mapsto (r, \overline{1})$, $y \mapsto (s, \overline{0})$.

- $\begin{cases} \ell \equiv -1 \pmod 3 \\ \ell \equiv 1 \pmod 5 \end{cases} \Rightarrow \ell \cong -4 \pmod{15} \Rightarrow yxy^{-1} = x^{-4}$

  In modo analogo a prima $x^3 \in Z_G$ e si verifica manualmente $G \cong D_3 \times \mathbb{Z}/5\mathbb{Z}$.

- $\begin{cases} \ell \equiv -1 \pmod 3 \\ \ell \equiv -1 \pmod 5 \end{cases} \Rightarrow \ell \cong -1 \pmod{15} \Rightarrow yxy^{-1} = x^{-1}$

  Riconosciamo adesso la presentazione di D_{15}. Si ha allora $G \cong D_{15}$.

Esempio - (*) gruppi semplici piccoli: Quali sono i possibili ordini ≤ 100 di un gruppo semplice.
Ricordiamo che un gruppo G si dice semplice se i suoi unici sottogruppi normali sono $\{e\}, G$.

dim. Si raccomanda di provare prima l'esercizio per conto proprio, perché per quanto noioso è utile per ripassare tutte le tecniche viste sulla classificazione gruppi. Si lascia qui uno sketch di svolgimento, detto n l'ordine del gruppo G da studiare.

Vediamo prima i casi noti dalla teoria:

- $n = p$ primo $\Rightarrow G$ semplice (perché?)
- $n = p^k$ con p primo $\Rightarrow G$ NON semplice (perché?)
- $n = pq$ con p, q primi $\Rightarrow G$ NON semplice (perché?)
- $n = 2d$ con d dispari $\Rightarrow G$ NON semplice (perché?)

Vediamo ora dei casi in base a come si scompone in fattori primi $n \leq 100$. I casi a mano generalmente si trattano con Sylow (se si mostra $n_p = 1$ per qualche primo $p|n$ allora il Sylow è normale, quindi il gruppo non è semplice; potrebbero funzionare approcci che usino cardinalità cominciando col supporre $n_p > 1 \forall p|n$)

- n ha ≥ 4 primi distinti. Allora $n \geq 2 \cdot 3 \cdot 5 \cdot 7 = 210$ assurdo. Quindi il caso non si pone.
- $n = p^a q^b r^c$ con $p < q < r$ primi e $a, bc \geq 1$.
  - se $c \geq 2$ allora $n \geq 2 \cdot 3 \cdot 5^2 > 100$. Quindi $c = 1$.
  - se $b \geq 3$ $n \geq 2 \cdot 3^3 \cdot 5 > 100$. Quindi $b = 1, 2$
  - se $a = b = 1$, $n = pqr \Rightarrow G$ NON semplice (per esercizio)
  - se $b = 2$, allora necessariamente per $n \leq 100$ $p = 2, q = 3, r = 5$ e $n = 90$ già trattato
  - resta $n = p^a qr$ con $a > 1$, che dà i casi $n = 60, 84$. Per $n = 60$ esiste A_5 che è semplice. Per $n = 84$ si mostra G NON semplice.
- $n = p^a q^b$ con p, q primi. Escludiamo i casi $a = b = 1$, già trattati. Abbiamo allora solo i seguenti casi:
  - $n = 2^a \cdot 3^b$ che possono essere trattati a mano. Un modo veloce di gestirli è notare che $n_3 = 4$ oppure 16.
    - ◦|42 se $n_3 = 4$ l'azione di coniugio sull'insieme dei 3-Sylow dà un'immersione di G in S_4 (il nucleo dell'azione è normale in G quindi deve essere banale se G semplice), che ci dà pochi casi tutti NON semplici.

◦|42 se $n_3 = 16$ abbiamo per cardinalità solo $n = 48, 96$ e si potrebbero trattare a mano. Si può però notare che $n_2|3$ in entrambi i casi e quindi $n_2 = 3$ e in modo analogo a prima se G fosse semplice dovremmo poterlo immergere in S_3, assurdo. Quindi NON sono semplice.

- $n = 2^k p$ con p primo. Il caso $k = 1$ è stato già trattato, $k = 2$ si può trattare a parte, gli altri $(n = 40, 56, 80, 88)$ vanno fatti a mano e NON sono mai semplici.
- rimangono infine i casi $n = 45, 63, 75, 99, 100$, che si trattano a mano e NON sono mai semplici

Gli unici gruppi semplici di ordine fino a 100 sono allora $\mathbb{Z}/p\mathbb{Z}$ e A_5.

1.12 Invertibili modulo n

(Non tutti gli anni viene svolta ad Aritmetica)
Proposizione - invertibili modulo n: $(\mathbb{Z}/n\mathbb{Z})^*$ (come gruppo moltiplicativo) è ciclico se e solo se si ha $n = 2, 4, p^k, 2p^k$ con p primo dispari, $k \geq 1$.

dim. La dimostrazione per $n = p$ è data ad aritmetica. I casi $n = 2, 4$ si verificano manualmente.

Mostriamo prima il caso $n = p^k$. Sia r un generatore modulo p.

lemma: uno tra r e $r + p$ è generatore $\pmod{p^2}$.

dim. Poiché $\varphi(p^2) = p(p-1)$ e $r, r+p$ sono coprimi con p^2 si ha $\mathrm{ord}_{p^2}(r), \mathrm{ord}_{p^2}(r+p) | p(p-1)$. Ma poiché entrambi sono per definizione generatori $\pmod{p}$ deve necessariamente valere $p-1 | \mathrm{ord}_{p^2}(r), \mathrm{ord}_{p^2}(r+p)$. Quindi per entrambi gli ordini abbiamo due possibilità: $p-1$ e $p(p-1)$. Supponiamo per assurdo che entrambi gli ordini siano $p-1$. Sviluppando il binomio di Newton si ha:

$$1 \equiv (r+p)^{p-1} = \sum_{i=0} p - 1 \binom{p-1}{i} p^i r^{p-1-i} \equiv r^{p-1} + (p-1)pr^{p-2} \equiv 1 - pr^{p-2} \pmod{p^2},$$

dove la penultima congruenza segue dal fatto che per $i \geq 2$ l'addendo nella sommatoria è divisibile per p^2 e quindi $\equiv 0 \pmod{p^2}$. Si ha quindi $0 \equiv pr^{p-2} \pmod{p^2}$ che è assurdo essendo r, p coprimi.

Sia ora s il generatore modulo p^2 trovato grazie al lemma. Ci occorre prima di tutto un lemma.

lemma: se $a, m \geq 1$ si ha $(1+mp)^{p^a} \equiv 1 + mp^{a+1} \pmod{p^{a+2}}$.

dim. Per induzione su a.

- Per il caso $a = 1$ basta usare il binomio di Newton:

$$(1+mp)^p \equiv \sum_{i=0}^{p} \binom{p}{i} (mp)^i \equiv 1 + mp^2 + m^2 p^3 \frac{p-1}{2} \equiv 1 + mp^2 \pmod{p^3}$$

  dove nella congruenza centrale abbiamo eliminato i termini con $i \geq 3$ in quanto chiaramente divisibili per p^3.
- Per il passo induttivo $a \mapsto a+1$ scriviamo $(1+mp)^{p^a} = 1 + mp^{a+1} + m'p^{a+2}$ (è l'ipotesi induttiva) e procediamo in modo analogo:

$$(1+mp)^{p^{a+1}} = (1+p^{a+1}(m+m'p))^p \equiv \sum_{i=0}^{p} \binom{p}{i} p^{i(a+1)} (m+m'p)^i \equiv 1 + p^{a+2}(m+m'p) \equiv 1 + mp^{a+2} \pmod{p^{a+3}}$$

lemma: s è generatore modulo p^k per ogni $k \geq 2$.

dim. Usando che s è generatore modulo p^2 e Lagrange si ha $p(p-1)|\text{ord}_{p^k}(s)|\varphi(p^k) = p^{k-1}(p-1)$, da cui segue che $\text{ord}_{p^k}(s) = p^h(p-1)$ per qualche $1 \leq h \leq k-1$. Supponiamo per assurdo che $h < k-1$ e quindi che $\text{ord}_{p^k}(s)|p^{k-2}(p-1)$. Poiché s era per costruzione anche un generatore modulo p si ha $s^{p-1} = 1 + mp$ per qualche $m \in \mathbb{Z}$. Usando il lemma appena mostrato si ha allora

$$1 \equiv s^{p^{k-2}(p-1)} =\equiv (1+mp)^{p^{k-2}} \equiv 1 + mp^{k-1} \pmod{p^k},$$

da cui segue che $mp^{k-1} \equiv 0 \pmod{p^k}$, che implica $p|m$. Ciò è però impossibile visto che si avrebbe $s^{p-1} \equiv 1 \pmod{p^2}$, ma s è un generatore modulo p^2.

Questo conclude la dimostrazione della ciclicità per il caso $n = p^k$. Per $n = 2p^k$ si ha per il teorema cinese del resto:

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^k\mathbb{Z})^* \cong (\mathbb{Z}/p^k\mathbb{Z})^*,$$

dove l'ultima uguaglianza segue dal fatto che $(\mathbb{Z}/2\mathbb{Z})^*$ è il gruppo banale.

1.13 Consigli e reminder per risolvere gli esercizi

- spesso vanno usati i punti precedenti;
- vale la pena conoscere (bene) la struttura di D_n e S_n;
- i sottogruppi di S_n in generale fanno un po' schifo. Alla richiesta di trovare sottogruppi di ordine dato in S_n, quasi sempre si risponde con centralizzatori o normalizzatori, eventualmente intersecati con A_n;
- i gruppi normali sono i Ker di omomorfismi, quindi di omomorfismi *da* gruppi semplici ce ne sono ben pochi;
- talvolta aiuta contare gli elementi di un certo ordine;
- commutare/essere normale equivale a commutare con/essere normale a un insieme di generatori;
- i prodotti $A \rtimes B$ sono generati da $A \times \{e\}$ e $\{e\} \times B$;
- $Z_G(H) \lhd N_G(H)$, inoltre $N_G(H)/Z_G(H) \hookrightarrow \text{Aut}(H)$;
- nel dubbio fai agire G su $H < G$ per coniugio;
- il numero n_p di p-Sylow è l'indice in G del normalizzatore di un p-Sylow. Segue che il numero di p-Sylow di un prodotto diretto è il prodotto dei numeri di p-Sylow;
- se ho tanti p-Sylow, i normalizzatori sono piccoli;
- il centro sta quantomeno nell'intersezione di tutti i normalizzatori, quindi se i p-Sylow sono tanti e i normalizzatori sono piccoli, anche il centro non è troppo grande;
- qualche p-Sylow di solito è caratteristico;
- il generato da una classe di coniugio (o da un insieme di classi di coniugio) è normale. Quindi se G è semplice, ogni classe di coniugio genera;
- i p-Sylow di un sottogruppo sono tutti coniugati tramite elementi *del sottogruppo*. Se P è un p-Sylow di G ed è contenuto in un sottogruppo H, allora P è un p-Sylow di H.

2 Teoria degli anelli

Dove non diversamente specificato, A è un anello commutativo con unità con operazioni $+$ e $\cdot$ (il cui simbolo verrà omesso). L'elemento neutro della somma sarà indicato con 0, quello del prodotto con 1.

2.1 Definizioni e richiami di Aritmetica

Definizione - ideale: un ideale I di A è un sottogruppo additivo di A dotato della proprietà di assorbimento, ossia tale che $\forall a \in A\, aI \subseteq I$.
Definizione - ideale generato: dato un sottoinsieme $S \subseteq A$ l'ideale generato da S è $(S) = \bigcap_{S \subseteq I \lhd A} I$.
Definizione - ideale principale: un ideale I di A è detto principale se $\exists x \in A$ tale che $I = (x)$.
Definizione - ideale primo: $P \lhd A$ è detto primo se $\forall x, y \in A\ xy \in P \Rightarrow x \in P$ o $y \in P$.
Proposizione - ideali principali primi: $P = (x)$ è primo $\Leftrightarrow x$ è un elemento primo di A.
Definizione - ideale massimale: $M \lhd A$ proprio è detto massimale se $\forall I \lhd A\ M \subseteq I \subseteq A \Rightarrow I = M$ o $I = A$.
Definizione - elemento irriducibile: Sia A un dominio. $x \in A$ si dice irriducibile se $\forall a, b \in A\ x = ab \Rightarrow a \in A^* \vee b \in A^*$.
Definizione - elemento primo: Sia A un dominio. $p \in A \setminus (A^* \cup \{0\})$ si dice primo se $\forall a, b \in A\ p|ab \Rightarrow p|a \vee p|b$.
Definizione - elementi associati: Sia A un dominio. $x, y \in A$ si dicono associati, "$x \sim y$" se vale una delle seguenti condizioni equivalenti:

(i) $\exists u \in A^*\ x = uv$;

(ii) $x|y \wedge y|x$;

(iii) $(x) = (y)$.

Proposizione - primi e irriducibili: Sia A un dominio. Valgono le seguenti implicazioni:

(i) x primo $\Rightarrow x$ irriducibile;

(ii) x primo $\Leftrightarrow (x)$ primo;

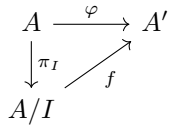
(iii) x irriducibile $\Leftrightarrow (x)$ massimale nella classe degli ideali principali di A.

dim. dimostriamo solamente (iii). ($\Rightarrow$), dato x irriducibile $\forall y \in A(x) \subseteq (y) \subsetneq A \Rightarrow \exists a \in A x = ya$, ma poiché x irriducibile e $(y) \neq A$ necessariamente $a \in A^*$, cioè $x \sim y$ e quindi $(x) = (y)$, cioè (x) massimale tra gli ideali principali. ($\Leftarrow$), sia $x = ab$ con $a \notin A^*$, per massimalità $(x) = (a) \subsetneq A$, da cui $\exists c\ a = xc$. Segue $x(1 - bc) = 0$ e quindi $b \in A^*$, cioè x irriducibile.

2.2 Ideali e proprietà

Gli ideali di un anello possono in un certo senso essere pensati come l'analogo dei sottogruppi normali in un gruppo. Essi sono infatti i nuclei degli omomorfismi, e valgono per essi teoremi analoghi a quelli visti in teoria dei gruppi, come vedremo adesso. Per questo motivo scegliamo la stessa notazione per indicarli: $I \lhd A$.

Teorema - 1° di omomorfismo (per anelli): Siano $\varphi : A \to A'$ un omomorfismo di anelli e $I \lhd A$ tale che $I \subseteq \mathrm{Ker}(\varphi)$. Allora $\exists! f$ che fa commutare il diagramma a lato.
Inoltre $\mathrm{Imm}(f) = \mathrm{Imm}(\varphi)$ e f iniettiva $\Leftrightarrow I = \mathrm{Ker}(\varphi)$.



dim. Applichiamo il 1° teorema di omomorfismo per gruppi (considerando A, A' come gruppi additivi) e notiamo che la funzione ottenuta è un omomorfismo di anelli, per le proprietà del quoziente.

Teorema - di corrispondenza (per anelli): Sia $I \lhd A$ e $\pi_I : A \to A/I$ la proiezione. Allora π_I induce una corrispondenza tra gli ideali di A/I e gli ideali di A che contengono I. Tale corrispondenza preserva: ordinamento per inclusione, indice, ideali primi, ideali massimali.

dim. Per il teorema di corrispondenza per gruppi (un anello è in particolare un gruppo additivo abeliano) si ha che, detti $X = \{H \leq A \mid I \subseteq H\}$ e $Y = \{\overline{H} \leq A/I\}$, la funzione $\alpha : X \to Y$ che mappa $H \overset{\alpha}{\mapsto} \pi_I(H)$ è una bigezione tra i sottogruppi additivi di A e i sottogruppi additivi di A/I. Restringiamo ora α a $X' = \{H \lhd A \mid I \subseteq H\}$ e definiamo analogamente definiamo $Y' = \{\overline{H} \lhd A/I\}$ Sia $\tilde{\alpha}$ la funzione ristretta. Poiché π_I è omomorfismo di anelli suriettivo, immagine di ideali è ideale (esercizio) e quindi $\tilde{\alpha}$ manda ideali in ideali. Sempre per omomorfismo, controimmagine di ideali è ideali, quindi $\tilde{\alpha} : X' \to Y'$ è anche suriettiva. Ma allora per iniettività α, $\tilde{\alpha}$ è una bigezione. $\tilde{\alpha}$ Preserva indice e contenimenti perché α lo faceva. Questa corrispondenza preserva inoltre primalità e massimalità perché π_I è un omomorfismo suriettivo il cui kernel (I) è contenuto in tutti gli elementi di X'.

Teorema - cinese del resto per anelli: Siano $I, J \lhd A$ e $f : A \to A/I \times A/J$ tale che $f(a \mapsto (a+I, a+J))$. Allora f è omomorfismo di anelli, $\mathrm{Ker}(f) = I \cap J$ e $(I, J) = A \Leftrightarrow f$ suriettiva.

dim. Che sia omomorfismo di anelli segue dal fatto che sia la proiezione su I che quella su J lo sono. $\mathrm{Ker}(f) = \{a \in A \mid a + I = I \text{ e } a + J = J\} = \{a \in A \mid a \in I \text{ e } a \in J\} = I \cap J$. Per la suriettività, $(I, J) = A \Rightarrow 1 \in (I, J) \Rightarrow \exists x \in I, y \in J \; x+y = 1$. Allora $\forall a, b \in A$ dalla proprietà di assorbimento segue che $f(ax+by) = (ax+by+I, ax+by+J) = (by+I, ax+J) = (b(1-x)+I, a(1-y)+J) = (b+I, a+J)$. Nel verso opposto, f suriettiva $\Rightarrow \forall a, b \in A \; \exists x \in A \; (x+I, x+J) = (a+I, b+I) \Rightarrow \exists x \in A \; (x+I, x+I) = (1+I, J) \Rightarrow x \in J, \exists y \in I \; x = 1+y \Rightarrow 1 \in (I, J) \Rightarrow (I, J) = A$.

