Algebra I

Alberto Andrenucci

29 novembre 2017

Nozioni fondamentali su gruppi, azioni e automorfismi.

Definizione 1 (Automorfismi)**.** *G gruppo, definiamo $Aut(G) = \{f : G \to G \text{ isomorfismi}\}$. $(Aut(G), \circ)$ è un gruppo con la composizione.*

- $id_G \in Aut(G)$;
- $\forall \varphi, \psi \in Aut(G) \implies \varphi \circ \psi \in Aut(G)$
- $\forall \varphi \in Aut(G), \varphi \circ id_G = id_G \circ \varphi = \varphi$
- $\forall \varphi \in Aut(G), \varphi^{-1} \in Aut(G)$

Quali sono gli automorfismi di $\mathbb{Z}$? Dimostriamo che $Aut(\mathbb{Z}) = \{\pm id\}$. Essendo $\mathbb{Z}$ un gruppo ciclico, basta decidere dove mandare l'elemento 1.

$\varphi_a : \mathbb{Z} \to \mathbb{Z} \quad | \quad \varphi_a(1) = a \quad \varphi_a(n) = na$

Questi sono endomorfismi, quali sono bigettivi?

Surgettività: $\varphi_a(\mathbb{Z}) = a\mathbb{Z} \implies a\mathbb{Z} = \mathbb{Z} \iff a = \pm 1$;

Iniettività: $\varphi_1 = id; \varphi_{-1} = -id$ sono iniettivi.

Proposizione 1. *$Aut(\mathbb{Z}n) \cong (\mathbb{Z}n)^*$*

Dimostrazione. Sia $\varphi_a : \mathbb{Z}n \to \mathbb{Z}n \quad | \quad \varphi_a(\overline{1}) = \overline{a}$. Poiché si tratta di un omomorfismo si deve avere che $o(\overline{a})|o(\overline{1}) = n$. φ_a iniettiva $\iff o(\overline{a}) = o(\overline{1}) = n$ e dunque ci sono $\Phi(n)$ possibili valori per $\overline{a}$ ($\overline{a} \in (\mathbb{Z}n)^*$).

$\Phi : (\mathbb{Z}n)^* \to Aut(\mathbb{Z}n) \quad | \quad \Phi(\overline{a}) = \overline{\varphi_a}$

Si verifica facilmente che è ben definito questo omomorfismo e che è surgettivo, verifichiamo l'iniettività: $\Phi(\overline{a}) = \Phi(\overline{b}) \iff \varphi_a = \varphi_b \iff \overline{a} = \overline{b}$

□

Esercizio 1. *Trovare $Aut(\mathbb{Q})$ e $Aut(\mathbb{R})$.*

Definizione 2 (Automorfismo Interno)**.** *$g \in G, \quad \varphi_g : G \to G \quad | \quad \varphi(x) = gxg^{-1}$ si chiama coniugio o automorfismo interno. $Int(G) = \{\varphi_g | g \in G\}$*

Osservazione 1. *$\varphi_g \in Aut(G)$.*

- *φ_g ben definito;*
- *φ_g omomorfismo bigettivo:*
  - *Omomorfismo:* $\forall x, y \in G \quad \varphi_g(x)\varphi_g(y) = (gxg^{-1})(gyg^{-1}) = gxyg^{-1} = \varphi_g(xy)$;
  - *Iniettivo:* $\mathrm{Ker}(\varphi_g) = \{x|\varphi_g(x) = e\} = \{x|gxg^{-1} = e\} = \{x|gx = g\} = \{e\}$
  - *Surgettivo:* $\forall y \in G \quad x = g^{-1}yg \mapsto y$

Proposizione 2. *$Int(G) \triangleleft Aut(G)$; $Int(G) \cong G/Z(G)$.*

Dimostrazione. 1) $\varphi_e \in Int(G), \ \varphi_e = id$;
$\forall \varphi_g, \varphi_h \in Int(G), \ \varphi_g \circ \varphi_h = \varphi_{gh}$;
$\forall \varphi_g \in Int(G) \implies (\varphi_g)^{-1} = \varphi_{g^{-1}} \implies Int(G) < Aut(G)$
$\forall f \in Aut(G), \ \forall \varphi_g \in Int(G), \ \underbrace{f \circ \varphi_g \circ f^{-1}}_{\varphi_{f(g)}} \in Int(G)$;

Verifica: $f \circ \varphi_g \circ f^{-1}(x) = f(\varphi_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) = f(g)xf(g^{-1}) = f(g)x(f(g))^{-1} = \varphi_{f(g)}(x) \implies Int(G) \triangleleft Aut(G)$.

2) Nel caso di gruppi abeliani sono entrambi l'identità, $Int(G) \cong G/G = e$.
$\Phi : G \mapsto Int(G) \quad | \quad \Phi(g) = \varphi_g$, abbiamo già visto che Φ è un omomorfismo surgettivo. $\mathrm{Ker}(\Phi) = \{g|\varphi_g = id\}$. $\forall x \in G, \ gxg^{-1} = x \iff gx = xg \implies \mathrm{Ker}(\Phi) = \{g|\varphi_g = id\} = Z(G)$. Dal primo teorema di omomorfismo segue l'isomorfismo che cercavamo. □

Osservazione 2. *$H < G, \ H \triangleleft G \iff \varphi_g H = H \ \ \forall \varphi_g \in Int(G)$, ovvero i sottogruppi normali di G sono i sottogruppi invarianti per automorfismi interni di G.*

Definizione 3 (Caratteristico)**.** *$H < G$ si dice caratteristico se è invariante per $Aut(G)$ ovvero se $\forall f \in Aut(G), \ f(H) = H$.*

Osservazione 3. *Caratteristico $\implies$ normale, ma il viceversa è falso.*

Esempio 1. *$\mathbb{Z}2 \times \mathbb{Z}2$ ha 3 sottogruppi di ordine 2. $\langle 1, 0\rangle$ non è caratteristico ma è normale.*

Definizione 4 (Azione di un gruppo su un insieme)**.** *Sia G un gruppo e sia X un insieme. Un'azione di G su X è un omomorfismo $\varphi : G \mapsto S(X) = \{f : X \mapsto X | f \ bigettiva\}$ | $\varphi(g) = \varphi_g (che \ ad \ x \mapsto \varphi_g(x) = gx)$.*

Osservazione 4. *Un'azione φ definisce su X una relazione di equivalenza: $x \sim y \iff \exists g \in G | x = gy (= \varphi_g(y))$.*

Definizione 5 (Orbita)**.** *La classe di equivalenza di x secondo quest'azione si dice orbita di x: $orb(x) = \{gx | g \in G\}$.*

$$X = \overset{\circ}{\bigcup_{x \in R}} orb(x) \qquad \text{dove R è un insieme di rappresentanti delle orbite}$$

$$\text{Se } |X| < \infty \implies |X| = \sum_{x \in R} |orb(x)|.$$

Definizione 6 (Stabilizzatore)**.** *$\forall x \in X$ si dice stabilizzatore di x $St(x) = \{g \in G | gx = x\}$*

Notiamo che $St(x) < G$ ma in generale non è normale.

$gx = hx \iff h^{-1}gx = x$; $\varphi_g(x) = \varphi_h(x) \iff \varphi_h^{-1}\varphi_g(x) = \varphi_{h^{-1}}\varphi_g(x) \iff \varphi_{h^{-1}g}(x) = x \iff h^{-1}gx = x \iff h^{-1}g \in St(x) \iff g \in hSt(x) \iff gSt(x) = hSt(x)$ ovvero le classi laterali dello stabilizzatore sono le stesse.

Proposizione 3. *Gli elementi dell'orbita di x sono in corrispondenza biunivoca con le classi laterali di $St(x)$.*

$$orb(x) \longleftrightarrow \{gSt(x)\}$$

$$gx \longleftarrow g$$

Se $|G| < \infty \implies |G| = |St(x)| \cdot |orb(x)| \ \forall x \in X$. Ovviamente $|orb(x)| \mid |G|$.

Esempio 2. *G gruppo, $X = G$.*

$$G \longrightarrow Int(G) < S(x)$$

$$g \longmapsto \varphi_g(x) = gxg^{-1}$$

E' un azione di G su se stesso.
$orb(x) = \{gx | g \in G\} = \{gxg^{-1} | g \in G\} =$ classe di coniugio, si indica con $Cl(x)$ oppure C_x.

$St(x) = \{g \in G | gxg^{-1} = x\} = Z_G(x) =$ centralizzatore di x (insieme degli elementi che commutano con x).

Se G è finito $\implies |G| = |Cl(x)| \cdot |Z_G(x)| \forall x \in G$.

$$\bigcap_{x \in G} Z(x) = Z(G)$$

Esempio 3. *G gruppo, $X = \{sottogruppi \ di \ G\}$.*

$$\varphi : G \longrightarrow S(X)$$

$$g \longrightarrow \varphi_g \ (H \mapsto gHg^{-1})$$

φ omomorfismo, ben definito.
$St(H) = \{g \in G | gHg^{-1} = H\} =^{def} N_G(H) =$ normalizzatore in G di H, il più grande sottogruppo di G in cui H è normale.