Teorema - lemma di Zorn: Sia $(X, \leq)$ un insieme non vuoto parzialmente ordinato (poset). Esso si dice induttivo se ogni catena (sottoinsieme di X totalmente ordinato) ammette maggiorante. Se X è induttivo, allora esiste un elemento massimale.

dim. Si rimanda al corso di teoria degli insiemi.

Proposizione - ideali massimali: Sia $\mathscr{F} = \{I \lhd A\}$ l'insieme degli ideali di A. Allora $\mathscr{F}$ è un insieme induttivo, ossia verifica le ipotesi del lemma di Zorn. Allora valgono le seguenti:

- ogni anello possiede ideali massimali (basta applicare Zorn a $\mathscr{F}$);
- ogni elemento non invertibile di A è contenuto in un ideale massimale (basta applicare Zorn a $\mathscr{F} \cap$ {ideali contenenti l'elemento});
- ogni ideale proprio è contenuto in un ideale massimale (basta applicare Zorn a $\mathscr{F} \cap$ {ideali contenenti l'ideale fissato}).

Teorema - caratterizzazione ideali primi e massimali: I ideale. Allora valgono le seguenti:

- I è primo $\Leftrightarrow A/I$ dominio;
- I è massimale $\Leftrightarrow A/I$ campo.

Come corollario, I massimale implica I primo.

dim. A/I dominio $\Leftrightarrow \forall x, y \in A\ ((x+I)(y+I) = I \Leftrightarrow x+I = I \vee y+I = I) \Leftrightarrow \forall x, y \in A\ (xy+I = I \Leftrightarrow x+I = I \vee y+I = I) \Leftrightarrow \forall x, y \in A\ (xy \in I \Leftrightarrow x \in I \vee y \in I) \Leftrightarrow I$ è primo. A/I campo $\Leftrightarrow$ ogni suo elemento è invertibile $\Leftrightarrow$ i suoi unici ideali sono 0 e $A/I \Leftrightarrow$ (per corrispondenza) gli unici ideali contenenti I sono I e $A \Leftrightarrow I$ è massimale

Teorema - ideali e omomorfismi: Sia $f : A \to B$ omomorfismo di anelli. Allora valgono le seguenti:

- controimmagine di ideale è ideale;
- controimmagine di ideale primo è ideale primo.

Se f è suriettivo valgono inoltre:

- immagine di ideale è ideale;
- controimmagine di ideale massimale è ideale massimale;
- immagine di un ideale massimale è ideale massimale.

dim. esercizio.

Parliamo ora di operazioni tra ideali. Nelle definizioni I, J sono due ideali qualsiasi di A.
Definizione - ideali coprimi: I, J si dicono coprimi se $I + J = A$. Intuitivamente, due ideali sono coprimi se l'unico ideale che *divide* (i.e. contiene) entrambi è $(1) = A$. Analogamente, I, J coprimi $\Leftrightarrow \exists x \in I, y \in J\ x + y = 1$.
Definizione - intersezione di ideali: $I \cap J$ è un ideale.
Definizione - prodotto di ideali: indichiamo con IJ l'ideale (IJ) generato da $\{ij \mid i \in I, j \in J\}$.
Proposizione - prodotto e intersezione: $IJ \subseteq I \cap J$. Se inoltre I, J sono coprimi, vale l'uguaglianza.

dim. Il contenimento segue dalla proprietà di assorbimento comune sia a I che a J. Se inoltre $\exists x \in I, y \in J\ x + y = 1$ si ha $\forall z \in I \cap J\ z = xz + yz \in IJ$, dunque l'uguaglianza.

Definizione - radicale: indichiamo con $\sqrt{I}$ l'ideale $\{x \in A \mid \exists n \in \mathbb{N}\ x^n \in I\}$.
Proposizione - radicale del prodotto: $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

dim. Dalla definizione segue che per ogni $I_1 \subseteq I_2$ ideali vale $\sqrt{I_1} \subseteq \sqrt{I_2}$. Quindi $IJ \subseteq I \cap J \Rightarrow \sqrt{IJ} \subseteq \sqrt{I \cap J}$. Per il contenimento inverso si nota che, preso $x \in \sqrt{I \cap J}$ e $n \in \mathbb{N}$ tale che $x^n \in I \cap J$ si ha $x^{2n} = x^n \cdot x^n \in IJ$ e dunque $x \in \sqrt{IJ}$.

Proposizione - radicale di un primo: se P è ideale primo $\sqrt{P} = P$

dim. Dalla definizione segue $P \subseteq \sqrt{P}$. Sia ora $x \in \sqrt{P}$ e $n = \min\{n' \in \mathbb{N} \mid x^{n'} \in P\}$. Se fosse $n > 1$, per primalità di P si avrebbe $x \cdot x^{n-1} = x^n \in P \Rightarrow x \in P \vee x^{n-1} \in P$, contro la minimalità di n. Quindi necessariamente $n = 1$, cioè $x \in P$.

Proposizione - radicale di un ideale: Per ogni $I \lhd A$ si ha

$$\sqrt{I} = \bigcap_{\substack{I \subseteq P \lhd A \\ P \text{ primo}}} P.$$

In particolare $\sqrt{(0)} = \bigcap_{P \lhd A \text{ primo}} P$.

dim. Notiamo innanzitutto che per Zorn esiste almeno un ideale massimale (dunque primo) che contiene I, dunque ci sono dei P da intersecare. Il contenimento "$\subseteq$" segue dalla monotonia del radicale. Per il contenimento inverso, sia $a \in A \setminus \sqrt{I}$: vogliamo mostrare che esiste un ideale primo che contiene I ma a cui a non appartiene. Si ha $0 \notin \langle a \rangle = \{a^n \mid n \in \mathbb{N}\}$ poiché $\langle a \rangle \cap I = \emptyset$. Detto $S = A \setminus \langle a \rangle$, sia $\mathscr{F} = \{J \lhd A \mid I \subseteq J \subseteq S\}$. $\mathscr{F}$ è non vuoto ($I \in \mathscr{F}$) e induttivo. Per il lemma di Zorn esiste un elemento massimale Q: se Q è primo abbiamo concluso. Dimostriamo che Q è un ideale primo, cioè che $x, y \notin Q \Rightarrow xy \notin Q$. Sia $x \notin Q$, allora:

- se $x \in S \setminus Q$, per massimalità di Q in S si ha $(Q, x) \nsubseteq S$, dunque esistono $k \in \mathbb{N}, q \in Q, b \in A$ tali che $q + bx = a^k$;
- se $x \in \langle a \rangle$, allora $\exists k \in \mathbb{N}\ x = a^k$ e quindi vale ancora l'enunciato sopra scegliendo $q = 0, b = 1$.

Dati allora $x, y \in A \setminus Q\ \exists k_1, k_2, \in \mathbb{N}, q_1, q_2 \in Q, b_1, b_2 \in A\ q_1 + b_1 x = a^{k_1} \wedge q_2 + b_2 y = a^{k_2}$. Dunque $a^{k_1+k_2} = (q_1 + b_1 x)(q_1 + b_2 y) = (q_1 q_2 + q_1 b_2 y + q_1 b_1 x) + b_1 b_2 xy$, dove $q_1 q_2 + q_1 b_2 y + q_1 b_1 x \in Q$ per le proprietà di assorbimento e sottogruppo. Ma $a^{k_1+k_2} \notin Q \Rightarrow b_1 b_2 xy \notin Q \Rightarrow xy \notin Q$.

2.3 Parti moltiplicative e campo dei quozienti

Definizione - parte moltiplicativa: un insieme $S \subseteq A$ è detto parte moltiplicativa se è un semigruppo moltiplicativo (ossia $\forall x, y \in S\ xy \in S$) che non contiene 0 e contiene 1.
Da ora in poi S sarà una parte moltiplicativa si A.
Definizione - localizzazione: si chiama localizzazione di A rispetto a S l'insieme $S^{-1}A := A \times S/\sim$ dove la relazione di equivalenza è definita da $(a, s) \sim (b, t) \Leftrightarrow at = bs$. Indichiamo $(a, s) \in S^{-1}A$ con $\frac{a}{s}$. $S^{-1}A$ è un anello le cui operazioni sono definite come le operazioni sulle frazioni.
Proposizione - A si immerge nella localizzazione: l'immersione $f : A \hookrightarrow S^{-1}A$ data da $f(a \mapsto \frac{a}{1})$ è un omomorfismo di anelli (la verifica è immediata).
Proposizione - invertibili della localizzazione: $(S^{-1}A)^* = \{\frac{a}{s} \in S^{-1}A \mid \exists b \in A\ ab \in S\}$. Inoltre $\left(\frac{a}{s}\right)^{-1} = \frac{bs}{ab}$ con b tale che $ab \in S$.

dim. Un elemento $\frac{a}{s}$ della localizzazione è invertibile sse $\exists \frac{b}{t} \in S^{-1}A$ tale che $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} = \frac{1}{1}$, cioè $ab = st$, che accade se e soltanto se esiste in S un multiplo di a.

Teorema - ideali della localizzazione: gli ideali di $S^{-1}A$ sono tutti e soli gli insiemi della forma $S^{-1}I$ con I ideale di A.

dim. Se I è un ideale di A allora $S^{-1}I = \{\frac{x}{s} \mid x \in I\}$ è un ideale di $S^{-1}A$. La proprietà di assorbimento di $S^{-1}I$ segue da quella di I e da S parte moltiplicativa. Inoltre $S^{-1}I$ è un sottogruppo additivo, infatti:

- $0 \in I \Rightarrow \frac{0}{1} \in S$;
- $\frac{x}{s} \in S^{-1}I \Rightarrow \frac{-x}{s} = -\frac{x}{s} \in S^{-1}I$ perché $x \in I \Rightarrow -x \in I$;
- $\frac{x}{s}, \frac{y}{t} \in S^{-1}I \Rightarrow \frac{x}{s} + \frac{y}{t} = \frac{xt+ys}{st} \in S^{-1}I$ perché $xt, ys \in I$ per la proprietà di assorbimento di I e $st \in S$ perché S parte moltiplicativa.

Dimostriamo ora che per ogni J ideale di $S^{-1}A$ esiste un I in A tale che $J = S^{-1}I$. Consideriamo l'immersione $f : A \hookrightarrow S^{-1}A$ data da $f(a \mapsto \frac{a}{1})$. Sia $I = f^{-1}(J)$ la controimmagine di J tramite l'omomorfismo f. Allora $S^{-1}I = \{\frac{x}{s} \mid f(x) \in J,\ s \in S\} = \{\frac{x}{s} \mid \frac{x}{1} \in J,\ s \in S\}$. Ma $\forall x \in A, s \in S$ vale $\frac{x}{1} \in J \Leftrightarrow \frac{x}{s} \in J$ (si moltiplica rispettivamente per $\frac{s}{1}$ e $\frac{1}{s}$), dunque $S^{-1}I = J$.

Dall'ultimo ragionamento segue che $f^{-1}(J) = f^{-1}(J \cap f(A))$, quindi moralmente "$f^{-1}(J) = J \cap A$".

Teorema - ideali primi della localizzazione: esiste una corrispondenza biunivoca tra gli ideali primi di $S^{-1}A$ e gli ideali primi di A disgiunti da S.

dim. Dimostriamo innanzitutto che se P è un ideale primo di A disgiunto da S, allora $S^{-1}P$ è un ideale primo di $S^{-1}A$. Si nota intanto $S^{-1}P \neq S^{-1}A$, infatti $S^{-1}P = S^{-1}A \Leftrightarrow \frac{1}{1} \in S^{-1}P \Leftrightarrow S \cap P \neq \emptyset$. Inoltre $S^{-1}P$ è un ideale per il teorema precedente. Mostriamo che è primo: dato $\frac{x}{s}\frac{y}{t} = \frac{xy}{st} = \frac{p}{r} \in S^{-1}P$ si ha $xyr = pst \in P$ per assorbimento, dunque per primalità vale almeno una tra $x \in P$, $y \in P$ e $r \in P$. Sappiamo $r \notin P$ perché $r \in S$ e $S \cap P = \emptyset$, segue $x \in P \vee y \in P$ e quindi $\frac{x}{s} \in S^{-1}P \vee \frac{y}{t} \in S^{-1}P$.

Sia ora $f : A \to S^{-1}A$ data da $f(a \mapsto \frac{a}{1})$ l'immersione. Siano $\mathcal{P} = \{P \lhd A \text{ primo} \mid P \cap S = \emptyset\}$ e $\mathcal{Q} = \{Q \lhd S^{-1}A \mid \text{ primo}\}$. Consideriamo le due funzioni $\alpha : \mathcal{P} \to \mathcal{Q}$ definita da $\alpha(P \mapsto S^{-1}P)$ e $\beta : \mathcal{Q} \to \mathcal{P}$ definita da $\beta(Q \mapsto f^{-1}(Q) = Q \cap A)$. Per quanto prima, α è ben definita. β è ben definita perché la controimmagine di un ideale primo è un ideale primo e la controimmagine di ideali propri di $S^{-1}A$ ha intersezione banale con S. $\alpha \circ \beta = id$ per quanto visto nel teorema precedente. Mostriamo anche $\beta \circ \alpha = id$, ossia $\forall P \in \mathcal{P}\ P = f^{-1}(S^{-1}P)$. Il contenimento $P \subseteq f^{-1}(S^{-1}P)$ segue da $x \in P \Rightarrow \frac{x}{1} \in S^{-1}P \Rightarrow x \in f^{-1}(S^{-1}P)$. Per quello inverso osserviamo che $x \in f^{-1}(S^{-1}P) \Rightarrow \exists s \in S\ \frac{x}{s} = \frac{p}{r} \in S^{-1}P$ con $p \in P, r \in S$, quindi $xr = ps \in P$ e, poiché $r \in S$ e $S \cap P = \emptyset$, necessariamente $x \in P$. Quindi $f^{-1}(S^{-1}P) \subseteq P$.

Proposizione - ideali primi e parti moltiplicative: dato P ideale P è primo $\Leftrightarrow A \setminus P$ è una parte moltiplicativa.

dim. Sia $S = A \setminus P$. P è primo $\Leftrightarrow \forall x, y \in A\ xy \in P \Rightarrow x \in P$ o $y \in P \Leftrightarrow \forall x, y \in A\ x \notin P$ e $y \notin P \Rightarrow xy \notin P \Leftrightarrow \forall x, y \in A\ x \in S$ e $y \in S \Rightarrow xy \in S \Leftrightarrow \forall x, y \in A\ x \in S$ e $y \in S \Rightarrow xy \in S \Leftrightarrow S$ è un semigruppo moltiplicativo. Poiché $0 \in P \Rightarrow 0 \notin S$ S è una parte moltiplicativa.

Definizione - localizzazione: se P è un ideale primo, $S = A \setminus P$ allora $A_P = S^{-1}A$ è detto il localizzato di A a P; è un anello locale, ossia ha un solo ideale massimale.
Definizione - campo dei quozienti: se A è un dominio , e $S = A \setminus \{0\}$ allora indichiamo con K l'anello $S^{-1}A$, che è un campo, detto il campo dei quozienti di A. Esso è un campo ed è il minimo che contiene A.

2.4 UFD, PID, ED

Definizione - UFD: un dominio a fattorizzazione unica (o UFD: Unique Factorization Domain) è un dominio in cui per ciascun elemento non invertibile esiste una unica fattorizzazione come prodotto di elementi primi; la fattorizzazione si intende unica a meno dell'ordine e della moltiplicazione per invertibili.
Definizione - PID: un dominio a ideali principali (o PID: Principal Ideals Domain) è un dominio in cui tutti gli ideali sono principali.
Definizione - ED: un dominio euclideo (o ED: Euclidean Domain) è un dominio in cui

- esiste una funzione grado $d : A \setminus \{0\} \to \mathbb{N}$ tale che $\forall a, b \in A \setminus \{0\}\ d(a) \leq d(ab)$;
- $\forall a, b \in A, b \neq 0\ \exists q, r \in A$ tali che $a = qb + r$ e $r = 0$ oppure $d(r) < d(b)$.

Si noti che la seconda condizione parla della divisione (appunto) euclidea.
Teorema - caratterizzazione degli UFD: A UFD $\Leftrightarrow (i)$ ogni irriducibile è primo e (ii) ogni catena discendente di divisibilità è stazionaria (equivalentemente, ogni catena ascendente di ideali principali è stazionaria: condizione più debole di A Nötheriano).
Le condizioni sopra garantiscono rispettivamente l'unicità e l'esistenza della fattorizzazione in A.

dim. Ad algebra 2.

Esempio: Usando la caratterizzazione si mostra che $A = \mathbb{K}[\{\sqrt[n]{x} \mid n \geq 1\}]$ non è UFD, infatti esiste la catena discendente di divisibilità $\{x^{\frac{1}{2^n}}\}_{n\geq 1}$ per cui $x^{\frac{1}{2^{n+1}}} \mid x^{\frac{1}{2^n}}$.
Teorema - ideali primi in un PID: A PID $\Rightarrow$ gli unici ideali primi sono (0) e i massimali.

dim. (0) è primo in ogni dominio e i massimali sono primi in ogni anello. Sia ora $P = (x), P \neq \{0\}$ ideale primo. x primo $\Rightarrow$ x irriducibile, dunque (x) massimale nella classe degli ideali principali, che in un PID significa massimale.

Proposizione - come costruire un grado: prima di tutto si individuano gli invertibili e si assegna ad essi il grado 1. Si procede induttivamente, individuando gli elementi tali che dividere per essi dia come possibili resti solo 0 o elementi a cui è stato già assegnato un grado $< k \in \mathbb{N}$ e si assegna ad essi il grado k.

dim. Ad algebra 2 vedremo i dettagli.

Teorema - inclusioni: $ED \Rightarrow PID \Rightarrow UFD$.

dim. Per $PID \Rightarrow UFD$ usiamo la caratterizzazione degli UFD vista prima.

(i) Sia x irriducibile, allora (x) massimale nella classe degli ideali principali di A PID, dunque massimale, quindi x primo.

(ii) Sia $(a_1) \subseteq (a_2) \subseteq \dots$ una catena ascendente di ideali. Allora $I = \bigcup_{ns\in\mathbb{N}} a_n$ è un ideale. Poiché A è PID, è principale $I = (x)$ con $x \in A$. Poiché x appartiene all'unione degli (a_n) esiste un n_0 per cui $x \in (a_{n_0})$. Ma allora $(x) \subseteq (a_{n_0}) \subseteq (x) \Rightarrow (a_{n_0}) = (x)$ e quindi la catena è stazionaria da n_0 in poi, infatti $\forall n \geq n_0$ $(x) = (a_{n_0}) \subseteq (a_n) \subseteq (x)$.

Per $ED \Rightarrow PID$ consideriamo un generico ideale I di A e dimostriamo che è generato da un qualsiasi suo elemento di grado minimo in I, sia esso x. Dato $y \in I$, per divisione euclidea esistono $q, r \in A$ tali che $y = qx + r$ con $r = 0 \vee d(r) < d(x)$, ma $r = y - qx \in I$ non può avere grado minore di x, dunque $r = 0$, ossia $y \in (x)$. Quindi $I \subseteq (x) \subseteq I$, cioè $I = (x)$.

Definizione - massimo comune divisore: Ci sono definizioni differenti che si adattano alla struttura con cui stiamo lavorando; si dimostra però che sono consistenti. Siano $a, b \in A$ non entrambi nulli.

- in un UFD: siano $p_1, \dots, p_s$ i primi che dividono almeno uno tra a e b e siano $\alpha_i, \beta_i \in \mathbb{N}$ tali che $a = \prod_{i=1}^{s} p_i^{\alpha_i}, b = \prod_{i=1}^{s} p_i^{\beta_i}$. Allora $MCD(a, b) := \prod_{i=1}^{s} p_i^{\min(\alpha_i,\beta_i)}$;
- in un PID: $MCD(a, b)$ è definito come l'elemento d che soddisfa $(d) = (a, b)$;
- in un ED: $MCD(a, b)$ è definito come il risultato dell'algoritmo di Euclide (che termina sempre) applicato ad a, b.

dim. sono consistenti. Sia A PID; per quanto visto prima A è anche UFD. Consideriamo $d = MCD(a, b)$ secondo la definizione negli UFD. Dobbiamo dimostrare che vale anche $(d) = (a, b)$ e quindi d coincide con quello trovato dalla definizione per i PID. Guardiamo la fattorizzazione degli elementi in $(a, b) = \{ax+by \mid x, y \in A\}$. Possiamo sicuramente isolare dai due addendi $\prod_{i=1}^{s} p_i^{\min\{\alpha_i,\beta_i\}}$, da cui segue che $(a, b) \subseteq (d)$. Per l'altro contenimento, osserviamo che A PID $\Rightarrow \exists d' \in A$ $(a, b) = (d') \subseteq (d) \Rightarrow d' \mid \prod_{i=1}^{s} p_i^{\min\{\alpha_i,\beta_i\}}$. Se però almeno uno degli esponenti fosse più piccolo, diciamo quello di p_1 avrei un assurdo perché

esisterebbero $x, y \in A$ $d' = ax + by$ e basta allora guardare l'equazione modulo $p_1^{\min\{\alpha_1,\beta_1\}}$. Quindi $d' = d$.

Sia ora A ED; per quanto visto prima A è anche PID. Sia d tale che $(d) = (a, b)$. Se l'algoritmo di Euclide termina subito (cioè se $a = qb$), allora è chiaro $(b) = (a, b) = (d)$. Se invece $a = qb + r$ con $r \neq 0$, induciamo sul numero di passi dell'algoritmo. Per ogni x vale $(x|b \wedge x|r) \Leftrightarrow (x|b \wedge x|a)$. Sia allora $\tilde{d}$ l'elemento trovato dall'algoritmo applicato a b e r, per ipotesi induttiva $(\tilde{d}) = (b, r)$. Allora $\tilde{d}|a \wedge \tilde{d}|b$, da cui $\tilde{d}|d$, ma anche $d|b \wedge d|r$, da cui $d|\tilde{d}$, dunque $(d) = (\tilde{d})$.

Teorema - Bezout: Dato A PID $\forall a, b \in A$ $\exists x, y \in A$ tali che $ax + by = MCD(a, b)$.

dim. segue dalla definizione di massimo comune divisore.

Esempio - dominio non UFD: $\mathbb{Z}[\sqrt{-5}]$. Si usa che può essere dotato di una norma moltiplicativa (quella standard) e che $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, tutti primi.
Esempio - UFD non PID: $\mathbb{Z}[x]$ è UFD perché $\mathbb{Z}$ lo è, ma $(2, x)$ non è principale. O anche $\mathbb{Q}[x, y]$ è UFD per lo stesso motivo e (x, y) non è principale. Si noti che su $\mathbb{Z}[x]$ non vale il teorema di Bezout: $1 = MCD(2, x)$ non si scrive come combinazione lineare di 2 e x.
Esempio - PID non ED: $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. La dimostrazione è molto lunga e a lezione viene solo data l'idea. Se interessati a una trattazione dettagliata potete seguire questo link.
Proposizione - (*) MCD ed estensioni: Siano $A \subset B$ due UFD e $(a, b) \in A$. Indichiamo con $d_A = MCD_A(a, b)$ il massimo comun divisore di a e b su A, con d_B quello su B. Vale sempre $d_B \mid_B d_A$. Se inoltre su A o su B vale Bezout, allora anche $d_A \mid_B d_B$, ma l'ultima divisibilità è falsa in generale.

dim. Siano $a = d_A x$ e $b = d_A y$ con $x, y \in A$. Allora $MCD_B(a, b) = MCD_B(d_A x, d_A y) = d_A MCD_B(x, y)$, che è multiplo di d_A. Se in A vale Bezout, esistono $\alpha, \beta \in A$ $\alpha a + \beta b = d_A$. Da $d_B \mid_B a, b$ allora segue anche $d_B \mid_B d_A$, cioè d_B e d_A sono associati in B.

Senza ipotesi aggiuntive l'ultima affermazione è falsa: consideriamo $\mathbb{Z}[a, b]$, $MCD(a, b) = 1$ e l'immersione $\mathbb{Z}[a, b] \hookrightarrow \mathbb{Z}[a, b, x]$ tramite $a, b \mapsto ax, bx$. $MCD_{\mathbb{Z}[a,b,x]}(ax, bx) = x$, che non è unità.

Domanda: Vale in qualche senso anche l'inverso? È vero, per esempio, che dato A UFD, se per ogni B UFD estensione di A vale $\forall (a, b) \in A$ $d_B \mid_B d_A$, allora in A vale Bezout? Se trovate una risposta, per favore fateci sapere.

2.5 Anelli di polinomi

Definizione - $A[x]$: $A[x]$ è l'anello dei polinomi a coefficienti in A.
Proposizione - ideali primi: se P è un ideale primo di A allora $P[x]$ è un ideale primo di $A[x]$.

dim. basta notare che $\frac{A[x]}{P[x]} \cong \frac{A}{P}[x]$ e quindi P primo $\Leftrightarrow$ $\frac{A}{P}$ dominio $\Rightarrow$ $\frac{A}{P}[x]$ dominio $\Leftrightarrow$ $\frac{A[x]}{P[x]}$ dominio $\Leftrightarrow$ $P[x]$ primo.

Proposizione - invertibili: $A[x]^* = \{f(x) = \sum_{i=0}^{n} a_i x^i \in A[x] \mid a_0 \in A^*,\ a_1, \ldots, a_n \in \sqrt{(0)}\}$.

dim. Dimostriamo i due contenimenti.

Lemma: $\sqrt{(0)}[x] \subseteq \sqrt{(0)[x]}$

dim. sia $f(x) \in \sqrt{(0)}[x]$. Poiché $f(x)$ ha finiti coefficienti tutti nilpotenti, esiste un esponente M tale che tutti i coefficienti elevati a quel numero diano 0. Allora sviluppando con il multinomio di Newton si ha che $f(x)$ elevato alla $\deg(f)M$ fa il polinomio nullo, da cui segue $f(x) \in \sqrt{(0)[x]}$.

Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ tale che $a_0 \in A^*,\ a_1, \ldots, a_n \in \sqrt{(0)}]$. Allora $f(x) = a_0 - xg(x)$ dove $g(x) \in \sqrt{(0)}[x] \subseteq \sqrt{(0)[x]}$. Quindi esiste un esponente $M \in \mathbb{N}$ tale che $g(x)^M = 0$. Scegliamo senza perdita di generalità M dispari (se un esponente funziona, chiaramente funzionano tutti quelli maggiori o uguli a lui). Sia $h(x) = a_0^{-1} x g(x)$. Chiaramente anche $h(x)^M = 0$ Da $1 = 1 - h(x)^M = (1 - h(x))(1 + h(x) + \cdots + h(x)^{M-1})$ segue che $f(x)a_0^{-1}(1 + h(x) + \cdots + h(x)^{M-1}) = (a_0 + a_0 h(x))a_0^{-1}(1 + h(x) + \cdots + h(x)^{M-1}) = (1 + h(x))(1 + h(x) + \cdots + h(x)^{M-1}) = 1$ e quindi $f(x)$ è invertibile. Ciò dimostra $A[x]^* \supseteq \{f(x) = \sum_{i=0}^{n} a_i x^i \in A[x] \mid a_0 \in A^*,\ a_1, \ldots, a_n \in \sqrt{(0)}$.

Per l'altro contenimento consideriamo r tale che $f(x)r(x) = 1$. Allora $f(0)r(0) = 1$ e quindi $a_0 \in A^*$. Prendiamo ora un qualsiasi ideale primo P di A. $P[x]$ è primo per il lemma precedente e $\frac{A[x]}{P[x]} \cong \frac{A}{P}[x]$. Consideriamo l'uguaglianza $f(x)r(x) = 1$ in $\frac{A}{P}[x]$. Poichè quest'ultimo è un dominio, si ha che $\overline{f}(x)\overline{r}(x) = \overline{1} \Rightarrow \overline{f}(x) \in (\frac{A}{P}[x])^* \Rightarrow \overline{f}(x) \in (\frac{A}{P})^*$ e quindi $\overline{f}(x)$ è una costante. Da ciò segue che tutti i coefficienti diversi da a_0 sono in P, ossia $f(x) - a_0 \in P[x]$. Ma allora $f(x) - a_0 \in \bigcap_{P \lhd A \text{ primo}} P[x] = \sqrt{(0)}[x]$. Da ciò segue $A[x]^* \subseteq \{f(x) = \sum_{i=0}^{n} a_i x^i \in A[x] \mid a_0 \in A^*,\ a_1, \ldots, a_n \in \sqrt{(0)}$

Definizione - contenuto: dato A UFD, $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ chiamiamo contenuto di f $c(f) = MCD(a_0, \ldots, a_n)$.
Definizione - polinomio primitivo: dato A UFD, $f \in A[x]$ si dice primitivo se $c(f) = 1$.
Teorema - lemma di Gauss: Sia A UFD e $f, g \in A[x]$. Allora $c(fg) = c(f)c(g)$.

dim. Consideriamo prima di tutto il caso in cui sia f che g sono primitivi. Sia $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. Allora $f(x)g(x) = \sum_{k=1}^{n+m} x^k (\sum_{i=0}^{k} a_i b_{k-i})$. Sia ora p un qualsiasi primo, e siano n_0, m_0 i minimi interi tali che a_{n_0}, b_{m_0} non siano multipli di p (devono esistere altrimenti non si potrebbe avere $c(f) = c(g) = 1$). Allora si ha $\sum_{i=0}^{n_0+m_0} a_i b_{k-i} \equiv a_{n_0} b_{m_0} \not\equiv 0 \pmod{p}$ e quindi $p \nmid c(fg)$. Quindi anche $c(fg) = 1$ poiché non è diviso da nessun primo.

Nel caso generale, consideriamo $f_1, g_1 \in A[x]$ primitivi e tali che $f = c(f)f_1, g = c(g)g_1$. Allora si ha $c(fg) = c(c(f)c(g)f_1 g_1) = c(f)c(g)c(f_1 g_1) = c(f)c(g)$ per quanto detto.

Corollario - 1: Sia A UFD, K il suo campo dei quozienti e $f, g \in A[x]$ con g primitivo tali che $g(x) \mid f(x)$ in $K[x]$. Allora $g(x) \mid f(x)$ in $A[x]$.

dim. Sia $h(x) \in K[x]$ tale che $f(x) = g(x)h(x)$ e siano $a \in A, h_1 \in A[x]$ tali che $ah(x) = h_1(x)$ (basta considerare i coefficienti di h come ridotti ai minimi termini e prendere il mcm dei denominatori). Allora si ha $af(x) = g(x)h_1(x)$. Applichiamo il lemma di Gauss e otteniamo che $ac(f) = c(g)c(h_1) = c(h_1)$, e quindi $a \mid c(h - 1)$, da cui segue $h(x) = \frac{h_1(x)}{a} \in A[x]$, come voluto.

Corollario - 2: Sia A UFD, K il suo campo dei quozienti, $f \in A[x]$ e $g, h \in K[x]$ tali che $f(x) = g(x)h(x)$. Allora $\exists g_1, h_1 \in A[x]$ con $\deg(g_1) = \deg(g)$, $\deg(h_1) = \deg(h)$, e $f(x) = g_1(x)h_1(x)$.

dim. Come prima siano $a, b \in A, g_0, h_0 \in A[x]$ tali che $ag(x) = g_0(x)$. Sia $g_0(x) = c(g_0)g_1(x)$ con $g_1(x)$ primitivo. Allora $g_1(x) \mid f(x)$ in $K[x]$ e siamo nelle ipotesi del corollario 1, e quindi $g_1(x) \mid f(x) in A[x]$. Da $af(x) = ag(x)h(x) = c(g_0)g_1(x)h(x)$ segue che allora possiamo definire $h_1(x) := a^{-1}c(g_0)h(x) \in A[x]$ e abbiamo la tesi.

Teorema - equivalenza interessante: A campo $\Leftrightarrow A[x]$ PID.

dim. Supponiamo $A[x]$ PID. Notiamo intanto che $A[x]$ dominio $\Rightarrow A$ dominio, essendo A un sottoanello di $A[x]$. Consideriamo l'omomorfismo di valutazione in 0 $\psi_0 : A[x] \to A$. Chiaramente è suriettivo (basta

guardare i polinomi costanti) e $\text{Ker}(\psi_0) = (x)$, da cui segue $A[x]/(x) \cong A$. Poiché l'immagine A è un dominio, necessariamente l'ideale (x) è primo, e quindi, essendo $\neq (0)$, per quanto visto sugli ideali primi nei PID è un ideale massimale. Allora per $A[x]/(x) \cong A$ vale che A è un campo.

Sia ora A un campo. Allora $A[x]$ è un ED con grado dato dal grado del polinomio (dimostrazione vista ad aritmetica), e quindi in particolare è un PID.

Teorema - irriducibili in $A[x]$: Se A è UFD gli irriducibili di $A[x]$ sono tutti e soli gli elementi f tali che o $f \in A$ irriducibile oppure $\deg(f) \geq 1$, $c(f) = 1$ e f irriducibile in $K[x]$.

dim. Chiaramente $f(x) = g(x)h(x)$ con $g(x)h(x) \in A[x] \Rightarrow \deg(g), \deg(h) \leq \deg(f)$. Quindi se $\deg(f) = 0$ per forza se si fattorizza f in $A[x]$ la fattorizzazione deve contenere solo costanti, ossia elementi di A, e quindi è irriducibile se e solo se è irriducibile in A.

Se invece $\deg(f) \geq 1$ distinguiamo i casi. Se $c(f) \neq 1$ allora $f(x) = c(f)f_1(x)$ con $f_1(x)$ primitivo non costante. Nessuno dei due termini è invertibile e quindi f non è irriducibile. Se invece $c(f) = 1$ notiamo intanto che f irriducibile in $K[x] \Rightarrow f(x)$ irriducibile in $A[x]$ (una fattorizzazione in $A[x]$ è valida anche in $K[x]$). Dimostriamo ora che irriducibile in $A[x] \Rightarrow$ irriducibile in $K[x]$. Se f riducibile in $K[x]$ esistono $g, h \in K[x]$ tali che $\leq \deg(g)\deg(h) < \deg(f)$ e $f = gh$ e quindi , per il secondo corollario del lemma di Gauss esisterebbero $g_1, h_1 \in A[x]$ tali che $\deg(g_1) = \deg(g)$, $\deg(h_1) = \deg(h)$, e $f(x) = g_1(x)h_1(x)$, da cui f è riducibile anche in $A[x]$. Quindi se f è un polinomio primitivo non costante, è irriducibile in $A[x]$ se e solo se lo è in $K[x]$.