$orb(H) = \{gHg^{-1} | g \in G\} =$ coniugati di H.

Se G è finito: $|G| = |N_G(H)| \cdot |orb(H)|$.

$H \triangleleft G \iff N_G(H) = G \iff orb(H) = \{H\}$ $\qquad |orb(H)| = |\{gHg^{-1} | g \in G\}| = \underbrace{[G : N_G(H)]}_{indice \ del \ normalizzatore}$

Formula delle classi, teorema di Cauchy e teorema di Cayley.

Ricapitoliamo quanto detto fin ora. G gruppo, $\varphi : G \longrightarrow S(X)$, ovvero G agisce su X tramite φ. Supponiamo che G agisca su G. Allora:

$$|G| < \infty \implies |G| = \sum_{x \in R} |orb(x)| = \sum_{x \in R} \frac{|G|}{|St_G(x)|}$$

In particolare, essendo St_G un sottogruppo di G, la sua cardinalità divide quella del gruppo. E' molto interessante distinguere gli elementi che hanno orbita banale dagli altri. Chiamiamo come al solito R l'insieme dei rappresentanti e $R' = R - \{x \in G \mid orb(x) = \{x\}\}$. Si ha dunque:

$$\sum_{x \in R} \frac{|G|}{|St_G(x)|} = \sum_{\substack{x \in R \\ orb(x) = \{x\}}} 1 + \sum_{x \in R'} \frac{|G|}{|St_G(x)|}$$

Nel caso particolare dell'azione di coniugio:

$$\varphi : G \longrightarrow S(G)$$
$$g \mapsto \varphi_g(x \mapsto gxg^{-1})$$
$$orb(x) = \{gxg^{-1} | g \in G\} = Cl(x) \qquad St_G(x) = Z_G(x)$$

Quali sono gli elementi che hanno orbita banale per il coniugio?

$$Cl(x) = \{gxg^{-1} | g \in G\} = \{x\} \iff gxg^{-1} = x \ \forall g \in G \iff x \in Z(G)$$

Da questo si ricava:

$$|G| = \sum_{x \in Z(G)} 1 + \sum_{x \in R'} \frac{|G|}{|St_G(x)|} \qquad R' = R - Z(G)$$

$$\implies |G| = |Z(G)| + \sum_{x \in R'} \frac{|G|}{|Z_G(x)|}$$

Quest'ultima uguaglianza è chiamata **formula delle classi** (di coniugio).

Applicazioni ai p-gruppi.

Definizione 7 (p-gruppo)**.** *Sia p un numero primo. Un p-gruppo è un gruppo finito G con $|G| = p^n$.*

Proposizione 4. *Il centro di un p-gruppo è non banale.*

Dimostrazione.

$$p^n = |G| = |Z(G)| + \sum_{x \in R'} \frac{|G|}{|Z_G(x)|}$$

Osservo ora chi sono gli elementi della somma.

$$x \in R' \ \ Z_G(x) \subsetneq G \implies \frac{|G|}{|Z_G(x)|} > 1 \implies p \ \Big| \ \frac{|G|}{|Z_G(x)|}$$

$$\implies p \ \Big| \ \sum_{x \in R'} \frac{|G|}{|Z_G(x)|} \implies |Z(G)| = |G| - \sum_{x \in R'} \frac{|G|}{|Z_G(x)|} = p^n - p \cdot k \implies p \mid |Z(G)|$$

□

Osservazione 5. *Un sottogruppo non banale di un p-gruppo è un p-gruppo.*

Teorema 1. *Un gruppo di ordine p^2 è abeliano.*

Dimostrazione. $|G| = p^2 \implies |Z(G)| \mid p^2 \implies |Z(G)| \in \{1, p, p^2\}$. Chiaramente il centro non può avere ordine 1 perché G è un p-gruppo e ha un centro non banale.

$$|Z(G)| = p \implies {}^{G}\!/_{Z(G)} \text{ ha ordine p} \implies {}^{G}\!/_{Z(G)} \text{ ciclico}$$

Ma questo è assurdo perché ${}^{G}\!/_{Z(G)}$ è ciclico $\iff$ G è abeliano. Per esclusione allora $|Z(G)| = p^2$. □

Teorema 2 (Teorema di Cauchy)**.** *p primo, G gruppo finito. Se $p \mid o(G) \implies \exists x \in G \mid o(x) = p$.*

Osservazione 6. *Per il teorema di Lagrange sappiamo che se* $H < G \implies |H| \mid |G|$ *e se* $x \in G \implies o(x) \mid o(G)$. *Vale il viceversa? Se* $d \mid o(G) \exists x \in G \mid o(x) = d$*? Questo è falso, basta prendere come controesempio* $\mathbb{Z}2 \times \mathbb{Z}2$ *che non ha elementi di ordine* 4. *Se invece ci chiediamo se* $\exists H < G \mid o(H) = d$ *questa cosa è vera solo i gruppi abeliani.*

Osservazione 7. *E' comodo ricordare che se* G *è abeliano,* $x, y \in G \mid o(x) = m, o(y) = n \implies \exists z \in G \mid o(z) = m.c.m(m, n)$.

Dimostrazione. (Teorema di Cauchy) $|G| = p \cdot n$. Procediamo per induzione su n. Il passo base è ovvio, poiché se $n = 1$ allora G è ciclico di ordine $p \implies o(x) = p$. Suppongo vera la tesi per gruppi di ordine $p \cdot m$ con $m < n$.

Caso 1) $\exists H < G$ proprio t.c. $p \mid o(H) \implies |H| = p \cdot m \implies m < n \implies$ per ipotesi induttiva $\exists x \in H \mid o(x) = p \implies x \in G$ poiché $x \in H$.

Caso 2) $\forall H < G$ proprio, $p \nmid o(H)$. Utilizziamo qui la formula delle classi.

$$p \cdot n = |G| = |Z(G)| + \sum_{x \in R'} \frac{|G|}{|Z_G(x)|}$$

$x \in R' \implies Z_G(x) < G$ proprio $\implies p \nmid |Z_G(x)| \implies p \Big| \frac{|G|}{|Z_G(x)|} \implies p \mid |Z(G)|$ ma nessun sottogruppo proprio di G ha cardinalità divisibile per $p \implies Z(G) = G \implies G$ abeliano. Concludiamo utilizzando il teorema di Cauchy per gruppi abeliani, il quale ci dice che $\exists x \in G \mid o(x) = p$.

□

Abbiamo già visto che i gruppi di ordine p sono tutti isomorfi a $\mathbb{Z}/p\mathbb{Z}$, mentre i gruppi di ordine p^2 sono tutti isomorfi a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ oppure a $\mathbb{Z}/p^2\mathbb{Z}$. Quali sono i gruppi di ordine 6?

Proposizione 5. G *gruppo,* $o(G) = 6$. *Allora se* G *è abeliano* $G \cong \mathbb{Z}6$ *altrimenti* $G \cong S_3$.

Dimostrazione. $|G| = 6 \implies$ per Cauchy $\exists x, y \in G \mid o(x) = 2, o(y) = 3$. Se G è abeliano allora $o(xy) = 6 \implies G$ ciclico $\implies G = \langle xy \rangle \implies G \cong \mathbb{Z}6$.

Se G non è abeliano considero $\langle x, y \rangle < G$. Ricordiamo che preso $HK = \{hk | h \in H, k \in K\}$, $HK < G \iff HK = KH$ e che $|HK| = \frac{|H||K|}{|H \cap K|}$ come insieme.

Allora si ha $|\langle x \rangle \langle y \rangle| = 6 \implies G = \langle x \rangle \langle y \rangle, \langle x \rangle = \{e, x\}, \langle y \rangle = \{e, y, y^2\} \implies G = \{e, x, y, xy, y^2, xy^2\}$. Esibiamo dunque un isomorfismo fra G ed S_3.

$$\varphi : G \longrightarrow S_3 \text{ t.c. } \varphi(x) = \tau, \quad \varphi(y) = \sigma$$

□

Teorema 3 (Teorema di Cayley)**.** G *gruppo* $\implies G$ *è isomorfo ad un sottogruppo di* $S(G)$. *In particolare se* $|G| = n \implies G$ *è isomorfo ad un sottogruppo di* S_n.

Dimostrazione. L'obiettivo è trovare un'azione fedele di G in se stesso, ossia un omomorfismo $\Phi : G \to S(G)$ iniettivo.

$$\Phi : G \longrightarrow S(G)$$
$$g \mapsto \varphi_g (x \mapsto gx)$$

E' chiaramente ben definito perché $\varphi_g \in S(G)$. $\varphi_g : G \to G$ è bigettiva: infatti $\varphi_g(x) = \varphi_g(y) \iff gx = gy \iff x = y$ ed è surgettiva perché $\forall y \in G \varphi_g(g^{-1}y) = y$, $g^{-1}y \in G$. Vediamo che $\Phi(gh) = \Phi(g)\Phi(h)\ \forall g, h \in G$, infatti $\varphi_{gh} = \varphi_g \circ \varphi_h$ e, applicando ad $x \in G$, ottengo $(gh)x = g(hx)$.
Dimostriamo che Φ è iniettivo: $\text{Ker}(\Phi) = \{g \in G \mid \varphi_g = id\}$. $\varphi_g(x) = x\ \forall x \in G \iff gx = x \iff g = e$. □

Osservazione 8. *Nessuno mi dice che* n *è il più piccolo ordine di* $S(G)$ *affinché ci sia l'immersione: basti pensare a* $\mathbb{Z}/10\mathbb{Z}$ *che chiaramente si immerge in* S_{10}*, ma sarebbe bastato anche* S_5.