Teorema - polinomi UFD: A UFD $\Rightarrow A[x]$ UFD.

dim. Sia K il campo dei quozienti di A e sia $f(x) \in A[x]$. Allora $f(x) \in K[x]$ che per quanto visto è un PID e quindi un UFD. Sia $f(x) = \prod_{i=1}^{s} g_i(x)^{\alpha_i}$ la fattorizzazione di $f(x)$ in $K[x]$ (wlog g_i tutti non costanti). Dal corollario 2 del lemma di Gauss segue che esistono $h_1, \ldots, h_s \in A[x]$ tali che $\deg(g_i) = \deg(h_i)$ $\forall i = 1, \ldots, s$ (si nota che dalla dimostrazione del lemma e del fatto che i g_i erano irriducibili in $K[x]$ segue che anche gli h_i sono irriducibili in $K[x]$) e $f(x) = \prod_{i=1}^{s} h_i(x)^{\alpha_i} = \prod_{i=1}^{s} (c(h_i)k_i(x))^{\alpha_i} = \prod_{i=1}^{s} c(h_i)^{\alpha_i} \prod_{i=1}^{s} k_i(x)^{\alpha_i}$ dove i k_i sono polinomi primitivi non costanti. Poiché essi sono primitivi e irriducibili in $K[x]$ (per costruzione) sono anche irriducibili in $A[x]$. Il fatto che la fattorizzazione $\prod_{i=1}^{s} k_i(x)^{\alpha_i}$ sia l'unica possibile per il secondo termine segue dall'unicità della fattorizzazione in $K[x]$. Inoltre $\prod_{i=1}^{s} c(h_i)^{\alpha_i} \in A \Rightarrow$ possiede un'unica fattorizzazione in irriducibili poiché A è UFD. Quindi i due termini che compongono $f(x)$ hanno ciascuno un fattorizzazione unica, e metterle insieme fornisce una e una sola fattorizzazione per $f(x)$ perché in un caso stiamo considerando solo irriducibili di $A[x]$ in A e nell'altro caso solo irriducibili in $A[x] \setminus A$.

Teorema - criterio di Eisenstein: Sia A UFD, $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ primitivo e $p \in A$ un primo tale che (i) $p \nmid a_n$, (ii) $p \mid a_i$ per $i = 0, \ldots, n-1$, (iii) $p^2 \nmid a_0$. Allora $f(x)$ è irriducibile in $A[x]$ (e quindi anche in $K[x]$ per uno dei teoremi precedenti).

dim. Chiaramente si deve avere $\deg(f) = n \geq 1$. Supponiamo che esistano $g, h \in A[x]$ tali che $f(x) = g(x)h(x)$. Vediamo l'equazione di prima modulo p, considerando le immagini dei polinomi nell'anello $\frac{A}{(p)}[x] \cong \frac{A[x]}{(p)[x]}$. Per ipotesi: $a_n x^n \equiv \overline{f}(x) = \overline{g}(x)\overline{h}(x) \pmod{p}$. Poiché se il prodotto di due polinomi è un monomio allora sono entrambi monomi (basta guardare i termini di grado minimo e massimo nel prodotto e notare che i gradi devono coincider), l'unica possibilità è $\overline{g}(x) = bx^j, \overline{h}(x) = cx^k$ con $j + k = n$ e $b, c \not\equiv 0 \pmod{p}$ (poiché $bc \equiv a_n \not\equiv 0 \pmod{p}$). Allora si ha $g(x) = bx^j + pg_1(x), h(x) = cx^k + ph_1(x)$ dove $g_1, h_1 \in A[x]$. Notiamo ora che se $j, k \geq 1$ $a_0 f(0) = g(0)h(0) = pg_1(0) \cdot ph_1(0) = p^2 g_1(0)h_1(0)$ e si

ha quindi un assurdo. Quindi almeno uno tra j e k è uguale a 0. Supponiamo senza perdita di generalità j. Allora si ha anche $k = n - j = n$. Guardiamo i gradi dei polinomi. $f(x) = g(x)h(x) \Rightarrow n = \deg(f) = \deg(g) + \deg(h)$ Poiché $h = cx^n + ph_1(x)$ e $p \nmid c$, necessariamente $\deg(h) \geq n \Rightarrow \deg(h) = n, \deg(g) = 0$, che è assurdo perché allora g è una costante che divide f, che contraddice il fatto che f sia primitivo.

2.6 L'anello $\mathbb{Z}[x]$

Proposizione - ideali primi e massimali: Gli ideali primi di $\mathbb{Z}[x]$ sono della forma: $(p), (p, \mu(x)), (\lambda(x))$ dove p è un primo, $\mu(x), \lambda(x)$ sono polinomi rispettivamente irriducibili in $\mathbb{F}_p[x]$ e $\mathbb{Z}[x]$. Gli ideali massimali, invece, sono solo quelli della forma $(p, \mu(x))$ con $p, \mu(x)$ come prima.

dim. Sia $M \subseteq \mathbb{Z}[x]$ un ideale massimale. Notiamo che massimale $\Rightarrow$ primo quindi caratterizziamo prima gli ideali primi e poi vediamo se possono essere massimali. Consideriamo l'immersione $\iota : \mathbb{Z} \to \mathbb{Z}[x]$. ι è un omomorfismo, quindi controimmagine di ideale primo è ideale primo: $\iota^{-1}(M) = M \cap \mathbb{Z} \subseteq \mathbb{Z}$ è ideale primo. Poiché $\mathbb{Z}$ è PID, gli ideali primi sono (0) e i massimali, dove i massimali sono della forma (p) con p primo. Distinguiamo i casi.

- $M \cap \mathbb{Z} = (p)$: proiettiamo M in $\mathbb{F}_p[x]$ (usiamo che $\frac{\mathbb{Z}[x]}{(p)[x]} \cong \frac{\mathbb{Z}}{(p)}[x] = \mathbb{Z}/p\mathbb{Z}[x] = \mathbb{F}_p[x]$). Poiché la proiezione, che chiamiamo π_p, è un omomorfismo suriettivo, immagine di ideale primo è ideale primo. Come prima poiché $\mathbb{F}_p[x]$ è PID si ha o $\pi(M) = (0)$ o $\pi_p(M) = (\overline{\mu(x)})$ con $\mu(x)$ irriducibile in $\mathbb{F}_p[x]$ (e $\overline{\mu(x)}$ ottenuto riducendo modulo p tutti i coefficienti di un opportuno polinomio $\mu[x] \in \mathbb{Z}[x]$ (che esiste sempre, ad esempio $\mu(x) = x$). Nel primo caso si ha che l'ideale è primo ma non massimale, perché contenuto certamente in un ideale del secondo tipo. Nel secondo caso invece $M = \pi_p^{-1}(\pi_p(M)) = \pi_p^{-1}((\overline{\mu(x)})) = \mu[x] + \mathrm{Ker}(\pi_p) = \mu[x] + (p) = (p, \mu(x))$.
- $M \cap \mathbb{Z} = (0)$: prendiamo il campo dei quozienti di $\mathbb{Z}$, $\mathbb{Q}$. Per teoria vista a lezione M ideale primo in $\mathbb{Z}[x]$ corrisponde a $S^{-1}M$ ideale primo in $\mathbb{Q}[x]$, dove $S = \mathbb{Z}\backslash\{0\}$. Quindi, poiché $\mathbb{Q}[x]$ è PID, $S^{-1}M = (\lambda(x))$ con $\lambda(x) \in \mathbb{Q}[x]$ irriducibile. Notiamo ora che per il lemma di Gauss $\forall p(x) \in \mathbb{Z}[x]$ primitivo si ha (indichiamo $(p(x))A[x]$ l'ideale generato da $p(x)$ in $A[x]$) $((p(x))\mathbb{Q}[x]) \cap \mathbb{Z}[x] = (p(x))\mathbb{Z}[x]$. Il lemma di Gauss ci dice infatti che se un polinomio a coefficienti interi è divisibile in $\mathbb{Q}$ per p, allora lo è anche in $\mathbb{Z}$, e quell'equazione riflette insiemisticamente questo enunciato. Scegliendo allora un rappresentante a coefficienti interi e primitivo per $\lambda[x]$ si ha $M = ((\lambda(x))\mathbb{Q}[x]) \cap \mathbb{Z}[x] = (\lambda(x))\mathbb{Z}[x]$. Dimostriamo ora che gli ideali di questa forma non sono massimali. $(\lambda(x))$ è massimale $\Leftrightarrow \frac{\mathbb{Z}[x]}{(\lambda(x))}$ è campo. Poiché $\lambda(x)$ deve essere non costante, esiste un valore x_0 tale che $\lambda(x_0) \neq 0, \pm 1$. Esiste allora q un primo che divide x_0. Se $\frac{\mathbb{Z}[x]}{(\lambda(x))}$ campo, allora esisterebbero $a(x), b(x) \in \mathbb{Z}[x]$ tali che $qa(x) + \lambda(x)b(x) = 1$. Ma valutando questa relazione in $x = x_0$ si avrebbe allora un assurdo guardando la divisibilità per q.

3 Teoria dei campi

Dove non diversamente specificato Ω è un campo qualsiasi con operazioni $+$ e $\cdot$ (il cui simbolo verrà omesso). L'elemento neutro della somma sarà indicato con 0, quello del prodotto con 1. K, L, F, E saranno sempre sottocampi di questo campo ambiente Ω.

3.1 Definizioni e richiami di Aritmetica

Definizione - estensione di campo: per dire che K è un sottocampo di Ω si scrive Ω/K e si dice che Ω è un'estensione di campo (o semplicemente "estensione") di K. Indichiamo con $[\Omega : K] = \dim_K(\Omega)$ la dimensione di Ω come spazio vettoriale su K. L'estensione si dice finita se $[\Omega : K] < +\infty$.

Definizione - estensione semplice: dato $\alpha \in \Omega \setminus K$ si indica con $K(\alpha)$ il minimo campo contenuto in Ω contenente sia K che α.

Definizione - estensione generata: dato $S \subseteq \Omega$, indichiamo con $K(S) = \bigcap_{\substack{K \subseteq K' \subseteq \Omega \\ K' \text{campo}}} F$ l'estensione generata da S su K.

Definizione - composto di campi: dati L, F, indichiamo con LF il minimo campo che li contiene entrambi, ossia $L(F) = F(L)$.

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi_\alpha} & K(\alpha) \\ \downarrow{\scriptstyle \pi} & \nearrow_{\sim} & \\ \frac{K[x]}{\mathrm{Ker}(\varphi_\alpha)} & & \end{array}$$

Sia ora $\alpha \in \Omega$. Indichiamo con φ_α l'omomorfismo di valutazione in α, ossia $\varphi_\alpha : K[x] \to K[\alpha]$ tale che $\varphi_\alpha(f(x) \mapsto f(\alpha))$. Poiché come visto sopra $K[x]$ è un PID, $\mathrm{Ker}(\varphi_\alpha)$ è principale, ossia $\exists \mu_\alpha(x) \in K[x]$ tale che $\mathrm{Ker}(\varphi_\alpha) = (\mu_\alpha(x))$.

Definizione - trascendente: se $\mu_\alpha(x)$ definito sopra è il polinomio nullo, α si dice trascendente (su K).

Definizione - algebrico: se $\mu_\alpha(x)$ non è il polinomio nullo, α si dice algebrico (su K). In questo caso $K(\alpha) \cong K[x]$, ossia è proprio come se α fosse un'indeterminata, ossia non si "combina" con nessun elemento diverso da s stessa (e infatti possiamo pensare l'indeterminata x è un elemento trascendente su qualsiasi campo).

Definizione - polinomio minimo: se α è algebrico, fissiamo $\mu_\alpha(x)$ come l'unico generatore monico di $\mathrm{Ker}(\varphi_\alpha)$. Esso coincide con l'unico polinomio tale che (i) è monico, (ii) è irriducibile, (ii) si annulla in α. (Si dimostra l'unicità e l'equivalenza delle definizioni). $\mu_\alpha(x)$ così definito è detto il polinomio minimo di α su K. Vale che $\deg(\mu_\alpha(x)) = \deg \frac{K[x]}{(\mu_\alpha(x))} = [K(\alpha) : K]$

Definizione - estensione algebrica: L/K si dice algebrica se ogni elemento di L è algebrico su K.

Proposizione - estensione finita è algebrica: se L/K è finita di grado n basta notare che $\forall \alpha \in L$ $1, \alpha, \ldots, \alpha^n$ sono linearmente dipendenti e quindi esiste un polinomio di grado al più n che si annulla in α (la combinazione lineare delle potenze di α fino a n che dà come risultato 0).

3.2 Proprietà delle estensioni di campo

Teorema - torri di estensioni finite: dato il diagramma a lato, vale L/K finita $\Leftrightarrow$ L/F e F/K sono finite. Inoltre in questo caso $[L : K] = [L : F][F : K]$.

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

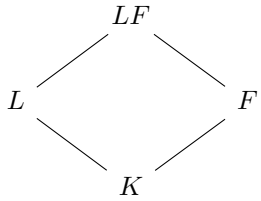
dim. Se L/K è finita, poiché $F \subseteq L$ anche F/K è finita. Inoltre una qualsiasi K-base per L/K è un F-insieme di generatori per L/F, quindi anche L/F finita. Nell'altro verso, date L/F e F/K entrambe finite

consideriamo due basi $\alpha_1, \ldots, \alpha_n \in L$ e $\beta_1, \ldots, \beta_m \in F$ tali che $L = F(\alpha_1, \ldots, \alpha_n)$ e $F = K(\beta_1, \ldots, \beta_m)$. Mostriamo che $\{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ sono una base per L/K.

- sono generatori: sia $\gamma \in L$; per $\{\alpha_i\}$ base $\exists f_1, \ldots, f_n \in F$ $\gamma = \sum_{i=1}^{n} f_i\alpha_i$; analogamente per $\{\beta_i\}$ base $\forall f_i$ $\exists k_{i,1}, \ldots, k_{i,m} \in K$ $f_i = \sum_{j=1}^{m} k_{i,j}\beta_j$. Mettendo insieme le varie espressioni: $\gamma = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{m} k_{i,j}\beta_j = \sum_{i=1}^{n}\sum_{j=1}^{m} k_{i,j}\alpha_i\beta_j$ e quindi $\alpha_i\beta_j$ generano
- lineare indipendenza: se $0 = \sum_{i=1}^{n}\sum_{j=1}^{m} k_{i,j}\alpha_i\beta_j = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{m} k_{i,j}\beta_j$ si ha per lineare indipendenza degli α_i che $\forall i = 1, \ldots, n$ $\sum_{j=1}^{m} k_{i,j}\beta_j = 0$ e allora per lineare indipendenza dei β_j $\forall i = 1, \ldots, n$ $\forall j = 1, \ldots, m$ $k_{i,j} = 0$.

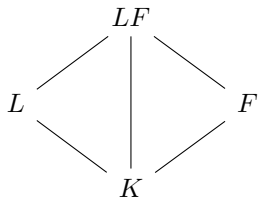
Questo dimostra che l'estensione è finita e la moltiplicatività.

Teorema - shift di estensioni finite: dato il diagramma a lato, vale L/K finita $\Rightarrow$ LF/F finita. Inoltre, $[LF : F] \leq [L : K]$.



dim. Basta notare che se $\alpha_1, \ldots, \alpha_n$ è una base per L/K, allora genera LF/F.

Teorema - composto di estensioni finite: dato il diagramma a lato, vale L/K finita e F/K finita $\Rightarrow$ LF/F finita. Inoltre, $[LF : K] \leq [L : K][L : F]$.



dim. Per shift, da L/K finita, segue LF/F finita e $[LF : F] \leq [L : K]$. Allora per torri da LF/F e F/K finite segue LF/K finita e $[LF : K] = [LF : F][F : K] \leq [L : K][F : K]$.

Fatto: Un'estensione finitamente generata da elementi algebrici è algebrica.

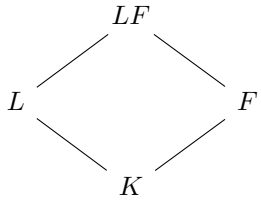
dim. Basta notare che gli elementi algebrici hanno grado finito sul campo base e quindi un'estensione generata da un numero finito di essi ha grado finito (al più il prodotto dei gradi). L'estensione è finita, dunque algebrica.

Teorema - torri di estensioni algebriche: dato il diagramma a lato, vale L/K algebrica $\Leftrightarrow$ L/F e F/K sono algebriche.

dim. Se L/K è algebrica e $\alpha \in L$ allora α algebrico su $K \Rightarrow \alpha$ algebrico su F perché almeno un polinomio in $F[x]$ (il polinomio minimo di α su K) si annulla in α. Quindi L/F algebrica. Inoltre se $\alpha \in F \subseteq L$ allora α algebrico su K per ipotesi, e quindi F/K algebrica.