Esercizio 2 (Difficile)**.** *Qual è il minimo* n *t.c.* $G < S_n$*?*

Definizione 8 (Generato)**.** *Sia* G *un gruppo,* S *un suo sottoinsieme. Il generato da* $S, \langle S \rangle$ *è il più piccolo sottogruppo di* G *che contiene* S.

Osservazione 9. *Questo sottogruppo esiste e lo esibisco:*

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subset H}} H$$

dove il RHS è chiaramente non vuoto perché vi è G.

Proposizione 6. $\langle S\rangle = \{s_1 \cdots s_k \mid k \in \mathbb{N}\}$, *parole di lunghezza finita.*

Dimostrazione. Chiamo $X = \{s_1 \cdots s_k \mid k \in \mathbb{N}\},\ s_i \in S \cup S^{-1},\ S^{-1} = \{s^{-1} | s \in S\}$. Dico che $X = \langle S\rangle$. So che $\langle S\rangle = \bigcap_{\substack{H \leq G \\ S \subset H}} H$.

$X \subseteq \langle S\rangle$, basta far vedere $X \subset H\ \forall H$ nell'intersezione. So che $S \subset H$ e che $H < G \implies S^{-1} \subset H \implies S, S^{-1} \subset H \implies X \subset H \forall H \supset S \implies X \subset \bigcap_{\substack{H \leq G \\ S \subset H}} H = \langle S\rangle$.

Claim: mi basta vedere che X è un sottogruppo di G, ma questa verifica è facile (infatti $S \subset X \implies X$ è uno degli $H \implies X \supset \bigcap H = \langle S\rangle$). □

Osservazione 10. $|G| < \infty \implies \langle S\rangle = \{s_1 \cdots s_k \mid k \in \mathbb{N}, s_i \in S\}$ *poiché se è finito gli inversi di ogni elemento si esprimono in funzione dei prodotti di* s_i *(*s_i *ha ordine finito).*

Definizione 9 (Commutatore)**.** *G gruppo, definiamo il commutatore di* $g, h \in G$ $[g, h] = ghg^{-1}h^{-1}$.

Definizione 10 (Gruppo derivato)**.** $G' =< [g, h] \mid g, h \in G >$ *è detto gruppo derivato (o gruppo dei commutatori) di G.*

- $G' = \{e\} \iff G$ abeliano.
- $G' \triangleleft G :\ \forall x \in G x[g, h]x^{-1} \in G\ \forall g, h \in G$, infatti: $xghg^{-1}h^{-1}x^{-1} = xgx^{-1}xhx^{-1}xg^{-1}x^{-1}xh^{-1}x^{-1} = [xgx^{-1}, xhx^{-1}] \in G'$.
- G' è caratteristico in G: $f \in Aut(G) \implies f([g, h]) = [f(g), f(h)]$.

Osservazione 11. *Basta verificare sui generatori, infatti ad esempio:*

- $\langle S\rangle$ *abeliano* $\iff \forall s_1, s_2 \in S\ s_1s_2 = s_2s_1$*;*
- $\langle S\rangle$ *normale* $\iff \forall g \in G\ \forall s \in S\ gsg^{-1} \in \langle S\rangle$*;*
- $\langle S\rangle$ *caratteristico* $\iff \forall f \in Aut(G),\ \forall s \in S\ f(s) \in \langle S\rangle$.

Proposizione 7. $H \triangleleft G$, G/H *abeliano* $\iff G' \subset H$.

Dimostrazione. G/H abeliano $\iff \forall x, y \in G\ xHyH = yHxH \iff xyH = yxH \iff x^{-1}y^{-1}xy \in H \iff \forall x, y \in G [x, y] \in H \iff G' \subset H$. □

Il gruppo diedrale.

Prendo un poligono regolare e fisso $n = \#\text{lati}$.

$$D_n = \{\text{isometrie di un n-agono regolare}\} = \{n \text{ rotazioni e } n \text{ simmetrie}\}$$

Rappresento D_n come:

$$D_n = \langle \rho, \vartheta : \ \rho^n = e, \ \vartheta^2 = e, \ \vartheta\rho\vartheta = \rho^{-1} \rangle$$

Con queste informazioni ho dunque definito D_n; supponiamo di avere $g \in D_n$ della forma $g = \rho^{a_1} \cdot \vartheta^{b_1} \cdots \rho^{a_n} \cdot \vartheta^{b_n}$. Allora posso ricondurmi ad una parola della forma:

$$(*) \ \vartheta\rho^i \qquad (**) \ \rho^i \qquad 0 \leq i \leq n-1$$

tramite le relazioni: $\rho^n = e, \ \rho\rho^{-1} = e, \ \vartheta^2 = e, \ \vartheta\vartheta^{-1} = e, \ \vartheta\rho\vartheta = \rho^{-1}$.

Osservazione 12. *I generatori di D_n sono del tipo (*)$\vartheta = \vartheta\rho^0$, (**)$\rho = \rho^1$.*

Osservazione 13. *Gli elementi della forma (*) o (**) stanno tutti in D_n, ossia sono tutti generati da ρ e ϑ.*

Osservazione 14. *Moltiplicando e facendo l'inverso di elementi del tipo (*) o (**) ottengo ancora elementi del tipo (*) o (**).*

Dimostrazione. 1 $(**)\cdot(**) \implies \rho^i \cdot \rho^j = \rho^{i+j}, \quad i+j < n \implies \rho^i \cdot \rho^j = \rho^{i+j}, \ i+j \geq n \implies \rho^i \cdot \rho^j = \rho^{i+j-n}$;

2 $(*)\cdot(**) \implies \vartheta\rho^i\rho^j = \vartheta\rho^{i+j}, \quad i+j < n \implies \vartheta\rho^i\rho^j = \vartheta\rho^{i+j}, \ i+j \geq n \implies \vartheta\rho^i\rho^j = \vartheta\rho^{i+j-n}$;

3 $(**)\cdot(*) \implies \rho^i\vartheta\rho^j = \vartheta\vartheta\rho^i\vartheta\rho^j = \vartheta\vartheta\rho^i\vartheta^{-1}\rho^j \implies \vartheta\rho^i\vartheta^{-1} = \underbrace{\vartheta\rho\vartheta\vartheta^{-1}\rho\vartheta\vartheta^{-1}\cdots\vartheta\rho\vartheta^{-1}}_{\substack{\text{sono } i \text{ e ognuno di essi} \\ \text{mi produce un } \rho^{-1}}}$

$\implies \vartheta\rho\vartheta^{-1} = \rho^{-i} \implies \rho^i\vartheta\rho^j = \vartheta\vartheta\rho^i\vartheta^{-1}\rho^j = \vartheta\rho^{-i}\rho^j = \vartheta\rho^{-i+j}$.

$-i+j > n \implies \vartheta\rho^{-i}\rho^j = \vartheta\rho^{-i+j}, \quad -i+j \leq n \implies \vartheta\rho^{-i}\rho^j = \vartheta\rho^{-i+j+n}$;

4 $(*)\cdot(*) \implies \vartheta\rho^i\vartheta\rho^j = \rho^{-i}\rho^j = \rho^{-i+j}, \quad -i+j > n \implies \rho^{-i}\rho^j = \rho^{-i+j}, \ -i+j \leq n \implies \rho^{-i}\rho^j = \rho^{-i+j+n}$

□

Potevo anche definire gli esponenti di ρ come classi di equivalenza:

$$\rho^{[i]} = \rho^i \quad [i] \in \mathbb{Z}/n\mathbb{Z}, \text{ ben definita perché } \rho^n = e$$

Problema: mi chiedo se sia possibile che due elementi coincidano, cioè se è possibile che per qualche i, j si abbia $\rho^i = \vartheta\rho^j$.

Considero una funzione che manda il mio n-agono nel piano reale. In questo caso le isometrie di D_n corrispondono ad un sottogruppo di $O_2(\mathbb{R})$. Prendo una funzione che mandi:

$$\rho \longmapsto \begin{pmatrix} \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n}) \\ -\sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix} = M_\rho$$

$$\vartheta \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = M_\vartheta$$

Devo verificare che questa funzione sia ben definita e sia un omomorfismo, cioè verificare che mandi $g \mapsto M_g, \ g' \mapsto M_{g'}, \ g^{-1} \mapsto (M_g)^{-1}, \ gg' \mapsto M_g M_{g'}$. Definisco allora la mia funzione sui rappresentanti: $\rho^i \mapsto (M_\rho)^i, \ \vartheta \mapsto M_\vartheta, \ \vartheta\rho^i \mapsto M_\vartheta(M_\rho)^i$. Per verificare che sia un omomorfismo mi basta provare che $(M_\rho)^n = id, \ (M_\vartheta)^2 = id, \ M_\vartheta M_\rho M_\vartheta = (M_\rho)^{-1}$.