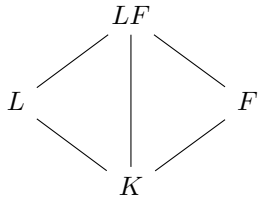
Per la freccia inversa, notiamo che $\alpha \in L$ è algebrico su F e quindi esiste il suo polinomio minimo su F $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in F$ $\forall i = 0, \ldots, n$. Allora α è algebrico su $K(a_0, \ldots, a_n) \subseteq F$. Poiché F/K è algebrica $K(a_0, \ldots, a_n)$ è un'estensione di K finitamente generata da elementi algebrici e quindi è finita, che ci permette di dire che allora anche $K(\alpha, a_0, \ldots, a_n)$ è finita, e quindi algebrica, su K, e quindi α è algebrico su K.

Teorema - shift di estensioni algebriche: dato il diagramma a lato, vale L/K algebrica $\Rightarrow$ LF/F algebrica.



dim. Basta notare che se $\forall \alpha \in L$, se $f(x) \in K[x]$ è il polinomio minimo di α su K, allora in particolare esso è un polinomio di $F[x]$ che si annulla in α, e quindi α ha un polinomio minimo su F, e quindi è algebrico su F. Quindi $F(L) = LF$ è algebrica su F.

Teorema - composto di estensioni algebriche: dato il diagramma a lato, vale L/K algebrica e F/K algebrica $\Rightarrow$ LF/F algebrica.



dim. Per shift, da L/K algebrica, segue LF/F algebrica. Allora per torri da LF/F e F/K algebriche segue LF/K algebrica.

Definizione - campo algebricamente chiuso: K si dice algebricamente chiuso se ogni polinomio in $K[x]$ ha almeno una radice in K. Si verifica facilmente che K algebricaente chiuso sse gli unici irriducibili sono i polinomi di grado al più 1 e sse ogni polinomio in $K[x]$ si spezza nel prodotto di fattori di grado 1.
Definizione - chiusura algebrica: $\overline{K}$ è una chiusura algebrica di K se $K \subseteq \overline{K}$, $\overline{K}/K$ è algebrica e $\overline{K}$ è algebricamente chiuso.
Teorema - esistenza e unicità della chiusura algebrica: Per ogni campo K esiste una chiusura algebrica, che è unica a meno di isomorfismo (ossia date due chiusure algebriche esiste un isomorfismo, tale che ristretto a K sia l'identità, tra esse).

dim. Ad algebra 2.

Teorema - algebrici su un campo: Gli elementi algebrici su K formano a loro volta un campo.

dim. Sia $K' = \{\alpha \in \overline{K} \mid \alpha \text{ algebrico su } K\}$. Presi $\alpha, \beta \in \overline{K}'$ $K(\alpha, \beta)$ è finita perché α, β sono algebrici $\Rightarrow$ poiché $\alpha + \beta, \alpha\beta, \frac{\alpha}{\beta} \in K(\alpha, \beta)$ essi hanno grado finito su K e quindi sono algebrici $\Rightarrow$ $\alpha + \beta, \alpha\beta, \frac{\alpha}{\beta} \in K'$. Quindi K' è un campo.

Teorema - chiusura algebrica di $\mathbb{Q}$: $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebrico su } \mathbb{Q}\}$

dim. $\overline{\mathbb{Q}}$ campo segue dal teorema precedente, $\overline{\mathbb{Q}}/\mathbb{Q}$ algebrica segue dalla definizione. Manca mostrare che è algebricamente chiuso. Sia $f(x) \in \overline{\mathbb{Q}}[x]$ e sia α una radice di f nella chiusura algebrica di $\overline{\mathbb{Q}}$. Allora per definzione $\overline{\mathbb{Q}}(\alpha)/\overline{\mathbb{Q}}$ è algebrica, e quindi per torri anche $\overline{\mathbb{Q}}(\alpha)/\mathbb{Q}$ è algebrica, e quindi α algebrico su $\mathbb{Q} \Rightarrow \alpha \in \overline{\mathbb{Q}}$.

Definizione - campo di spezzamento: sia $\mathscr{F} = \{f_i \mid i \in I\}$ una famiglia di polinomi in $K[x]$. Il campo di spezzamento di $\mathscr{F}$ su K è allora il minimo campo in $\overline{K}$ che contiene tutte le radici di tutti i polinomi in $\mathscr{F}$.

3.3 Criterio della derivata e campi finiti

Proposizione - criterio della derivata: $f(x) \in K[x]$ ha radici multiple in $\overline{K} \Leftrightarrow (f(x), f'(x)) \neq 1$.

dim. ($\Leftarrow$) Notiamo $f \neq 0 \Rightarrow (f(x), f'(x)) \neq 0$. Sia $\alpha \in \overline{K}$ una radice di (f, f'). Scriviamo $f(x) = (x - \alpha)g(x) \in \overline{K}[x]$. Deriviamo f con la regola di Leibniz, valutando f' in α si ha $0 = f'(\alpha) = g(\alpha) + (\alpha - \alpha)g'(x)$, da cui $g(\alpha) = 0$, cioè $g(x) = (x - \alpha)h(x)$ e quindi $f(x) = (x - \alpha)^2 h(x)$.

($\Rightarrow$) Sia $f(x) = (x - \alpha)^2 g(x) \in \overline{K}[x]$, allora $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$, in particolare $(x - \alpha) \mid f'(x)$. Poiché $f(x), f'(x) \in K[x]$ e $f(\alpha) = f'(\alpha) = 0$, detto $\mu_\alpha(x) \in K[x]$ il polinomio minimo di α su K

sia ha $\mu_\alpha(x)|f(x), f'(x)$ e dunque $\mu_\alpha(x) \mid (f(x), f'(x))$ che deve quindi essere nullo o avere grado positivo: in particolare $(f(x), f'(x)) \neq 1$.

Corollario - derivata di irriducibili: Sia $f(x) \in K[x]$ irriducibile. f ha radici multiple $\Leftrightarrow f'(x) = 0$.

dim. Notiamo $(f(x), f'(x)) \mid f(x)$ e $f(x)$ irriducibile, dunque $(f(x), f'(x)) \in \{1, f(x)\}$. Per il criterio della derivata allora f ha radici multiple $\Leftrightarrow (f(x), f'(x)) = f(x)$. Ma $\deg f'(x) \leq \deg f(x)$ e $f(x) \mid f'(x)$ implicano necessariamente $f'(x) = 0$.

Proposizione - omomorfismo di Fröbenius: Sia K un campo a caratteristica p. Allora la mappa $\Phi : K \to K$ tale che $\Phi(a \mapsto a^p)$ è un omomorfismo iniettivo (detto *di Fröbenius*). Se K è finito quindi Φ è un automorfismo.

dim. Notiamo che $\Phi(0) = 0$, $\Phi(1) = 1$ e $\Phi(a)\Phi(b) = \Phi(ab)$ perché un campo è commutativo. Manca solo $\Phi(a) + \Phi(b) = \Phi(a + b)$, ma sviluppando il binomio di Newton, $(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$, infatti $k \neq 0, p \Rightarrow p \mid \binom{p}{k}$. (Quest'ultima identità viene talvolta indicata come "binomio ingenuo".) Chiaramente $\mathrm{Ker}(\Phi) = \{0\}$, quindi l'omomorfismo è iniettivo. Se K è finito, tanto basta a dire che Φ è un automorfismo.

Definizione - campo perfetto: K si dice perfetto se ogni polinomio irriducibile $f(x) \in K[x]$ ha radici tutte distinte in $\overline{K}$.
Proposizione - due classi di campi perfetti: Se K è un campo finito o di caratteristica 0, allora è perfetto.

dim. Sia $f \in K[x]$ irriducibile, $f(x) = \sum_{i=0}^{n} a_i x^i$, $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Sappiamo che f ha radici multiple $\Leftrightarrow f'(x) = 0$, cioè se $\forall i = 1 \dots n$ vale $i a_i = 0$.

Se K è a caratteristica 0, allora $(\forall i = 1 \dots n \; i a_i = 0) \Rightarrow f(x) = a_0$ costante. In questo caso f non ha radici oppure è il polinomio nullo.

Se K è finito e a caratteristica p, allora $f'(x) = 0$ se e solo se per tutti gli indici $i = 1 \dots n$ non multipli di p vale $a_i = 0$. Ma allora $f(x) = \sum_{i=0}^{m} a_{pi} x^{pi} = g(x^p)$ con $g(t) = \sum_{i=0}^{m} a_{pi} t^i \in K[x]$. Per l'omomorfismo di Fröbenius $f(x) = g(x^p) = g(x)^p$: assurdo poiché f è irriducibile.

Teorema - esistenza e unicità di $\mathbb{F}_{p^n}$: Per ogni primo p e intero $n \geq 1$, esiste un unico campo F con p^n elementi all'interno di una fissata chiusura algebrica di $\mathbb{F}_p$.

dim. Se F esiste, allora $\#F^* = p^n - 1$, dunque per Lagrange gli elementi di F^* sono radici in $\overline{\mathbb{F}_p}$ di $x^{p^n - 1} - 1$ e gli elementi di F sono radici di $f(x) = x^{p^n} - x$. Per il criterio della derivata queste radici sono tutte distinte, infatti $f'(x) = p^n x^{p^n - 1} - 1 = -1$ in caratteristica p. Ma allora $F = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0\}$ è l'unico candidato p^n-campo (unicità). Si verifica che F così definito contiene 0, 1, è chiuso per somma, prodotto, opposti e inversi (esercizio), dunque è un campo (esistenza).

Dunque $\mathbb{F}_{p^n}$ è il campo di spezzamento su $\mathbb{F}_p$ di $x^{p^n} - x = 0$ e $\mathbb{F}_{p^n}^*$ sono tutte e sole le $p^n - 1$-esime radici dell'unità.
Teorema - Sottogruppi moltiplicativi di un campo: Sia K campo e $G < K^*$ un sottogruppo moltiplicativo. Se G è finito, allora è ciclico.

dim. Sia $\#G = n$, $\forall g \in G \; g^n = 1$. Definiamo $f_d(x) = x^d - 1 \in K[x]$. Per Ruffini f_d ha al più d radici in G. Sia $G_d = \{\alpha \in G \mid \alpha^d - 1 = 0\}$, vale $\#G_d \leq d$. Sia $k_d = \#\{\alpha \in G \mid \mathrm{ord} g = d\}$. Se $d \nmid n$, allora $k_d = 0$,

se invece $d \mid n$ e $k_d > 0$, dato $g \in G$ ord$g = d$ si ha $\langle g \rangle \subseteq G_d$, ma allora per cardinalità $\langle g \rangle = G_d$, dunque $k_d = \varphi(d)$. Si ha

$$n = \#G = \sum_{d|n} k_d \leq \sum_{d|n} \varphi(d) = n,$$

che quindi sono tutte uguaglianze e $k_n = \varphi(n) \geq 1$, cioè $\exists g \in G$ ord$g = n$, vale a dire G ciclico.

Corollario - $\mathbb{F}_{p^n}^*$: $\mathbb{F}_{p^n}^*$ è ciclico. Inoltre $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ per qualche $\alpha \in \overline{\mathbb{F}_p}$.

dim. $\mathbb{F}_{p^n}^* = \langle \alpha \rangle \wedge \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n} \Rightarrow \mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$.

Osservazione - non vale l'implicazione inversa: $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \not\Rightarrow \langle \alpha \rangle = \mathbb{F}_{p^n}^*$.

dim. Funziona più o meno qualunque controesempio con $p^n - 1$ non primo. Consideriamo $\mathbb{F}_9 \cong \frac{\mathbb{F}_3[x]}{(x^2+1)} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$: ogni elemento $\alpha \in \mathbb{F}_9 \setminus F_3$ ha necessariamente polinomio minimo di grado 2 su $\mathbb{F}_3$, dunque $F_3(\alpha) = \mathbb{F}_9$. Tuttavia $\langle x \rangle = \{x, -1, x, 1\} \neq \mathbb{F}_9^*$.

Corollario - polinomi irriducibili su $\mathbb{F}_p$: Per ogni p primo, $n \geq 1$ naturale esistono in $\mathbb{F}_p[x]$ polinomi irriducibili di grado n.

dim. Sia $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ per qualche $\alpha \in \overline{\mathbb{F}_p}$, allora $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n = \deg \mu_\alpha(x)$ irriducibile.

Proposizione - inclusioni tra sottocampi: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m|n$.

dim. ($\Rightarrow$) Per torri $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]m$. ($\Leftarrow$) Ricordiamo il prodotto notevole $(x^m)^\lambda - 1 = (x^m - 1)((x^m)^{\lambda-1} + \cdots + 1)$, in particolare per $x = p$ si ha $p^n - 1 = a(p^m - 1)$ per un opportuno a intero. Allora $\forall \alpha \in \mathbb{F}_{p^m}^*$ $\alpha^{p^m-1} = 1$, ma allora anche $\alpha^{p^n-1} = (\alpha^{p^m-1})^a = 1^a = 1$, cioè $\alpha \in \mathbb{F}_{p^n}^*$.

Osservazione - radici di irriducibli: Sia $f(x) \in \mathbb{F}_p[x]$ irriducibile di grado n e siano $\{\alpha_1, \ldots, \alpha_n\} \subseteq \overline{\mathbb{F}_p}$ le sue radici (che sappiamo essere distinte). f è il polinomio minimo degli α_i su $\mathbb{F}_p$, quindi $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha_1) = \cdots = \mathbb{F}_p(\alpha_n) \cong \frac{\mathbb{F}_p[x]}{f(x)}$. Si noti che l'estensione semplice con una radice di f ha automaticamente incluso tutte le radici di tutti gli irriducibili di grado (esattamente) n.

Proposizione - Campo di spezzamento su $\mathbb{F}_q$ ($q = p^n$): Sia $f \in \mathbb{F}_q[x]$ $f(x) = f_1^{e_1}(x) \ldots f_r^{e_r}(x)$ con gli $f_i(x)$ irriducibili e deg $f_i = d_i$. Allora, detto $d = [d_1, \ldots, d_r]$ l'mcm dei gradi, il campo di spezzamento di f su $\mathbb{F}_q$ è $\mathbb{F}_{q^d}$

dim. Il campo di spezzamento (in seguito, cds) di f su $\mathbb{F}_q$ è il composto dei cds degli f_i su $\mathbb{F}_q$. Il cds di f_i su $\mathbb{F}_q$ è $\mathbb{F}_{q^{d_i}}$. Sia allora $\mathbb{F}_{q^c}$ il cds f su $\mathbb{F}_q$. Vale $\mathbb{F}_{q^{d_i}} \subset \mathbb{F}_{q^c}$ se e solo se $d_i|c$, dunque $d = [d_1, \ldots, d_r] \mid c$. $\mathbb{F}_{q^d}$ è il più piccolo campo che contiene tutti gli $\mathbb{F}_{q^{d_i}}$, vale a dire il cds.

Teorema - Campo di spezzamento su $\mathbb{F}_p$ di $x^n - 1$: Sia $n = p^a m$ con $(m, p) = 1$. Allora il campo di spezzamento di $x^n - 1$ su $\mathbb{F}_p$ coincide con il cds di $x^m - 1$ su $\mathbb{F}_p$ ed è uguale a $\mathbb{F}_{p^d}$ con $d = \text{ord}_{\mathbb{Z}/n\mathbb{Z}^*} p$.

dim. $x^{p^a m} - 1 = (x^m - 1)^{p^a}$ per il binomio ingenuo, dunque moltiplicare m per una potenza di p cambia solo la molteplicità delle radici di $x^m - 1$. Sia $G_n = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^n = 1\} = G_m = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^m = 1\}$. $\#G_m = m$ per il criterio della derivata, infatti $(x^m - 1, mx^{m-1}) = 1$. Sappiamo che il campo di spezzamente $\mathbb{F}_p(G_m)$ è un'estensione finita, quindi uguale a $\mathbb{F}_{p^d}$ per qualche d: ci chiediamo chi è d.

Lemma: $G_m = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^m = 1\} \leq \mathbb{F}_{p^d}^* = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^d-1} = 1\}$ se e solo se $m \mid p^d - 1$.

dim. ($\Rightarrow$) Per Lagrange $m = \#G_m | \#\mathbb{F}_{p^d}^* = p^d - 1$. ($\Leftarrow$) Sia $p^d - 1 = ml$. Allora per ogni $\alpha \in G_m$ si ha $\alpha^{p^d-1} = (\alpha^m)^l = 1^l = 1$, cioè $\alpha \in \mathbb{F}_{p^d}^*$.

Per il lemma, $d = \min\{k \mid m|p^k - 1\} = \min\{k \mid p^k \equiv 1 \pmod m\} = \text{ord}_{\mathbb{Z}/n\mathbb{Z}^*} p$.