Dalla definizione di $D_n = \langle \rho, \vartheta : \rho^n = e, \ \vartheta^2 = e, \ \vartheta\rho\vartheta = \rho^{-1} \rangle$ so che la cardinalità di D_n può essere al massimo $2n$, ma potrebbe anche essere minore per via del problema espresso sopra. Se chiamo φ la funzione definita sopra, allora:

$$\varphi : \{\text{parole in } \rho, \vartheta\}/\{\text{relazioni tra parole}\} \longrightarrow \langle M_\vartheta, M_\rho \rangle$$

è un omomorfismo surgettivo e di conseguenza, poiché l'immagine ha almeno $2n$ elementi, il diedrale ha cardinalità esattamente $2n$.

Tutto questo dimostra che $o(\rho) = n$.

Quanti sono gli elementi di ordine r in D_n? So che $\exists C_n < D_n$ con $C_n = \langle \rho \rangle$ ciclico. $\forall r \mid n$ gli elementi di ordine r in C_n sono $\varphi(r)$. Considero ora le riflessioni $\vartheta\rho^i$: qual è l'ordine? $(\vartheta\rho^i)^2 = (\vartheta\rho^i)(\vartheta\rho^i) = \vartheta\rho^i\vartheta\rho^i = \rho^{-i}\rho^i = e \implies$ ogni riflessione ha sempre ordine 2.

$$r = 2 \implies \begin{cases} n \text{ pari} \implies n+1 \text{ elementi di ordine 2} \\ n \text{ dispari} \implies n \text{ elementi di ordine 2} \end{cases}$$

$$r \neq 2 \implies \begin{cases} r \mid n \implies \varphi(r) \text{ elementi di ordine r} \\ r \nmid n \implies \text{non ho elementi di ordine r} \end{cases}$$

Teorema 4 (Sottogruppi di D_n)**.** *I sottogruppi di D_n possono essere solo di due tipi:*

- *$H < C_n$ e ne abbiamo esattamente uno per ogni divisore di n;*
- *$H = (H \cap C_n) \sqcup \tau(H \cap C_n)$ e ne abbiamo d di ordine $\frac{2n}{d}$ per ogni $d|n$.*

Dimostrazione. Se $H < C_n$ allora sappiamo che esiste un unico gruppo di ordine d per ogni $d|n$.
Se invece $H \not< C_n$, H contiene almeno una rotazione: $\tau = \sigma\rho^i$. Consideriamo l'omomorfismo f che fa commutare il seguente diagramma:

$$\begin{array}{ccc} D_n & \xrightarrow{\Phi} & O_2(\mathbb{R}) \\ {\scriptstyle f}\downarrow & \swarrow_{det} & \\ \{\pm 1\} \cong \mathbb{Z}_2 & & \end{array}$$

E' facile vedere che $\operatorname{Ker} f = C_n \triangleleft D_n$ e dunque possiamo considerare la restrizione dell'omomorfismo ad H:

$$\begin{array}{ccc} H & \xrightarrow{f|_H} & f(H) \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle id} \\ D_n & \xrightarrow{f} & \mathbb{Z}_2 \end{array}$$

Da cui si ricava che $f^{-1}(0) \sqcup f^{-1}(1) = (H \cap C_n) \sqcup \tau(H \cap C_n) = H$ poiché conosciamo il Ker della trasformazione. Poiché $(H \cap C_n) < C_n \implies H \cap C_n = \langle \rho^d : d|n \rangle$ e il suo unico laterale sarà composto dagli elementi della forma $\tau(H \cap C_n) = \{\sigma\rho^{d+i}, \sigma\rho^{2d+i}, \ldots, \sigma\rho^{n-m+i}\}$ che dipende unicamente dalla classe di $i \mod m$. □

Riflessione per capire cosa abbiamo fatto in questa lezione. Sostanzialmente se H è un sottogruppo di C_n non ci sono problemi, altrimenti se non è un sottogruppo del gruppo ciclico delle rotazioni, allora sarà composto da due parti: una che è il generato della rotazione che è nell'intersezione tra H e C_n, l'altra che è invece generata dalla riflessione composta con tutte le rotazioni, ovvero $\langle \vartheta\rho^i \rangle$.

$$H \not< C_n \implies H = \{\rho^k, \rho^{2k}, \ldots, \rho^{n-k}\} \cup \{\vartheta\rho^i, \vartheta\rho^{i+m}, \ldots, \vartheta\rho^{i+n-m}\}$$

Gruppo simmetrico.

Definizione 11. *Sia X un insieme. $\mathcal{S}(X) = \{f : X \to X | f$ è bigettiva$\}$ è l'insieme delle permutazioni di X.*

Osservazione 15. *Se $X = \{1, \dots, n\}$, allora $\mathcal{S}(X) = S_n$ con $|S_n| = n!$.*

Esempio 4.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 7 & 6 & 8 & 4 & 5 & 9 & 10 \end{pmatrix} = (123)(47)(563)(9)(10) = (123)(47)(568)$$

Da questo esempio osservo che σ è una composizione di bigezioni, inoltre ogni permutazione può essere scritto come prodotto di permutazioni cicliche disgiunte in modo unico a meno dell'ordine e della scrittura.

Osservazione 16.
- *Cicli disgiunti commutano;*
- *Un k-ciclo ha k scritture differenti (#scelte per il primo elemento);*
- *I cicli sono orbite.*

Dimostrazione. Prendo $\sigma \in S_n$ e considero $\varphi : G = \langle \sigma \rangle \to S_n$. Questa è un'azione. Allora $orb(x) = \{\sigma^k(x)\}_{k \in \mathbb{Z}}$

$$\{\sigma^k(x)\}_{k \in \mathbb{Z}} = \{x, \sigma(x), \dots, \sigma^{n-1}(x)\}$$

Quindi ottengo il ciclo $(x, \sigma(x), \dots, \sigma^{n-1}(x))$ da cui osservo che le orbite sono disgiunte perché univocamente determinate dall'azione φ e la scrittura non conta poiché sono cicliche. □

Corollario 1. *S_n è generato da cicli.*

Osservazione 17. *In S_n ci sono $\binom{n}{k}(k-1)!$ k-cicli.*

Esempio 5. *In S_{10} ci sono $\binom{10}{5}4!$ 5-cicli.*
$\#\{\sigma \in S_{12} |$ *siano di tipo* $3+3+2+2+2\} = \frac{\binom{12}{3}\binom{9}{3}}{2!}2!2!\frac{\binom{6}{2}\binom{4}{2}\binom{2}{2}}{3!}1!1!1!$

Ordine di una permutazione.

Proposizione 8. *L'ordine di un k-ciclo è k e l'ordine di una permutazione è il minimo comune multiplo dell'ordine dei suoi cicli disgiunti.*

Dimostrazione. Prendo $\sigma = (a_1, \dots, a_k)$ e $\sigma^k = id$, $\sigma^k(a_i) = a_{i+k} = a_i$. Ora considero $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ con σ_i cicli disgiunti e $o(\sigma_i) = k_i$. Prendo $m = [k_1, \dots k_r]$. Allora si ha $\sigma^m = (\sigma_1 \circ \cdots \circ \sigma_r)^m = \sigma_1^m \circ \cdots \circ \sigma_r^m = id$. Se $\exists d \in \mathbb{Z}$ t.c. $\sigma^d = id \implies \sigma_1^d \circ \cdots \circ \sigma_r^d = id$, allora suppongo $\sigma_i(a) \neq a$. Si ha dunque $\sigma_j(a) = a \ \forall i \neq j \implies \sigma_i^d(a) = a \implies k_i | d \ \forall i \implies m | d$. Quindi m è il minimo. □

Trasposizioni.

Proposizione 9. *Tutte le permutazioni sono prodotto di trasposizioni, quindi queste ultime sono generatori per S_n.*

Dimostrazione. Mi basta dimostrare che i cicli sono prodotti di trasposizioni. Prendo il k-ciclo $(1 \ \dots \ k) = (1 \ k)(1 \ k-1)(1 \ k-2) \dots (1 \ 2)$. Ora mi basta osservare che 1 va in 2 e fare la verifica su un qualunque altro elemento: funziona (convincersene). □

Osservazione 18. *La struttura come prodotto di permutazioni non è unica, ma è unica la parità del numero di trasposizioni.*

Proposizione 10. *L'applicazione*

$$sgn : S_n \longrightarrow \{\pm 1\} = \mathbb{Z}^*$$
$$\sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{(\sigma(i) - \sigma(j))}{(i-j)}$$

è un omomorfismo di gruppi. Inoltre se σ è una trasposizione, $sgn(\sigma) = -1$.

Corollario 2. *$sgn(\sigma)$ mi da la parità del numero di trasposizioni che compio in una qualsiasi altra scrittura di σ come prodotto di trasposizioni.*

Dimostrazione. Voglio che *sgn* sia ben definita $\forall \sigma \in S_n$, ovvero che $sgn(\sigma) \in \{\pm 1\}$. σ è bigettiva, allora:

- Numeratore: Abbiamo $\sigma(i) - \sigma(j) \in \{\sigma(i), \sigma(j)\}$ qualsiasi tra $\{1, \dots, n\}$;
- Denominatore: Abbiamo $i - j \in \{i, j\}$ qualsiasi tra $\{1, \dots, n\}$ con $i < j$.

Al variare di i, j in $\{1, \dots, n\}$ sia il numeratore che il denominatore mi descrivono tutti i valori possibili e dunque, a meno di segni, semplificando si ottiene 1. Dunque sgn è ben definita.

$$sgn(\sigma \circ \tau) = \prod_{1 \le i < j \le n} \left(\frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j} \right)$$

$$= \prod_{1 \le i < j \le n} \left(\frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \right) \cdot sgn(\tau) = sgn(\sigma) \cdot sgn(\tau)$$

poiché τ è bigettiva. Dunque sgn è un omomorfismo.

Se σ è trasposizione, scrivo $\sigma = (a\ b)$.

- Se $\{i, j\} \cap \{a, b\} = \emptyset \implies \sigma(i) = i \ \wedge \sigma(j) = j \implies sgn((a\ b)) = 1$;
- Se $\{i, j\} \cap \{a, b\} = \{i, b\} \vee \{a, i\} \implies sgn((i\ b)) = \frac{i-b}{i-a} = 1 \ \vee sgn((a\ i)) = \frac{i-a}{i-b} = 1$
- Se $\{i, j\} \cap \{a, b\} = \{a, b\} \implies sgn((a\ b)) = \frac{b-a}{a-b} = -1$

□

Classi di coniugio in S_n.

Teorema 5. *Due permutazioni in S_n sono coniugate $\iff$ hanno lo stesso tipo di decomposizione in cicli disgiunti.*

Dimostrazione. $\implies$) Prendo σ e $\tau\sigma\tau^{-1}$, con $\sigma = (a_1, \dots, a_k)$ e $\tau(a_i) = b_i$. Ma allora $\tau\sigma\tau^{-1}(b_i) = \tau(\sigma(a_i)) = \tau(a_{i+1}) = b_{i+1}$ e dunque ottengo il k-ciclo $(b_1, \dots, b_k)$. Ora, se $x \neq b_i \ \forall i$ ho che $\tau^{-1}(x) \neq a_i \implies \tau\sigma(\tau^{-1}(x)) = \tau\tau^{-1}(x) = x$ poiché $\tau^{-1}(x)$ è punto fisso per σ.

Se invece $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ cicli disgiunti, allora $\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \dots (\tau\sigma_r\tau^{-1})$ e se i σ_i sono disgiunti lo sono anche i $\tau\sigma_i\tau^{-1}$ per come sono definiti.

$\impliedby$) $\sigma = (a_1 \dots a_k)$. Se ora prendo $\tau\sigma\tau^{-1} = \rho$, poiché $\tau(a_i) = b_i$ si ha che $\rho = (b_1 \dots b_k)$.

□

Ancora sul diedrale: sottogruppi e automorfismi.

Ricapitoliamo quanto è stato detto sul diedrale. Se consideriamo D_n sappiamo già che al suo interno vi è C_n come gruppo ciclico. Abbiamo dunque detto che se $H < D_n$ allora ho due possibilità: o $H < C_n$ oppure $H = (H \cap C_n) \cup^\circ (\tau H \cap C_n)$, dove τ è una riflessione.

Esempio 6. *Quali sono i sottogruppi di D_4?*
$D_4 = \langle \rho, \sigma \mid \rho^4 = \sigma^2 = id, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle$. *Come ben sappiamo,* $C_4 < D_4, C_4 = \langle \rho \rangle \supset \langle \rho^2 \rangle \cong \mathbb{Z}/2\mathbb{Z} \supset \{e\}$.
Analizziamo gli altri casi.

- $H \cap C_4 = \langle \rho \rangle \implies H = D_4$;
- $H \cap C_4 = \langle \rho^2 \rangle \implies \begin{cases} H = \langle \rho^2, \sigma \rangle = \langle \rho^2, \sigma\rho^2 \rangle = \langle \rho^2, \sigma\rho^{2k} \rangle \\ H = \langle \rho^2, \sigma\rho \rangle \end{cases}$
- $H \cap C_4 = \{e\} \implies H = \langle \sigma \rangle, \langle \sigma\rho \rangle, \langle \sigma\rho^2 \rangle, \langle \sigma\rho^3 \rangle$.

Esercizio 3. *Trovare tutti i sottogruppi di D_6.*

Come già visto posso creare un morfismo da $D_n \to GL_2(\mathbb{R})$ oppure posso mandare $D_n \to S_n$, ponendo $f(\rho) = (1, 2, \dots, n)$ e $f(\sigma) = (2, n)(3, n-1)\dots$

Quali sono i sottogruppi normali del diedrale? Sicuramente C_n ha indice 2 in D_n e di conseguenza $C_n \triangleleft D_n$. Se n è pari $\langle \rho^2 \rangle \subset C_n$ e considero $H \not< C_n$ t.c. $H \cap C_n = \langle \rho^2 \rangle$. Ma allora $H = \langle \rho^2 \rangle \cup^\circ \tau\langle \rho^2 \rangle$ con τ riflessione. In totale questo ha n elementi e chiaramente è normale poiché $[D_n : H] = 2$. Se n è pari ci sono due sottogruppi di questo tipo: $\langle \rho^2, \sigma \rangle$ oppure $\langle \rho^2, \sigma\rho \rangle$. I sottogruppi di indice 2 in D_n sono tutti normali e in particolare sono:

$$\begin{cases} C_n & \text{se } n \text{ è dispari} \\ C_n, \langle \rho^2, \sigma \rangle, \langle \sigma\rho, \rho^2 \rangle & \text{se } n \text{ è pari} \end{cases}$$

Sappiamo anche che $H < G$ è normale $\iff$ H è invariante per coniugio, ovvero se $gHg^{-1} = H \ \forall g \in G$. Mi chiedo quali sono le classi di coniugio di questi elementi.

- $\rho^j \rho^i \rho^{-j} = \rho^i$;
- $\sigma\rho^j \rho^i \rho^{-j} \sigma = \rho^{-i}$;
- $\rho^j \sigma \rho^i \rho^{-j} = \sigma\rho^{-j} \rho^i \rho^{-j} = \sigma\rho^{i-2j}$;
- $\sigma\rho^j \sigma\rho^i \rho^{-j} \sigma = \rho^{i-2j}\sigma = \sigma\rho^{2j-i}$.

Di conseguenza i viene mandato o in $-i+$numero pari oppure in $i-$ numero pari. Da questo si ricava subito che se n è pari, $\sigma\rho^i \sim \sigma\rho^j \iff i \equiv j \mod 2$. Se invece n è dispari tutte le riflessioni sono coniugate tra di loro. Quando n è dispari un sottogruppo che contiene una riflessione ed è normale le contiene tutte. Se n è dispari e $H \triangleleft D_n \quad \sigma\rho^i \in H \implies H = D_n$.

$H \triangleleft D_n$ proprio $\implies$ $H < C_n$ $\implies$ tutti i sottogruppi di C_n sono normali in D_n (vero sia per n pari che per n dispari). Se n è pari, $H \triangleleft D_n$, $\sigma\rho^i \in H$ è coniugata con $\sigma\rho^{i+2} \in H \implies \rho^2 \in H$. Ma allora se $H \neq D_n \implies H = \langle \rho^2, \sigma\rho^i \rangle$.

Ricordando che ogni sottogruppo ciclico di ordine finito n ha un unico sottogruppo di ordine $m \ \forall m|n \implies$ tutti i sottogruppi di un gruppo ciclico sono caratteristici.

Proposizione 11. *$G \triangleright H > K$, K caratteristico in $H \implies K \triangleleft G$.*

Dimostrazione. Se $\varphi : H \longrightarrow H$ è automorfismo, allora $\varphi(K) = K$. Sia $g \in G, \varphi_g : G \to G$ t.c. $\varphi(x) = gxg^{-1}$. Ma allora $\varphi_g(H) = H \implies \varphi_g|_H : H \to H$ è automorfismo e dunque $\varphi_g|_H(K) = \varphi_g(K) = K$. Poiché $gKg^{-1} = K \ \forall g \implies K$ normale. □

$$\text{Se } H < D_n \implies \begin{cases} H < C_n \implies H \cong \mathbb{Z}/m\mathbb{Z} \quad m|n \\ H \not< C_n \implies H \cong D_m \quad m|n \quad H \cap C_n = \langle \rho^{\frac{n}{m}} \rangle \end{cases}$$

Qual è il centro del diedrale? Se n è pari è $\langle \rho^{\frac{n}{2}} \rangle$, altrimenti è $\{e\}$.