3.4 Estensioni normali

Con "immersione" intenderemo sempre un omomorfismo di anelli (quindi anche di campi) iniettivo.
Notiamo primariamente che un omomorfismo di campi diverso dall'omomorfismo banale è necessariamente iniettivo (basta notare che gli unici ideali, quindi possibili nuclei dell'omomorfismo, (0) e il campo stesso). Da ora fino alla fine delle dispense escluderemo l'omomorfismo banale da tutti i ragionamenti, in modo che un omomorfismo di campi sia sempre un'immersione.
Proposizione - immersioni con estensioni semplici: Dato $\alpha \in \overline{K}$, le immersioni $\varphi : K(\alpha) \to \overline{K}$ tali che $\varphi|_K = id$ sono tante quante le radici distinte di $\mu_\alpha(x)$ in $\overline{K}$.

dim. Per il 1° teorema di omomorfismo costruire tale immersione equivale a costruire una $\tilde{\varphi} : K[x] \to \overline{K}$ tale che $(\mu_\alpha(x)) \subseteq \mathrm{Ker}(\tilde{\varphi})$. Notiamo ora che se $\tilde{\varphi}(x \mapsto \beta)$ allora $\tilde{\varphi}$ è l'omomorfismo di valutazione in β. Quindi, usando di nuovo che poiché $\varphi|_K = id$, $\varphi(\mu_\alpha(x)) = \mu_\alpha(\varphi(x))$, $\mu_\alpha(x) \in \mathrm{Ker}(\tilde{\varphi}) \Leftrightarrow \mu_\alpha(\beta) = 0$. Quindi gli omomorfismi che vanno bene sono tutti e soli quelli in cui β è una radice di $\mu_\alpha(x)$.

Proposizione - estensione a un'estensione semplice: Sia K un campo perfetto, $\alpha \in \overline{K}$, $[K(\alpha) : K] = n$. Allora ogni immersione $\varphi : K \hookrightarrow \overline{K}$ tale che $\varphi(K) \in \mathrm{Aut}(K)$ ammette n estensioni distinte $\varphi_1, \ldots, \varphi_n : K(\alpha) \hookrightarrow \overline{K}$ tali che $\varphi_i|_K = \varphi$.

dim. Lo abbiamo già visto nello Proposizione 1 nel caso di $\varphi = id$. Occorre solo generalizzare. Per il primo teorema di omomorfismo costruire tale immersione equivale a costruire una $\tilde{\varphi} : K[x] \to \overline{K}$ tale che $(\mu_\alpha(x)) \subseteq \mathrm{Ker}(\tilde{\varphi})$. Come sopra se $\tilde{\varphi}(x \mapsto \beta)$ allora $\tilde{\varphi}$ è l'omomorfismo di valutazione in β e quindi $\mu_\alpha(x) \in \mathrm{Ker}(\tilde{\varphi}) \Leftrightarrow \varphi\mu_\alpha(\beta) = 0.$, dove $\varphi\mu_\alpha$ è il polinomio i cui coefficienti sono le immagini secondo φ dei coefficienti di $\mu_\alpha(x)$. Usando che $\varphi(K) \cong K \Rightarrow \varphi K[x] \cong K[x] \Rightarrow \varphi$ preserva l'irriducibilità $\varphi\mu_\alpha(x)$ è irriducibile. Allora, essendo K perfetto, ha n radici distinte. Le possibili scelte per β sono quindi tutte e sole le n radici di $\varphi\mu_\alpha(x)$.

Proposizione - estensione a un'estensione finita: Sia E/K finita, con $[E : K] = n$. Allora ogni immersione $\varphi : K \hookrightarrow \overline{K}$ ammette n estensioni distinte a E.

dim. Notiamo intanto che E/K finita $\Rightarrow E/K$ algebrica $\Rightarrow E \subseteq \overline{K}$ e quindi sarà tutto ben definito. Procediamo per induzione su n. Il passo base $n = 1$ è ovvio.

Consideriamo ora $\alpha \in E \setminus K$. Allora $[K(\alpha) : K] = m \geq 1$, $[E : K(\alpha)] = d = \frac{n}{m}$ (per torri). Se $d = 1$ la tesi segue dalla proposizione precedente. Se invece $n > d > 1$ usiamo la proposizione precedente per costruire m estensioni di φ, $\varphi_1, \ldots, \varphi_m$ a $K(\alpha)$. Per ipotesi induttiva, ciascun $\varphi_i : K(\alpha) \to \overline{K}$ ammette esattamente d estensioni $\varphi_{i,1}, \ldots, \varphi_{i,d}$ a E tali che $\varphi_{i,j}|_K = \varphi_i|_K = \varphi|_K$. Allora le $\varphi_{i,j}$ così costruite sono le estensioni cercate e sono tutte distinte (se $i_1 \neq i_2$ $\varphi_{i_1,j_1} \neq \varphi_{i_2,j_2}$ perché basta guardare le restrizioni a $K(\alpha)$, che per la proposizione precedente sono distinte; se invece $j_1 \neq j_2$ allora $\varphi_{i,j_1} \neq \varphi_{i,j_2}$ per ipotesi induttiva).

Dimostriamo che non ve ne sono altre. Sia $\psi : E \to \overline{K}$ un'estensione di φ. Allora $\psi|_{K(\alpha)} : K(\alpha) \to \overline{K}$ e quindi per la proposizione precedente, essendo le φ_i le uniche estensioni deve valere $\psi|_{K(\alpha)} = \varphi_i$ per un qualche i. Ma allora ψ estende un φ_i e per ipotesi induttiva, essendo le $\varphi_{i,j}$ le uniche possibili estensioni, $\psi = \varphi_{i,j}$ per un qualche j. Questo conclude la dimostrazione.

Proposizione - generalizzazione: Il fatto che esista almeno un'estensione è vero per qualsiasi E/K algebrica. Non lo dimostriamo in questo corso.
Definizione - coniugati: Chiamiamo coniugati su K di $\alpha \in \overline{K}$ le radici di $\mu_\alpha(x) \in K[x]$ (polinomio minimo di α su K).

Proposizione - immersioni e coniugati: Data E/K algebrica e $\alpha \in E$, le immersioni $\varphi : E \to \overline{K}$ tali che $\varphi|_K = id$ mandano necessariamente α in un suo coniugato su K.

dim. Basta osservare che, poiché $\varphi|_K = id$, $\varphi(\mu_\alpha(x)) = \mu_\alpha(\varphi(x))$ e quindi, sostituendo $x = \alpha$, $0 = \mu_\alpha(\varphi(\alpha))$.

Definizione - estensione normale: F/K algebrica si dice normale se $\forall \varphi : F \to \overline{K}$ tale che $\varphi|_K = id$ si ha $\varphi(F) = F$.

Fatto: se $\mathrm{char}(K) \neq 2$ le estensioni di grado 2 sono normali.

dim. Sia F/K di grado 2 e $\alpha \in F \backslash K$. Allora $[K(\alpha) : K] = 2$ e $F = K(alpha)$. Sia quindi $p(x) = x^2 + ax + b$ il polinomio minimo di α su K. Allora i coniugati di α sono $\frac{-a \pm \sqrt{\Delta}}{2}$ e quindi $F = K(\alpha) = K(\sqrt{\Delta})$. I coniugati di $\sqrt{\Delta}$ sono $\pm\sqrt{\Delta}$, quindi da $\varphi|_K = id$ si ha $\varphi(K(\sqrt{\Delta})) = K(\pm\sqrt{\Delta}) = K(\sqrt{\Delta})$ come voluto.

Teorema - proprietà delle estensioni normali: Sia F/K algebrica. Sono equivalenti:

(i) F/K normale;

(ii) $\forall f \in K[x]$ irriducibile se f ha una radice in F allora ha tutte le radici in F;

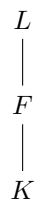
(iii) F è campo di spezzamento di una famiglia di polinomi.

dim. $(i) \Rightarrow (ii)$ Sia $f \in K[x]$ irriducibile, α una radice di f. Allora per irriducibilità $f(x) = u\mu_\alpha(x)$ con $u \in K^*$. Quindi senza perdita di generalità supponiamo $f(x) = \mu_\alpha(x)$. Siano $\alpha_1, \ldots, \alpha_n$ le radici di f. Consideriamo le n immersioni $\varphi_i : K(\alpha) \to F$ tali che $\varphi_i(\alpha) = \alpha_i$ e $\varphi_i|_K = id$ (esistono per le proposizioni precedenti). Dai fatti sopra dimostrati sappiamo che ciascuno di questi φ_i si estende a F (in realtà lo abbiamo dimostrato per estensioni finite); chiamiamo $\tilde{\varphi}_i$ l'estensione. Da F/K normale sappiamo $\tilde{\varphi}_i(F) = F \ \forall i = 1, \ldots, n$ e quindi $\tilde{\varphi}_i(\alpha) = \varphi_i(\alpha) = \alpha_i \in F$.

$(ii) \Rightarrow (iii)$ Consideriamo come famiglia di polinomi l'insieme dei polinomi minimi di tutti gli $\alpha \in F$. Sia F_0 il suo campo di spezzamento. Chiaramente $F \subseteq F_0$. Ma per l'ipotesi, (ii) poiché per costruzione ciascuno di questi polinomi ha almeno una radice in F, ciascuno di questi polinomi si fattorizza completamente in F, e quindi $F_0 \subseteq F$.

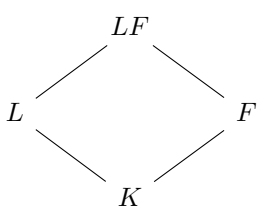
$(iii) \Rightarrow (i)$ Sia F campo di spezzamento di $\mathscr{F} = \{f_i(x) \mid i \in I\}$ con $f_i \in K[x]$ e Λ_i l'insieme contentente tutte le radici di f_i. Allora $F = K(\bigcup_{i \in I} \Lambda_i)$ e inoltre $\forall \varphi : F \to \overline{K}$ poiché le immersioni mandano coniugati in coniugati si ha $\forall i \in I \ \varphi(K(\Lambda_i)) = K(\Lambda_i)$ (φ agisce sulle radici permutandole, perché è iniettiva e fissa le radici di f_i) e quindi $\varphi(F) = \varphi(K(\bigcup_{i \in I} \Lambda_i)) = K(\bigcup_{i \in I} \Lambda_i) = F$.

Teorema - torri di estensioni normali: dato il diagramma a lato, vale L/K normale $\Rightarrow L/F$ normale.



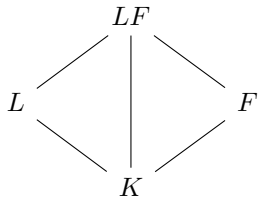
dim. L'algebricità di L/F segue dalle torri di estensioni algebriche. Sia $\varphi : L \to \overline{K}$ tale che $\varphi|_F = id$. Allora si ha $\varphi|_K = id$ perché $K \subseteq F$ e quindi per normalità di L/K si ha $\varphi(L) = L$, come voluto.

Teorema - shift di estensioni normali: dato il diagramma a lato, vale L/K normale e F/K algebrica $\Rightarrow LF/F$ normale.



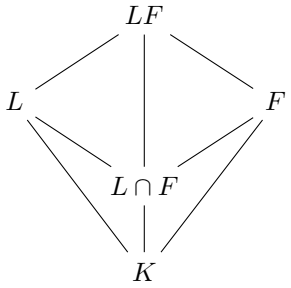
dim. L'algebricità di F/K serve per la buona definizione. L'algebricità di LF/F segue dallo shift di estensioni algebriche con L/K. Per la normalità, consideriamo $\varphi : LF \to \overline{K}$ tale che $\varphi|_F = id$. Allora si ha che $\varphi|_K = (\varphi|_F)|_K = id$. Consideriamo $\varphi|_L : L \to \overline{K}$. Vale $(\varphi|_L)|_K = id$ per quanto detto prima; allora per normalità di L/K, $\varphi(L) = \varphi|_L(L) = L$. Quindi, poiché $\varphi(F) = F$, $\varphi(LF) = LF$.

Teorema - composto di estensioni normali: dato il diagramma a lato, vale L/K normale e F/K normale $\Rightarrow$ LF/K normale.



dim. L'algebricità segue dal composto di estensioni algebriche. Per la normalità, consideriamo come prima $\varphi : LF \to \overline{K}$. Allora per normalità di L/K, $\varphi(L) = \varphi|_L(L) = L$. Analogamente $\varphi(F) = F$ e quindi $\varphi(LF) = LF$.

Teorema - implicazione di normalità: dato il diagramma a lato, vale L/K normale e F/K normale $\Rightarrow$ $(L \cap F)/K$ normale.



dim. L'algebricità è ovvia ($K \subseteq L \cap F \subseteq L$ e L/K algebrica $\Rightarrow$ $(L \cap F)/K$ algebrica). Per la normalità, consideriamo $\varphi : L \cap F \to \overline{K}$ tale che $\varphi|_K = id$. Poiché $LF/(L \cap F)$ è algebrica, φ può essere estesa a $\tilde{\varphi} : LF \to \overline{K}$. Allora, poiché L/K è normale, si ha $\tilde{\varphi}(L) = L$ e analogamente $\tilde{\varphi}(F) = F$. Quindi $\tilde{\varphi}(L \cap F) = \varphi(L \cap F) = L \cap F$.

3.5 Corrispondenza di Galois

Definizione - estensione separabile: L/K si dice separabile se $\forall \alpha \in L$ $\mu_\alpha(x)$ ha derivata non nulla. Osserviamo che ciò è certamente vero se il campo K è perfetto.

Definizione - estensione di Galois: L/K si dice di Galois se è normale e separabile. Osserviamo che se il campo K è finito o a caratteristica 0 (campi con cui lavoreremo per ora) per quanto detto allora "di Galois" e "normale" si equivalgono.

Definizione - gruppo di Galois: Se L/K è di Galois $Aut_K(L) = \{\varphi : L \to \overline{K} \mid \varphi|_K = id\}$ per quanto detto finora è un gruppo con la composizione. $Aut_K(L)$ si indica anche con $Gal(L/K)$ (gruppo di Galois di L su K). Inoltre se L/K è anche finita $\#Aut_K(L) = [L : K]$.

Teorema - Galoi di un campo di spezzamento: Sia $f \in K[x]$ irriducibile di grado n, e sia L il campo di spezzamento di f su K. Allora $n \mid [L : K] \mid n!$ e inoltre $Gal(L/K) \hookrightarrow S_n$.

dim. Sia $\alpha \in \overline{K}$ una radice di f. Allora per irriducibilità $f(x) = u\mu_\alpha(x)$ con $u \in K^*$. Poiché allora $K \subseteq K(\alpha) \subseteq L$ e $[K(\alpha) : K] = n$, si ha $n|[L : K]$ per torri.

Siano ora $\alpha_1, \ldots, \alpha_n$ le radici di f. Per quanto detto finora $\forall \varphi \in Gal(L/K)$ $\varphi(\{\alpha_1, \ldots, \alpha_n\}) = \{\alpha_1, \ldots, \alpha_n\}$ e quindi possiamo considerare l'azione di $Gal(L/K)$ su $\{\alpha_1, \ldots, \alpha_n\}$ data da $\varphi \mapsto \varphi_{\{\alpha_1,\ldots,\alpha_n\}}$. Questa mappa è chiaramente un omomorfismo iniettivo e quindi $Gal(L/K) \hookrightarrow S(\{\alpha_1, \ldots, \alpha_n\}) \cong S_n$, da cui segue $[L : K] = \#Gal(L/K) \mid \#S_n = n!$

Proposizione - irriducibilità e orbite: Sia $f \in K[x]$ di grado n, con radici $\alpha_1, \ldots, \alpha_n$ e sia L il campo di spezzamento di f su K. $Gal(L/K)$ agisce sulle radici di f per permutazione e l'azione è transitiva $\Leftrightarrow$ f è irriducibile.

dim. Consideriamo l'azione della dimostrazione precedente (è analoga anche se abbiamo tolto l'ipotesi di irriducibilità). In modo analogo a prima agisce per permutazione su {radici di $f(x)$}. Sappiamo poi dalle proposizioni dimostrate sopra che con questa azione $\text{orb}(\alpha) = \{\text{radici di } \mu_\alpha(x)\}$. Se α è radice di $f(x)$, allora si ha $\mu_\alpha \mid f$ e di conseguenza f irriducibile $\Leftrightarrow$ $f(x) = u\mu_\alpha(x)$ con $u \in K^*$ $\Leftrightarrow$ {radici di $f(x)$} = {radici di $\mu_\alpha(x)$} = $\text{orb}(\alpha)$ ovvero l'azione è transitiva.

Teorema - dell'elemento primitivo: Sia L/K finita e separabile. Allora L/K è semplice, ovvero $\exists \alpha \in L$ tale che $L = K(\alpha)$.

dim. Se K è un campo finito allora da L/K finita segue che anche L è un campo finito ($\#L = (\#K)^n$). È allora un fatto noto che $L^* = L \setminus \{0\}$ è ciclico (come gruppo moltiplicativo), e si ha la tesi.

Se K è infinito notiamo che L/K finita implica che è finitamente generata e quindi esistono $\alpha_1, \dots, \alpha_n$ tali che $L = K(\alpha_1, \dots, \alpha_n)$. Procediamo invece per induzione su n, trattando prima di tutto il caso $n = 2$ e poi passando al caso generale.

Sia $L = K(\alpha, \beta)$ e sia $d = [L : K]$. Allora per un teorema dimostrato precedentemente esistono esattamente d immersioni $\varphi_1, \dots, \varphi_d : L \to \overline{K}$ tali che $\varphi_i|_K = id$. Consideriamo $F(x) = \prod_{1 \le i < j \le d}((\varphi_i(\alpha) + x\varphi_i(\beta)) - (\varphi_j(\alpha) + x\varphi_j(\beta)))$. F è certamente non nullo perché prodotto di fattori non nulli: $(\varphi_i(\alpha) + x\varphi_i(\beta)) - (\varphi_j(\alpha) + x\varphi_j(\beta)) = 0 \Leftrightarrow \varphi_i(\alpha) + x\varphi_i(\beta) = \varphi_j(\alpha) + x\varphi_j(\beta) \Leftrightarrow \varphi_i(\alpha) = \varphi_j(\alpha)$ e $\varphi_i(\beta) = \varphi_j(\beta) \Leftrightarrow \varphi_i = \varphi_j$ ma vale sempre $i \neq j$.

Poiché il campo K è infinito, sicuramente esiste un $t \in K$ tale che $F(t) \neq 0$, e quindi i $\varphi_i(\alpha) + t\varphi_i(\beta)$ sono tutti distinti. Sia $\gamma = \alpha + t\beta \in L$ per questo fissato t. Per omomorfismo $\varphi_i(\gamma) = \varphi_i(\alpha) + t\varphi_i(\beta)$ e quindi si ha che $\varphi_1(\gamma), \dots, \varphi_n(\gamma)$ sono tutti distinti. Ciò implica che $[K(\gamma) : K] \ge d$ (sappiamo che il grado dell'estensione è il grado del polinomio minimo di γ su K e che le immagini di γ secondo questi omomorfismi sono radici di tale polinomio minimo; ne abbiamo trovate d distinte quindi il grado è almeno d). Ma da $K(\gamma) \subseteq L$ segue allora che $[K(\gamma) : K] = d$ e $L = K(\gamma)$.
A questo punto possiamo svolgere l'induzione. Per il passo base $n = 1$ la tesi è ovvia. Per il passo induttivo, notiamo che per ipotesi induttiva $L = K(\alpha_1, \dots, \alpha_n) = K(\beta, \alpha_n)$ e per quanto detto nel caso $n = 2$ esiste allora $\gamma \in L$ tale che $L = K(\beta, \alpha_n) = K(\gamma)$.

Definizione - campo fissato da un sottogruppo: Sia L/K di Galois, e $H \le Gal(L/K)$. Indichiamo con $L^H = Fix(H) = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$ il campo fissato da tutti gli elementi di H (è chiaramente un campo e poiché H è contenuto nel Galois si ha $K \subseteq L^H$).
Teorema - corrispondenza di Galois: Sia L/K di Galois finita. Allora c'è una corrispondenza tra i sottocampi di L che contengono K e i sottogruppi di $Gal(L/K)$, che associa il sottogruppo H al campo fissato L^H (e viceversa un campo al sottogruppo che lo fissa). Inoltre $H \lhd Gal(L/K) \Leftrightarrow L^H/K$ è normale e in tal caso $Gal(L^H/K) \cong \frac{Gal(L/K)}{Gal(L/L^H)}$.

dim. Sia $\mathscr{E} = \{F \text{ campo} \mid K \subseteq F \subseteq L\}$ e $\mathscr{G}_{L/K} = \{H \le Gal(L/K)\}$. Notiamo che per torri tutti i campi in $\mathscr{E}$ sono estensioni normali di K (tutto ben definito).

Definiamo $\alpha : \mathscr{E} \to \mathscr{G}$ $\alpha(F \mapsto Gal(L/F))$ e $\beta : \mathscr{G} \to \mathscr{E}$ $\beta(H \mapsto L^H)$.

Lemma 1: SIa $H \le Gal(L/K)$. Allora $M = L^H \Leftrightarrow H = Gal(L/M)$

dim. Sia M un campo con $K \subseteq M \subseteq L$. Per torri L/K di Galois $\Rightarrow L/M$ di Galois.
Sia $M = L^H$. Chiaramente $H \subseteq Gal(L/M)$. Allora per il teorema dell'elemento primitivo (stiamo lavorando con estensioni finite) si ha $L = M(\alpha)$ per un qualche $\alpha \in L$. Consideriamo $f(x) = \prod_{\sigma \in H}(x - \sigma(\alpha)) \in L[x]$. Notiamo che $\forall \rho \in H$, indicando di nuovo con ρf il polinomio applicando ρ ai coefficienti di f, si ha $\rho f(x) = \prod_{\sigma \in H}(x - \rho \circ \sigma(\alpha)) = \prod_{\tau \in H}(x - \tau(\alpha)) = f(x)$ e quindi $f(x) \in L^H[x] = M[x]$ (i suoi coefficienti restano invariati applicando $\rho \in H$). D'altra parte si ha $f(\alpha) = 0$ (basta prendere $\sigma = id$) e $\deg(f) = \#H$, da cui segue $\#Gal(L/M) = [L : M] = \deg(\mu_\alpha) \le \deg(f(x)) = \#H$. Quindi $\#Gal(L/M) = \#H$ (avevamo la disuguaglianza inversa per contenimento) e quindi $Gal(L/M) = H$.
Per l'altra freccia sia ora $H = Gal(L/M)$. $M \subseteq L^H$ segue dalle definizioni. Supponiamo ora per assurdo che $M \neq L^H$. Allora per teoria precedente $\exists \varphi : L^H \to \overline{M}$ tale che $\varphi \neq id$ ma $\varphi|_M = id$.

Possiamo estendere φ a L ottenendo $\tilde{\varphi} : L \to \overline{M}$ tale che di nuovo $\tilde{\varphi} \neq id$ ma $\tilde{\varphi}|_M = id$. Quindi $\tilde{\varphi} \in Gal(L/M) = H$. Allora per definizione $\tilde{\varphi}|_{L^H} = \varphi = id$ che è assurdo.

Usando il lemma appena dimostrato si ha da una parte $\alpha \circ \beta(H) = Gal(L/L^H) = H$ e quindi $\beta \circ \alpha = id$ e dall'altra $\beta \circ \alpha(F) = L^{Gal(L/F)} = F$ e quindi $\beta \circ \alpha = id$ (stiamo usando le due frecce della coimplicazione separatamente). Quindi α e β sono entrambe bigettive, e sono una l'inversa dell'altra.

Lemma 2: Sia $H \leq Gal(L/K)$, $\sigma \in Gal(L/K)$. Allora $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$.

dim. Basta notare che $\sigma(L^H) = \{\sigma(\alpha) \in L \mid \forall \varphi \in H \ \varphi(\alpha) = \alpha\} = \{\beta \in L \mid \forall \varphi \in H \ \varphi(\sigma^{-1}(\beta)) = \sigma^{-1}(\beta)\} = \{\beta \in L \mid \forall \varphi \in H \ \sigma \circ \varphi \circ \sigma^{-1}(\beta) = \beta\} = L^{\sigma H \sigma^{-1}}$.

Usando il lemma appena dimostrato si ha: $H \lhd Gal(L/K) \Leftrightarrow \forall \sigma \in Gal(L/K) \ \sigma H \sigma^{-1} = H$ Ma per il lemma 1 questo equivale a $\forall \sigma \in Gal(L/K) \ L^{\sigma H \sigma^{-1}} = L^H \Leftrightarrow \forall \sigma \in Gal(L/K) \ \sigma(L^H) = L^H \Leftrightarrow L^H/K$ è normale.

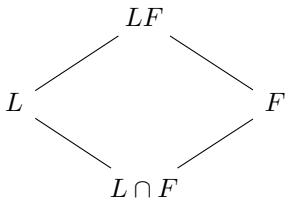
Infine mostriamo l'isomorfismo di gruppi. Sia $res : Gal(L/K) \to Gal(L^H/K)$ la restrizione a L^H. res è suriettivo perché L/K algebrica $\Rightarrow L/L^H$ algebrica e quindi ciascun omomorfismo in $Gal(L^H/K)$ si estende a uno in $Gal(L/K)$.
$\text{Ker}(res) = \{\sigma \in Gal(L/K) \mid \sigma|_{L^H} = id\} = Gal(L/L^H) = H$ per il lemma 1. Allora per il 1° teorema di omomorfismo si ha $Gal(L^H/K) \cong \frac{Gal(L/K)}{Gal(L/L^H)}$.

3.6 Gruppi di Galois in campi finiti

Teorema - campi finiti: TODO.

dim. TODO

3.7 Fatti sui gruppi di Galois



Teorema - del traslato: Sia $K = L \cap F$ e supponiamo LF/K di Galois. Allora LF/L è di Galois e $Gal(LF/L) \cong Gal(F/K)$.

dim. Consideriamo l'omomorfismo $res : Gal(LF/L) \to Gal(F/K)$ dato dalla restrizione a F. Esso è chiaramente un omomorfismo e $\text{Ker}(res) = \{\varphi \in Gal(LF/L) \mid \varphi|_F = id\}$. Ma $\forall \varphi \in Gal(LF/L) \varphi|_L = id$ per definizione e quindi $\varphi \in \text{Ker}(res) \Leftrightarrow \varphi|_L F = id \Leftrightarrow \varphi = id$ essendo LF il dominio di φ.
Per dimostrare la suriettività sia $I = Imm(res)$. Il suo campo fissato è $F^I = \{\alpha \in F \mid \forall \sigma \in I \sigma(\alpha) = \alpha\} = \{\alpha \in F \mid \forall \varphi \in Gal(LF/L) \varphi|_F(\alpha) = \alpha\} = F \cap \{\alpha \in LF \mid \forall \varphi \in Gal(LF/L) \varphi(\alpha) = \alpha\} = F \cap L = K$. Allora per corrispondenza di Galois $Imm(res) = I = Gal(F/K)$.

Corollario - moltiplicatività del composto: Sia come prima $K = L \cap F$, LF/K di Galois e supponiamo F/K di Galois. Allora $[LF : K] = [F : K][L : K]$.

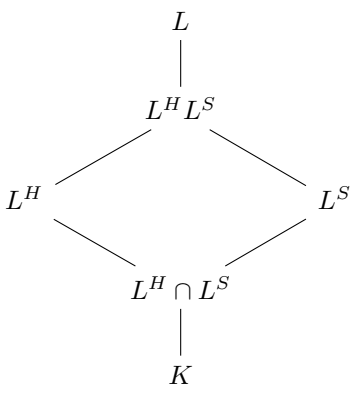
dim. Per il teorema, $Gal(LF/L) \cong Gal(F/K) \Rightarrow [LF : L] = [F : K]$. Ma per torri si ha allora $[LF : L] = [LF : L][L : K] = [F : K][L : K]$.

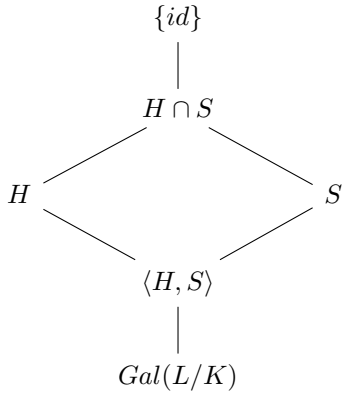
Teorema - campi fissati e operazioni: Sia L/K di Galois finita, e $H, S \leq Gal(L/K)$. Allora valgono le seguenti:

(*i*) $L^H \subseteq L^S \Leftrightarrow H \supseteq S$

(*ii*) $L^{H\cap S} = L^H L^S$

(*iii*) $L^{\langle H,S\rangle} = L^H \cap L^S$





dim. Per (*i*) basta notare che $H \supseteq S \Rightarrow L^H \subseteq L^S$ segue direttamente dalla definizione, mentre sempre per definizione $L^H \subseteq L^S \Rightarrow Gal(L/L^H) \supseteq Gal(L/L^S)$ e per uno dei lemmi visti a lezione $H = Gal(L/L^H), S = Gal(L/L^S)$.
Per (*ii*) notiamo intanto che per (*i*) $L^H \subseteq L^{H\cap S}$ e analogamente L^S, quindi $L^H L^S \subseteq L^{H\cap S}$. Per corrispondenza di Galois $L^H L^S = L^N$ per $N = Gal(L/L^H L^S)$. Ma allora $N = Gal(L/L^H) \cap Gal(L/L^S) = H \cap S$. Infatti si ha $Gal(L/L^H L^S) = \{\varphi : L \to \overline{K} \mid \varphi \text{ omomorfismo e } \varphi_{L^H L^S} = id\} = \{\varphi : L \to \overline{K} \mid \varphi \text{ omomorfismo e } \varphi_{L^H} = id, \varphi_{L^H} = id\} = Gal(L/L^H) \cap Gal(L/L^S)$.
Per (*iii*) come prima notiamo intanto che per (*i*) $L^H \supseteq L^{\langle H,S\rangle}$ e analogamente L^S. Quindi $L^H \cap L^S \supseteq L^{\langle H,S\rangle}$. Notiamo ora che $\alpha \in L^H \cap L^S \Rightarrow \forall\ \ni \in H, \psi \in S,\ \ni(\alpha) = \alpha = \psi(\alpha) \Rightarrow \forall \varphi \in \langle H, S\rangle,\ \varphi(\alpha) = \alpha \Rightarrow \alpha \in L^{\langle H,S\rangle}$ quindi $L^H \cap L^S \subseteq L^{\langle H,S\rangle}$.

Idea - come trovare i campi fissati
Teorema - estensioni con radici quadrate: Sia $\mathrm{char}(K) \neq 2$. Allora dati $\alpha, \beta \in K$, $K(\sqrt{\alpha}) = K(\sqrt{\beta}) \Leftrightarrow \alpha\beta$ è un quadrato in $K \Leftrightarrow \frac{\alpha}{\beta}$ è un quadrato in K

dim. $\alpha\beta$ è un quadrato in $K \Leftrightarrow \frac{\alpha}{\beta}$ è un quadrato in K è ovvia (basta moltiplicare/dividere per β^2).
$K(\sqrt{\alpha}) = K(\sqrt{\beta}) \Leftrightarrow \exists x, y \in K \sqrt{\alpha} = x + \sqrt{\beta} y$. Se $x = 0$ si ha $\sqrt{\frac{\alpha}{\beta}} \in K$ e la tesi ovva. Se $y = 0$ si ha $\sqrt{\alpha} \in K$, e allora $\alpha\beta$ è un quadrato in $K \Leftrightarrow \beta$ è un quadrato in K e quindi $\Leftrightarrow K(\beta) = K = K(\alpha)$. Altrimenti elevando al quadrato $\alpha = x^2 + \beta y^2 + 2xy\alpha\beta \Leftrightarrow \sqrt{\alpha\beta} = \frac{\alpha - x^2 - \beta y^2}{2xy} \in K \Leftrightarrow \frac{\alpha}{\beta}$ è un quadrato in K.

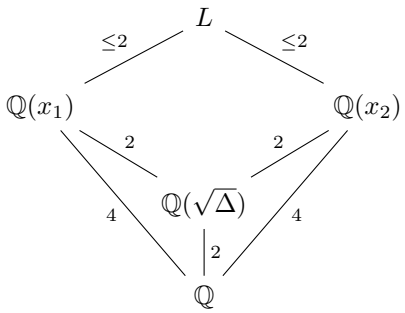
Teorema - Galois di una biquadratica: Il Galois del campo di spezzamento su $\mathbb{Q}$ di $x^4 + ax^2 + b \in \mathbb{Q}[x]$ irriducibile può avere tre strutture ($\Delta = a^2 - 4b$):

- D_4, se né b né $b\Delta$ sono quadrati in $\mathbb{Q}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, se né b è un quadrato in $\mathbb{Q}$
- $\mathbb{Z}/4\mathbb{Z}$, se $b\Delta$ è un quadrato in $\mathbb{Q}$

dim. Sia L il campo di spezzamento e $G = Gal(L/\mathbb{Q})$. Notiamo intanto che per la teoria vista $G \hookrightarrow S_4$. Scriviamo intanto le soluzioni per $t = x^2$, usando la formula risolutiva per le equazioni di secondo grado: $t_\pm = \frac{-a \pm \sqrt{\Delta}}{2}$. Siano poi $x_1 = \sqrt{\frac{-a+\sqrt{\Delta}}{2}}, x_2 = \sqrt{\frac{-a-\sqrt{\Delta}}{2}}, x_3 = -x_1, x_4 = -x_3$ le radici della biquadratica.

Si ha $L = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(x_1, x_3)$.

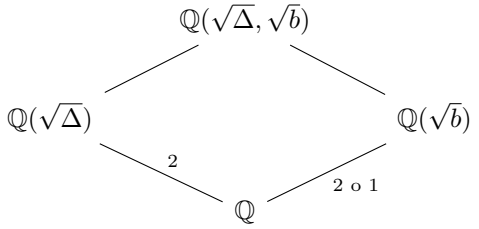
Consideriamo il diagramma di campi a lato. Notiamo che $t_+ \in \mathbb{Q}(x_1)$ e quindi $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(x_1)$. Analogamente $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(x_2)$. $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$ perché se fosse 1 allora il polinomio si spezzerebbe in due fattori. $[\mathbb{Q}(x_1) : \mathbb{Q}] = [\mathbb{Q}(x_2) : \mathbb{Q}] = 4$ perché il polinomio è irriducibile. Allora per torri $[\mathbb{Q}(x_1) : \mathbb{Q}(\sqrt{\Delta})] = 2$ e per shift ciò implica $[L : \mathbb{Q}(x_2)] \leq 2 \Rightarrow [L : \mathbb{Q}] = 4$ o 8.



Notiamo che $[L : \mathbb{Q}] = 4 \Leftrightarrow \mathbb{Q}(x_1) = \mathbb{Q}(x_2) \Leftrightarrow x_1 x_2 \in \mathbb{Q}(x_1) \Leftrightarrow x_1 x_2 \in \mathbb{Q}(x_1) \cap \mathbb{Q}(x_2) = \mathbb{Q}(\sqrt{\Delta})$. Ma $x_1 x_2 = \sqrt{b}$ (il termine noto del polinomio è il prodotto delle radici).