Quozienti di D_n. Per ogni sottogruppo normale ho un quoziente G/H e ogni quoziente è ottenuto in questo modo a meno di automorfismi.

$$D_n \triangleright \langle \rho^m \rangle \quad m|n \implies \left| D_n/\langle \rho^m \rangle \right| = 2m$$

Dimostriamo ora che $D_m \cong D_n/\langle \rho^m \rangle$.

$$D_n = \langle \rho, \sigma | \rho^n = \sigma^2 = id, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle$$

$$D_m = \langle r, s | r^m = s^2 = id, srs^{-1} = r^{-1} \rangle$$

Costruiamo una applicazione che mi mandi ρ^i in r^i e $\sigma\rho^i$ in sr^i. Si verifica facilmente che questo è un omomorfismo e che il kernel è proprio uguale a $\langle \rho^m \rangle$ da cui, per il primo teorema di omomorfismo, otteniamo la tesi.

Tra i quozienti di D_n con n pari non ho ancora considerato tutti quelli per un sottogruppo di indice 2. Ma se $H < G$ tale che $[G : H] = 2 \implies {}^{G}\!/_{H} \cong \mathbb{Z}/2\mathbb{Z}$.

Automorfismi di D_n. Consideriamo $\varphi : D_n \to D_n$ automorfismo. Chiaramente C_n viene mandato in C_n. Per generare C_n ho esattamente $\varphi(n)$ elementi tra cui scegliere. Se fisso ρ di ordine n in C_n ho che $\varphi(\rho)$ è una delle $\varphi(n)$ rotazioni di ordine n in C_n. Se σ è una riflessione in D_n allora necessariamente $\varphi(\sigma)$ deve essere una riflessione, ovvero ha ordine 2 e non è in C_n. Per mandare una riflessione in una riflessione ho esattamente n possibilità. Dunque:

$$|Aut(D_n)| = \varphi(n) \cdot n$$

Prodotto diretto e automorfismi.

Teorema di struttura dei gruppi abeliani finitamente generati. Sia G un gruppo abeliano finitamente generato. Allora G si scrive in modo unico (a meno dell'ordine) come prodotto diretto di gruppi ciclici.

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \qquad \text{con } n_1 | n_2 | \dots | n_s$$

Esempio 7. $\mathbb{Z}_{44} \times \mathbb{Z}_{88} \cong \mathbb{Z}_4 \times \mathbb{Z}_{11} \times \mathbb{Z}_8 \times \mathbb{Z}_{11}$

Definizione 12 (p-Sylow)**.** *Sia G un gruppo finito tale che $|G| = p^m n$ $(n,p) = 1$. $H < G, |H| = p^m$ si dice p-Sylow di G.*

Teorema 6. *Sia G un gruppo e siano $H, K \triangleleft G$. Allora:*

$$HK = G \wedge H \cap K = \{e\} \implies G \cong H \times K$$

Lemma 1. $H, K \triangleleft G, H \cap K = \{e\} \implies hk = kh \ \forall h \in H, \forall k \in K$

Dimostrazione.

$$\begin{cases} hkh^{-1}k^{-1} = \underbrace{(hkh^{-1})}_{\in K} k \in K \\ h \underbrace{(khk^{-1})}_{\in H} \in H \end{cases} \implies hkh^{-1}k^{-1} \in H \cap K = \{e\}$$

□

Dimostrazione del Teorema 6.

$$\begin{aligned} \varphi \colon H \times K &\to G \\ (h,k) &\mapsto hk \end{aligned}$$

φ è un omomorfismo per il lemma, è surgettivo perché $HK = G$ ed è iniettivo poiché $H \cap K = \{e\}$. □

Osservazione 19.

- *In un prodotto diretto i fattori commutano tra loro.*
- $G = H \times K \implies Z(H \times K) \cong Z(H) \times Z(K)$
- $Int(H \times K) = \frac{H \times K}{Z(H \times K)} \cong \frac{H \times K}{Z(H) \times Z(K)} = \frac{H}{Z(H)} \times \frac{K}{Z(K)} \cong Int(H) \times Int(K)$
- $Aut(H \times K) \cong Aut(H) \times Aut(K)$? *In generale questa cosa non vale. Ad esempio consideriamo:*

$$Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3 \ncong Aut(Z_2) \times Aut(\mathbb{Z}_2) \cong I$$

Teorema 7.

$$\begin{aligned} \Phi \colon Aut(H) \times Aut(K) &\to Aut(H \times K) \\ (f,g) &\mapsto \varphi(h,k) = (f(h), g(k)) \end{aligned}$$

Φ è un omomorfismo iniettivo ed è surgettivo $\iff$ $H \times \{e\}$ e $\{e\} \times K$ sono caratteristici in $H \times K$.

Dimostrazione. Φ è ben definito: $\forall (f,g) \in Aut(H) \times Aut(K), \varphi \in Aut(H \times K)$ poiché $\varphi(h,k) = (f(h), g(k)) \in H \times K$.

φ è omomorfismo: $\varphi[(h,k) \cdot (h',k')] = \varphi(hh', kk') = (f(h,h'), g(k,k')) = (f(h), g(k))(f(h'), g(k')) = \varphi(h,k)\varphi(h',k')$;

φ è iniettivo: $\operatorname{Ker} \varphi = \{(e_H, e_K)\}$;

φ è surgettivo: $\forall (h,k) \in H \times K \ \exists h' \in H, k' \in K : f(h') = h \ \ g(k') = k \implies \varphi(h',k') = (f(h'), g(k')) = (h,k)$

Φ omomorfismo: $\Phi((f,g)(l,m)) = \Phi(f,g) \circ \Phi(l,m)$;

Φ iniettivo: $\operatorname{Ker}(\Phi) = \{(f,g) | \Phi(f,g) = id_{H \times K}\} = \{(id_H, id_K)\}$;

Se H e K sono caratteristici in $H \times K \implies \Phi$ è surgettivo. Infatti $\forall \varphi \in Aut(H \times K), \exists f \in Aut(H), g \in Aut(K)$ t.c.
$\varphi = \Phi(f,g)$. Pongo:

$$\begin{aligned} f &= \Pi_H \circ \varphi|_{H \times \{e\}_K} \\ g &= \Pi_K \circ \varphi|_{\{e\}_H \times K} \end{aligned}$$

Allora $f \in Aut(H), \ g \in Aut(K)$. Infatti:

- f è omomorfismo perché composizione di omomorfismi;

- f è iniettiva. Se $f(h) = f(h') \implies \Pi_H(\varphi(h, e_K)) = \Pi_H(\varphi(h', e_K))$ e poiché $H \times \{e_K\}$ è caratteristico, $\varphi(h, e_K) = (a, e_K),\ \varphi(h', e_K) = (b, e_K)$.
  Ma allora necessariamente deve essere $f(h) = a$ e $f(h') = b$, di conseguenza $\varphi(a, e_K) = (f(h), e_K) = (f(h'), e_K) = \varphi(b, e_K)$ e visto che φ è iniettivo, $h = h'$.

- f è surgettiva. Prendiamo un $h \in H$. Essendo $H \times \{e_K\}$ caratteristico, la controimmagine di (h, e_K) è un suo elemento e dunque $\varphi^{-1}(h, e_K) = (h', e_K)$. Allora si ha $f(h') = \Pi_H(\varphi(h', e_K)) = \Pi_H(h, e_K) = h$.

Notiamo, in ultima istanza, che $\Phi(f, g) = \varphi$. Infatti si ha che:

$$(\Phi(f, g))(h, k) = (f(h), g(k)) = (\Pi_H(\varphi(h, e_K)), \Pi_K(\varphi(e_H, k))) = (\Pi_H(\varphi(h, k)), \Pi_K(\varphi(h, k))) = \varphi(h, k)$$

dove la penultima uguaglianza segue da:

$$\Pi_H(\varphi(h, e_K)) = \Pi_H(\varphi(h, e_K))\Pi_H(\varphi(e_H, k)) = \Pi_H(\varphi(h, e_K)\varphi(e_H, k)) = \Pi_H(\varphi(h, k))$$

□

Esercizio 4. *Dimostrare che* $Aut(\mathbb{Z}_{20} \times \mathbb{Z}_2) \cong D_4 \times \mathbb{Z}_5^*$

Esercizio 5. *Caratterizzare* $Z_{S_{10}}(\sigma),\ \sigma = (1234)(56)$.

Lemmi carini su sottogruppi e automorfismi.