Studiamo quindi quest'altro diagramma. Per quanto detto finora $[L : \mathbb{Q}] = 4 \Leftrightarrow [\mathbb{Q}(\sqrt{\Delta}, \sqrt{b}) : \mathbb{Q}] = 2$. Ma allora, poiché $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$ per torri $[\mathbb{Q}(\sqrt{\Delta}, \sqrt{b}) : \mathbb{Q}(\sqrt{\Delta})] = 1$, che si verifica quando

- b è quadrato in $\mathbb{Q} \Rightarrow [\mathbb{Q}(\sqrt{b}) : \mathbb{Q}] = 1$
- b non è un quadrato in $\mathbb{Q}$ e allora $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{b}) \Leftrightarrow b\Delta$ è quadrato



Studiamo le strutture dei gruppi nei due casi. Gli unici strutture possibili di un gruppo di ordine 4 sono $\mathbb{Z}/4\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Una caratteristica che li distingue certamente è la presenza o meno di un elemento di ordine 4 (e se ce ne è 1 , allora ce ne sono 2). Chiamiamo i 4 elementi del Galois $f\_i \in G$ tali che $f(x_1) = x_i$ per $i = 1, 2, 3, 4$ (sono questi perché per irriducibilità il Galois agisce transitivamente su $\{x_1, x_2, x_3, x_4\}$). È chiaro che $f_1 = id$ e f_3 ha ordine 2. Studiamo l'ordine di f_2. $f_2^2(x_1) = f_2(x_2) = f_2(\frac{\sqrt{b}}{x_1}) = \frac{f_2(\sqrt{b})}{x_2}$.

- Se b è un quadrato in $\mathbb{Q}$, allora $\frac{f_2(\sqrt{b})}{x_2} = \frac{\sqrt{b}}{x_2} = x_1$ e quindi f_2 ha ordine 2, da cui segue che $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- Se invece b non è un quadrato in $\mathbb{Q}$ allora esiste $c \in \mathbb{Q}$ tale che $\sqrt{b} = \frac{c}{\sqrt{\Delta}}$ per quanto detto. Allora $\frac{f_2(\sqrt{b})}{x_2} = \frac{c}{f_2(\sqrt{\Delta})x_2}$. Notando che $\sqrt{\Delta} = 2x_1^2 + a = -(2x_2^2 + a)$ si ha $f_2(\sqrt{\Delta}) = 2f_2(x_1)^2 + a = 2x_2^2 + a = -\sqrt{\Delta}$, e quindi $f_2^2(x_1) = -x_1 = x_3$, e f_2 ha ordine 4, da cui segue $G \cong \mathbb{Z}/4\mathbb{Z}$.

Nel caso in cui $[L : \mathbb{Q}] = 8$ invece, dal fatto che $G \hookrightarrow S_4$ si ha che G è un 2-Sylow di S_4, che si dimostra essere isomorfo a D_4.

Teorema - Galois delle radici dell'unità: Sia $\zeta_n = e^{\frac{i\pi}{n}}$ una radice n-esima dell'unità. Allora $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è di Galois e $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

dim. Notiamo intanto che $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è di Galois perché è campo di spezzamento di $x^n - 1$, essendo le radici di questo polinomio tutte le ζ_n^k con $k = 1, \ldots, n$. Consideriamo ora la funzione $\Phi : Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ tale che, se $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ manda $\zeta_n \mapsto \zeta_n^k$ allora $\Phi(\sigma) = k$.

Notiamo che un tale k esiste sempre perché per la teoria vista a lezione agisce sulle radici di $x^n - 1$, ovvero le potenze di ζ_n, permutandole, e quindi ζ_n sarà mandato in un certo ζ_n^k. Inoltre poiché si tratta di radici n-esime dell'unità, l'esponente viene definito in modo naturale ($\mod n$). Per dire che $k \in (\mathbb{Z}/n\mathbb{Z})^*$ e non solo $\mathbb{Z}/n\mathbb{Z}$, notiamo che $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ in quanto omomorfismo iniettivo deve preservare gli ordini

degli elementi e quindi $\text{ord}(\zeta_n^k) = \text{ord}(\zeta_n) = n$, che si verifica $\Leftrightarrow MCD(k,n) = 1 \Leftrightarrow k \in (\mathbb{Z}/n\mathbb{Z})^*$. Quindi Φ è ben definita. Φ è un omomorfismo perché, se $\sigma_1(\zeta_n \mapsto \zeta_n^{k_1})$ e $\sigma_2(\zeta_n \mapsto \zeta_n^{k_2})$ allora $\sigma_2 \circ \sigma_1(\zeta_n \mapsto (\zeta_n^{k_1})^{k_2} = \zeta_n^{k_1 k_2})$ e quindi $\Phi(\sigma_2 \circ \sigma_1) = k_1 k_2 = \Phi(\sigma_1)\Phi(\sigma_2)$.

Inoltre Φ è chiaramente iniettiva perché due omomorfismi del Galois sono diversi tra loro se e solo se è diversa l'immagine di ζ_n. Vorremmo ora mostrare che Φ è suriettiva, e quindi un isomorfismo, che è vero $\Leftrightarrow \varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = \#[Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#\text{coniugati di } \zeta_n$.

Lemma Fissiamo p primo che non divide n e $j \in \mathbb{Z}/p\mathbb{Z}$. Allora ζ_n^j e ζ_n^{pj} sono coniugate.

dim. Sia $f(x)$ il polinomio minimo di ζ_n^j. Se ζ_n^{pj} non è coniugato di ζ_n^j allora non è radice di $f(x)$. Sia allora $g(x) \neq f(x)$ il suo polinomio minimo. Per irriducibilità $MCD(f(x), g(x)) = 1$ e quindi vale anche $f(x)g(x) \mid x^n - 1$, essendo ζ_n^j, ζ_n^{pj} delle radici di $x^n - 1$. Ma ζ_n^{pj} radice di $g(x) \Rightarrow \zeta_n^j$ radice di $g(x^p)$ e quindi $f(x) \mid g(x^p)$. Notiamo ora che $f(x), g(x) \in \mathbb{Z}[x]$. Infatti, possiamo scrivere $f(x) = uf_1(x)$ con $u \in \mathbb{Z}$ e $f_1(x) \in \mathbb{Z}$ primitivo (basta prendere $u = mcm\{\text{denominatori dei coefficienti di } f\}$), notare che $f(x) \mid x^n - 1 \Rightarrow f_1(x) \mid x^n - 1$ (divisibilità tutte intese in $\mathbb{Q}$) $\Rightarrow$ per il lemma di Gauss $\exists q(x) \in \mathbb{Z}$ tale che $x^n - 1 = f_1(x)q(x) = uf(x)q(x)$ da cui si ricava, guardando i coefficienti di testa ($f(x)$ è monico per definizione) $u = \pm 1$. Si procede in modo analogo per g. Allora $f(x), g(x^p)$ sono polinomi a coefficienti interi primitivi e quindi per il lemma di Gauss $f(x) \mid g(x^p)$ in $\mathbb{Q} \Rightarrow \exists h(x) \in \mathbb{Z}[x]$ tale che $g(x^p) = f(x)h(x)$. Proiettiamo ora questa equazione in $\mathbb{F}_p$. Usando l'isomorfismo di Fröbenius abbiamo $g(x)^p = g(x^p) = f(x)h(x)$. Quindi in $\mathbb{F}_p$ tutte le radici di f sono anche radici di g. Ma $f(x)g(x) \mid x^n - 1$ anche in $\mathbb{F}_p$ e allora $x^n - 1$ dovrebbe avere radici doppie, assurdo perché allora per il criterio della derivata $MCD(x^n - 1, nx^{n-1}) = 0$ ma $MCD(x^n - 1, nx^{n-1}) = 1$ (usando che $p \nmid n$). Questo conclude la dimostrazione che ζ_n^{pj} è coniugato di ζ_n^j se $p \nmid n$.

Allora $\forall k = \prod_{j=1}^s p_j^{\alpha_j}$ coprimo con n si ha che ζ_n e ζ_n^k sono coniugate, e ciò lo si dimostra per induzione sulla somma degli esponenti. Infatti, il passo base con $k = 1$ è ovvio mentre applicando il lemma con $j = \prod_{j=1}^{s-1} p_j^{\alpha_j} \cdot p_s^{\alpha_s - 1}$ si ha che ζ_n^j e $\zeta_n^{p_s j} = \zeta_n^k$ sono coniugate, che unito all'ipotesi induttiva che ζ_n e ζ_n^j sono coniugate implica la tesi.

Questo dimostra che ζ_n ha almeno $\varphi(n)$ coniugati, e quindi $\deg(f) \geq \varphi(n)$. L'iniettività ci dava la disuguaglianza inversa, e quindi abbiamo $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(f) = \varphi(n)$, ovvero Φ descritta sopra è un isomorfismo, come voluto.

Teorema - Galois con radici di primi: TODO

Teorema - $\sqrt{\pm p} \in \mathbb{Q}(\zeta_p)$: Se p è un primo diverso da 2, allora $\sqrt{\pm p} \in \mathbb{Q}(\zeta_p)$, dove il segno $\pm$ dipende da p modulo 4: è $-$ se $p \equiv 3 \pmod 4$, $+$ se $p \equiv 1 \pmod 4$.
Nota: teorema non visto a lezione.

dim. TODO
seconda dim (non fatta a lezione, ma mi andava di aggiungerla). Se il lettore ha seguito/sta seguendo il corso di Analisi numerica si sarà imbattuto nella matrice di Fourier (un tipo particolare di matrice di Vandermonde). Dati $(x_1.x_2, \ldots, x_n)$ definiamo la Vandermonde (quadrata) con:

$$V(x_0, x_1, x_2, \ldots, x_m) = \begin{bmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \ldots & x_{n-1}^{n-1} \end{bmatrix}$$

E quella di Fourier con (detta ζ_n la radice n-esima dell'unità): $\Omega_n = V(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1})$ Si richiamano alcune proprietà, seguendo le definizioni date sopra:

- $\det(V) = \prod_{1 \le i < j \le n} (x_j - x_i)$
- $\Omega_n^2 = n \cdot \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \end{bmatrix} \quad \Rightarrow \quad \det(\Omega_n)^2 = n^n \cdot (-1)^{\frac{n(n+1)}{2}-1}$

Se sostituisco n con $p \ge 3$ primo, usando $\Omega_n = V(1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1})$ e quindi

$$\sqrt{p^p \cdot (-1)^{\frac{p(p+1)}{2}-1}} = \det(\Omega_n) = \prod_{1 \le i < j \le n} (\zeta_p^j - \zeta_p^i)$$

Il lato destro dell'equazione, essendo ottenuto da ζ_p con somme e prodotti, ci dice che $\sqrt{p^p \cdot (-1)^{\frac{p(p+1)}{2}-1}} \in \mathbb{Q}(\zeta_p)$. Ma poiché p dispari p^p è un intero moltiplicato per $\sqrt{p}$. Quindi $\sqrt{\pm p} \in \mathbb{Q}(\zeta_p)$. Il segno $\pm$ è dato da $\frac{p(p+1)}{2} - 1$ e basta quindi fare i casi: si vede che è uguale a -1 se $p \equiv 3 \pmod 4$, 1 se $p \equiv 1 \pmod 4$.

3.8 Teorema fondamentale dell'algebra

$\mathbb{C}$ è algebricamente chiuso.

dim. Sia $f(x) \in \mathbb{C}[x]$. Notiamo che $g(x) = f(x)\overline{f(x)} \in \mathbb{R}[x]$. Dimostriamo che il suo campo di spezzamento, che chiamiamo K, è $\mathbb{R}$ o $\mathbb{C}$, visto che $f(x)$ e $\overline{f(x)}$ hanno le radici coniugate e quindi i campi di spezzamento di f e g coincidono.

$$\begin{array}{c} K \\ | \\ K^{P_2} = \mathbb{R}(\alpha) \\ |_{d=1} \\ \mathbb{R} \end{array}$$

Sia $G = Gal(K/\mathbb{R})$ (gruppo finito perché K è campo di spezzamento di un unico polinomio) e sia P_2 un suo 2-Sylow. Allora $d = [G : P_2]$ è un dispari. Per corrispondenza di Galois K^{P_2} è un'estensione di $\mathbb{R}$ di grado d. Per il teorema dell'elemento primitivo essa è semplice, ossia $K^{P_2} = \mathbb{R}(\alpha)$ per un qualche $\alpha \in K$.

Detto $\mu(x) \in \mathbb{R}[x]$ il polinomio minimo di α, si ha $\deg(\mu(x)) = d$ dispari e quindi per il teorema dei valori intermedi $\mu(x)$ ha almeno una radice in $\mathbb{R}$. Ma allora, poiché $\mu(x)$ è irriducibile, deve valere per forza $d = 1$.

Quindi $\#G = 2^n$ per un qualche $n \in \mathbb{N}$ e allora per Sylow esiste una catena di sottogruppi $\{id\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$ tale che ciascun gruppo ha indice 2 nel successivo. Per corrispondenza di Galois esiste allora una catena di campi $K = K_0 \supset K_1 \supset \cdots \supset K_n = \mathbb{R}$ tale che ciascuna estensione ha grado 2 sulla successiva. Ma l'unica estensione di grado 2 di $\mathbb{R}$ è $\mathbb{C}$, e $\mathbb{C}$ non ha estensioni di grado 2. Quindi l'unica possibilità è $K = \mathbb{R}$ o $\mathbb{C}$ come voluto.

3.9 Esercizi

Esercizio: Si contino i polinomi monici irriducibili di grado 10 in $\mathbb{F}_p[x]$.

Soluzione: Lavoriamo in una chiusura algebrica $\overline{\mathbb{F}_p}$. Sia $f(x) \in \mathbb{F}_p[x]$ irriducibile di grado n di radici $\alpha_1, \ldots, \alpha_n$, allora $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha_i) \cong \frac{\mathbb{F}_p[x]}{(f(x))}$ per unicità di $\mathbb{F}_{p^{10}}$ in $\overline{\mathbb{F}_p}$. Identifichiamo ogni polinomio monico irriducibile con l'insieme delle sue 10 radici: per polinomi irriducibili distinti questi insiemi non si intersecano. $[\mathbb{F}_{p^{10}} : \mathbb{F}_p] = 10$, dunque ogni elemento $\alpha \in \mathbb{F}_{p^{10}}$ ha polinomio minimo di grado al più 10. Se $\deg \mu_\alpha(x) = d$, allora $\mathbb{F}_{p^d} = \mathbb{F}(\alpha) \subseteq \mathbb{F}_{p^{10}}$. Ma sappiamo che $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m|n$, dunque i possibili d sono 1,2,5,10. Gli elementi con polinomio minimo di grado 1 o 2 sono tutti e soli gli elementi di $\mathbb{F}_{p^2}$, così come gli elementi con polinomio minimo di grado 1 o 5 sono tutti e soli gli elementi d $\mathbb{F}_{p^5}$. Per il principio di inclusione-esclusione esistono $p^{10} - p^5 - p^2 + p$ elementi con polinomio minimo di grado 10, che corrispondono a $\frac{p^{10}-p^5-p^2+p}{10}$ polinomi monici irriducibili di grado 10.

Esercizio: Determinare il campo di spezzamento di $f_7(x) = x^7 - 1$ su $\mathbb{F}_5$ e su $\mathbb{F}_{11}$.

Soluzione: Si tratta di applicare il teorema sul cds di $x^n - 1$ su $\mathbb{F}_p$. $\#(\mathbb{Z}/7\mathbb{Z}^*) = 6$, dunque $d_5 = \mathrm{ord}_{\mathbb{Z}/7\mathbb{Z}^*} 5$ e $d_{11} = \mathrm{ord}_{\mathbb{Z}/7\mathbb{Z}^*} 11$ sono entrambi divisori di 6.

Si trova $d_5 = 6$ e $d_{11} = 3$, dunque il cds di $x^7 - 1$ su $\mathbb{F}_5$ e su $\mathbb{F}_{11}$ sono rispettivamente $\mathbb{F}_{5^6}$ e $\mathbb{F}_{11^3}$.

Esercizio: Determinare la forma della fattorizzazione di di $x^8 - 1$ su $\mathbb{F}_p$.

Soluzione: Se $p = 2$, allora $x^8 - 1 = (x-1)^8$. Assumiamo ora $p \neq 2$, quindi $(8, p) = 1$. Per quanto visto il campo di spezzamento di $x^8 - 1$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$ con $d = \mathrm{ord}_{\mathbb{Z}/8\mathbb{Z}^*} p$. Ricordiamo $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, dunque $d \in \{1, 2\}$. Ma allora $x^8 - 1$ si spezza come prodotto di fattori di grado uno e due su ogni $\mathbb{F}_p$ e c'è almeno un fattore di grado due se e solo se $d = 2$. Indipendentemente dal campo, $x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1) \ldots$ quindi $x^4 + 1$ è un irriducibile di $\mathbb{Z}[x]$ che per ogni p *non* è irriducibile su $\mathbb{F}_p$!

Da aritmetica sappiamo che dato $f(x) \in \mathbb{Z}[x]$, se, detta $\bar{f}(x)$ la proiezione di f modulo p, $\bar{f}(x)$ è irriducibile su $\mathbb{F}_p[x]$, allora f è irriducibile su $\mathbb{Z}[x]$. L'esercizio ci dice che non vale l'implicazione inversa, cioè esistono irriducibili di $\mathbb{Z}[x]$ che per ogni p sono riducibili su $\mathbb{F}_p[x]$ e $x^4 + 1$ è uno di questi.