Teorema 8. *Se G ha solo elementi di ordine due ed è finito, allora $G \cong (\mathbb{Z}_2)^n$.*

Dimostrazione. Se ogni elemento ha ordine due, allora il gruppo è abeliano poiché $a^2b^2 = e = (ab)^2 = abab$ e semplificando otteniamo $ab = ba\ \forall a, b \in G$. Procediamo per induzione sulla dimensione di G. Se $|G| = 2$ è banale. Supponiamo ora che sia vero per tutti i gruppi di cardinalità minore di 2^n e supponiamo che $2^n \leq |G| < 2^{n+1}$. Considero un insieme di generatori $\langle g_1, \dots, g_k \rangle$ per un generico sottogruppo $H < G$. Questo sarà chiaramente isomorfo a $(\mathbb{Z}_2)^h$ per ipotesi induttiva. Prendiamo ora un elemento $g \notin H$, $\langle g \rangle \cong \mathbb{Z}_2$ e sia H che $\langle g \rangle$ sono normali in G con intersezione banale e di conseguenza si ha:

$$\langle g, g_1, \dots, g_h \rangle \cong H \times \langle g \rangle \cong (\mathbb{Z}_2)^h \times \mathbb{Z}_2 \cong (\mathbb{Z}_2)^{h+1}$$

Se $\langle g, g_1, \dots, g_h \rangle \cong G$ abbiamo finito, altrimenti posso iterare.

□

Esempio 8. *G abeliano finito. Supponiamo che $H \triangleleft G$ sia ciclico e che G/H sia ciclico. Supponiamo ora che $\left(o(H), o(G/H)\right) = 1$. Allora G è ciclico.*

Parlando dei gruppi di ordine 8 abbiamo trovato $\mathbb{Z}_8$ che contiene un elemento di ordine 8 e $\mathbb{Z}_2^3$ che contiene solo elementi di ordine 1 e 2. Supponiamo ora che ci sia $g \in G$ t.c. $o(g) = 4$. Allora $\langle g \rangle \cong C_4$ è ciclico e $|\langle g \rangle| = 4$. Inoltre $C_4 \triangleleft G$.

G contiene altri elementi di ordine 4 fuori da C_4?

Supponiamo che non ce ne siano altri: allora $\exists h \notin C_4$ *t.c.* $o(h) = 2$. Prendiamo questa mappa:

$$\begin{aligned} \varphi_h \colon C_4 &\to C_4 \\ x &\mapsto hxh^{-1} \end{aligned}$$

Allora ci sono solo due possibilità: o questa mappa è l'identità, oppure è l'automorfismo inverso (semplicemente perché $Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$).

- $\varphi_h \equiv id_{C_4} \implies G \cong C_4 \times \mathbb{Z}_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ perché $\langle h \rangle$ e C_4 commutano.
- $\varphi_h \not\equiv id \implies hgh = g^{-1}$. Allora è naturale definire un omomorfismo da D_4 in G che si verifica subito essere surgettivo e iniettivo, dunque $G \cong D_4$.

Se invece $\exists k \notin C_4$ *t.c.* $o(k) = 4$ consideriamo:

$$\begin{aligned} \varphi_k \colon C_4 &\to C_4 \\ x &\mapsto kxk^{-1} \end{aligned}$$

Come prima ci sono solo due possibilità:

- Se $\varphi_k = id_{C_4} \implies G \cong \mathbb{Z}2 \times \mathbb{Z}4$ poiché $\langle k \rangle$ e $\langle g \rangle = C_4$ commutano, dunque si può costruire un morfismo da $\mathbb{Z}_4 \times \mathbb{Z}_4 \to G$ notando che l'immagine deve avere dimensione 8 poiché c'è G e quindi G sarà isomorfo ad un quoziente di $\mathbb{Z}_4 \times \mathbb{Z}_4$ rispetto al generato di un elemento di ordine 2 (più precisamente, posso quozientare per $\langle 2, 0 \rangle, \langle 2, 2 \rangle, \langle 0, 2 \rangle$).
- Se $\varphi_k \neq id$ $o(k) = 4, o(g) = 4, kgk^{-1} = g^{-1}$. Allora G contiene e, g, g^2, g^3, k e k^3 che è l'inverso di k. Ci chiediamo ora se $(kg)^2$ è l'identità. Ma questo non è vero perché, tramite le relazioni che abbiamo, si ottiene $kgkg = k^2 \neq id$. Ma allora in G c'è anche kg che ha ordine 4 e non sta nè in $\langle k \rangle$ nè in $\langle g \rangle$. Essendoci anche il suo inverso, che è gk, ho esaurito tutti gli 8 elementi. Ma in questo gruppo c'è un elemento di ordine 1, uno di ordine 2 e 6 di ordine 4. Dunque $G \cong Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ con queste regole: $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$, $i^2 = k^2 = j^2 = -1$ (mandiamo ad esempio $g \mapsto i, k \mapsto j, gk \mapsto k$). Questo dunque è l'unico altro gruppo di ordine 8. Non ce ne sono altri.

Proviamo a descrivere $Aut(D_n)$ come gruppo. Affinché un automorfismo sia ammissibile, devo mandare $\rho \mapsto \rho\sigma^i$ e $\sigma \mapsto \sigma^j$ con $i \in \mathbb{Z}_n$ e $j \in \mathbb{Z}_n^*$. Un generico $\varphi \in Aut(D_n)$ è determinato da quello che fa sulle riflessioni, infatti: $\sigma\rho \mapsto \sigma\rho^i\rho^j \implies \varphi(\rho) = \varphi(\sigma^{-1})\varphi(\sigma\rho)$.

Ma questa mappa che ho scritto è una affinità di $\mathbb{Z}_n$, ovvero ho moltiplicato per un coefficiente e ho traslato. In Aff($\mathbb{Z}_n$) c'è un sottogruppo delle traslazioni isomorfo a $\mathbb{Z}_n$ e quello delle omotetie che è isomorfo a $\mathbb{Z}_n^*$. $\mathbb{Z}_n$ è normale in Aff($\mathbb{Z}_n$).

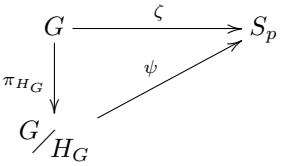
Come già sappiamo, se un gruppo G ha un sottogruppo di indice 2 allora questo è normale. Proviamo a generalizzare questo argomento.

Proposizione 12. *Se G ha ordine n e p è il più piccolo primo che divide n e H è un sottogruppo di G tale che $[G : H] = p \implies H \triangleleft G$.*

Dimostrazione. Consideriamo le classi laterali di H in G: $\{g_1H, \dots, g_pH\} = X$. Questo è un insieme di p elementi. La moltiplicazione a sinistra per un elemento di g permuta X e di conseguenza questo mi da un omomorfismo:

$$\begin{aligned} \zeta &\colon G \to S_p \\ g &\mapsto \pi_g \colon X \to X \qquad \pi_g(xH) = gxH \end{aligned}$$

Questa è l'azione di permutazione. Ci chiediamo ora qual è lo $\mathrm{Stab}(xH)$, ovvero quali sono i $g \in G | gxH = xH$. $gxH = xH \iff x^{-1}gxH = H \iff x^{-1}gx \in H \iff g \in xHx^{-1}$. Dunque lo stabilizzatore di una classe laterale è il coniugato di H rispetto ad x. Usiamo ora il fatto che $[G : H] = p$. Chiediamoci quindi cos'è $\mathrm{Ker}(\zeta)$. Se abbiamo calcolato lo stabilizzatore di un elemento siamo già a metà strada perché il nucleo è dato dall'insieme degli elementi di G che stabilizzano tutte le classi laterali. $g \in \mathrm{Ker}(\zeta) \iff g \in \bigcap xHx^{-1} := H_G$.



Sicuramente $\psi \colon {}^{G}\!/_{H_G} \to S_p$ è iniettiva.

Qual è la cardinalità di ${}^{G}\!/_{H_G}$? Non la conosco ma so che ${}^{G}\!/_{H}$ ha cardinalità p e so anche che se la mappa è iniettiva la cardinalità di ${}^{G}\!/_{H_G}$ divide la cardinalità di S_p che è $p!$. A questo punto ci sono solo due possibilità: o è 1 o è p perché è un numero che divide $p!$ e divide n che ha come più piccolo primo divisore p. Ma questo indice non può essere 1 perché l'indice di H_G in G è maggiore di p (vedi questa catena $G \supset H \supset H_G \implies [G : H] \leq [G : H_G]$). Ma allora $[G : H_G] = p \implies H_G = H$ poiché $H \supset H_G$ e $[G : H] = [G : H_G]$. Dunque $H = \bigcap xHx^{-1},\ x \in G = H_G \triangleleft G$ (poiché nucleo dell'omomorfismo ζ). □

Vogliamo calcolare $|Aut(\mathbb{Z} \times \mathbb{Z}_n)|$

In generale se $G = H \times K$ e H e K sono sottogruppi caratteristici allora $Aut(G) = Aut(H) \times Aut(K)$. $\mathbb{Z}_n$ è caratteristico in $\mathbb{Z} \times \mathbb{Z}_n$. Ogni elemento è del tipo (a, b): se $a \neq 0 \implies o(a, b) = \infty$, altrimenti se $a = 0$ l'ordine è finito e quindi questi elementi $(0, b)$ sono gli unici elementi di ordine finito e sono tanti quanti quelli in $\mathbb{Z}_n$.

Se noi abbiamo un gruppo G anche infinito e considero questo sottoinsieme $\{g \in G, o(g) \text{ finito}\}$, questo è un sottoinsieme caratteristico perché gli automorfismi preservano gli ordini degli elementi. Se è sottogruppo, allora è sottogruppo caratteristico. Sfortunatamente $\mathbb{Z}$ non è caratteristico in $\mathbb{Z} \times \mathbb{Z}_n$ perché se considero i due elementi $(1, \overline{0}), (0, \overline{1})$ questi chiaramente generano. Ma chi mi vieta di scegliere come coppia $(1, \overline{1}), (0, \overline{1})$ come generatori? Se creo una mappa che manda la prima coppia nella seconda, questa non manda $\mathbb{Z}$ in se stesso. Dunque $\varphi \in Aut(\mathbb{Z} \times \mathbb{Z}_n),\ \varphi(\{0\} \times \mathbb{Z}_n) = \{0\} \times \mathbb{Z}_n$ perché è caratteristico. Ma allora:

$$\begin{array}{ccc} {}^{\mathbb{Z} \times \mathbb{Z}_n}\!/_{\{0\} \times \mathbb{Z}_n} & \xrightarrow{\overline{\varphi}} & {}^{\mathbb{Z} \times \mathbb{Z}_n}\!/_{\{0\} \times \mathbb{Z}_n} \\ \cong \downarrow & & \cong \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z} \end{array}$$

Dunque, conoscendo gli automorfismi di $\mathbb{Z}$, che sono solo $\pm id$, abbiamo completamente determinato l'automorfismo. Rappresentiamo con una simil-matrice come possiamo costruirlo:

$$\left(\begin{array}{c|c} \overline{\varphi}(1, \overline{0}) & 0 \\ \hline \varphi(1, \overline{0}) = * \in \mathbb{Z}_n & \varphi(0, \overline{1}) = a \in \mathbb{Z}_n^* \end{array} \right)$$

Dove sulla prima riga considero le componenti lungo $\mathbb{Z}$ e sulla seconda le componenti lungo $\mathbb{Z}_n$ (lo zero in alto a destra è motivato dal fatto che l'immagine di $(0, 1)$ ha ordine finito). Questi mi determinano completamente l'automorfismo, dunque $|Aut(\mathbb{Z} \times \mathbb{Z}_n)| = 2n\varphi(n)$

Osservazione 20. *Sia G un gruppo abeliano e sia*

$$\begin{aligned} \psi_n &\colon G \to G \\ x &\mapsto x^n \end{aligned}$$

Preso un qualunque $\varphi \in Aut(G)$ il seguente diagramma commuta:

$$\begin{array}{ccc} G & \xrightarrow{\psi_n} & G \\ \varphi \downarrow & & \downarrow \varphi \\ G & \xrightarrow[\psi_n]{} & G \end{array}$$

E di conseguenza $\mathrm{Ker}(\psi_n)$ *e* $\psi_n(G)$ *sono caratteristici in G.*

Esempio 9. *Descrivere* $Aut(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4)$

Esempio 10. $G = Q_8 \times D_4,\ Z(G) = ?$

Il centro del prodotto è il prodotto dei centri e dunque $Z(G) = Z(Q_8) \times Z(D_4) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Esempio 11. *Determinare* $Aut(Q_8),\ Aut(D_4),\ Aut(Q_8 \times D_4)$.

I prodotti semidiretti.

Definizione 13 (Prodotto semidiretto)**.** *Siano H e K gruppi e sia:*

$$\begin{aligned}\varphi\colon K &\to Aut(H)\\ k &\mapsto \varphi_k\end{aligned}$$

un omomorfismo. Si definisce prodotto semidiretto di H e K via φ ($H \rtimes_\varphi K$) il prodotto cartesiano $H \times K$ con operazione definita da

$$(h,k)(h',k') = (h\varphi_k(h'), kk')$$

Proposizione 13. *$H \rtimes_\varphi K$ è un gruppo.*

Dimostrazione. Dobbiamo fare le verifiche:

- Chiusura rispetto all'operazione: facile da controllare, $kk' \in K, h\varphi_k(h') \in H$;
- L'operazione è associativa;
- (e_H, e_K) è l'elemento neutro: $(h,k)(e_H,e_K) = (h\varphi_k(e_H), ke_K) = (h,k)$; $(e_H,e_K)(h,k) = (e_H\varphi_{e_K}(h), e_Kk) = (\varphi_{e_K}(h),k)$, ma $\varphi_{e_K} = \varphi(e_K)$ ed essendo φ un omomorfismo, ho che $\varphi(e_K) = id \implies \varphi_{e_K}(h) = h$;
- Esistenza dell'inverso: $(h,k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) = (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) = (hh^{-1}, kk^{-1}) = (e_H, e_K)$. Poiché φ è omomorfismo, $\varphi(k^{-1}) = (\varphi(k))^{-1} \implies \varphi_{k^{-1}} = (\varphi_k)^{-1}$

□

Osservazione 21. *Il prodotto diretto è un caso particolare del prodotto semidiretto. Il caso è quello in cui φ è banale, cioè $\varphi(k) = id\ \forall k \in K$.*

Osservazione 22. *$\overline{H} = H \times \{e_K\}$, $\overline{K} = \{e_H\} \times K$. Allora $\overline{H} \triangleleft H \rtimes K, \overline{K} \triangleleft H \times K$.*
$\overline{H} \triangleleft H \rtimes_\varphi K$ poiché:

$$\begin{aligned}\Pi_K\colon H \rtimes_\varphi K &\to K\\ (h,k) &\mapsto k\end{aligned}$$

è un omomorfismo e $\overline{H} = \mathrm{Ker}(\Pi_K)$. In generale $\overline{K}$ non è normale in $H \rtimes_\varphi K$, ma vale che $\overline{K} \triangleleft H \rtimes_\varphi K \iff$ il prodotto è diretto. Comunque $K < H \rtimes_\varphi K$.

Teorema 9 (Teorema di decomposizione in prodotto semidiretto)**.** *Sia G un gruppo, supponiamo $H, K < G$ con $H \triangleleft G$. Supponiamo anche che $HK = G$ e che $H \cap K = \{e\}$. Allora $G \cong H \rtimes_\varphi K$ dove*

$$\begin{aligned}\varphi\colon K &\to Aut(H)\\ k \mapsto \varphi_k : H &\to H\\ h &\mapsto khk^{-1}\end{aligned}$$

Dimostrazione. Una volta verificato che φ_k è ben definita, consideriamo:

$$\begin{aligned}F : H \rtimes_\varphi K &\to G\\ (h,k) &\mapsto hk\end{aligned}$$

- F è un omomorfismo: $F((h,k)(h',k')) = F((h,\varphi_k(h'),kk') = h\varphi_k(h')kk' = hkh'k^{-1}kk' = hkh'k' = F((h,k))F((h',k'))$;
- F è surgettivo: ovvio perché $HK = G$;
- F è iniettivo: $F(h,k) = hk = e \implies k = h^{-1} \implies k \in H \cap K = \{e\} \implies k = h = e$.

□

Esempio 12. *$S_n \cong A_n \rtimes_\varphi (1\ 2)$ dove:*

$$\begin{aligned}\varphi\colon \langle(1\ 2)\rangle &\to Aut(A_n)\\ (1\ 2) &\mapsto \varphi_{(1\ 2)}(\sigma) = (1\ 2)\sigma(1\ 2)\end{aligned}$$

Esempio 13. *$D_n \cong \langle\rho\rangle \rtimes_\varphi \langle\sigma\rangle$ dove:*

$$\begin{aligned}\varphi\colon \langle\sigma\rangle &\to Aut(\langle\rho\rangle)\\ \sigma &\mapsto \varphi_\sigma(\rho) = \sigma\rho\sigma = \rho^{-1}\end{aligned}$$

Esempio 14. *Consideriamo $\mathbb{Z}_5 \rtimes_\varphi \mathbb{Z}_3$. Ci chiediamo a cosa può essere isomorfo questo gruppo. Notiamo però che può essere solo $\mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$ poiché $(3, \Phi(5)) = (3, 4) = 1 \implies \varphi(1) = id \implies \varphi$ è banale.*

Cerchiamo di generalizzare quello che è venuto fuori da questo esempio.

Proposizione 14. *Sia G un gruppo, $|G| = pq, p$ e q primi.*

- *$p = q \implies |G| = p^2 \implies G \cong \mathbb{Z}_{p^2} \vee G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ poiché abeliano.*
- *$p \neq q$. Supponiamo $p > q$. Se $q \nmid p - 1 \implies \exists$ un unico gruppo a meno di isomorfismo di ordine pq, $\mathbb{Z}_{pq}$. Se $q | p - 1 \implies \exists$ due gruppi a meno di isomorfismo: uno è $\mathbb{Z}_{pq}$, l'altro è non abeliano.*

Dimostrazione. Per Cauchy $\exists$ due sottogruppi di ordine p, q, chiamiamoli rispettivamente N_p e N_q. Abbiamo che $N_p \cong \mathbb{Z}_p$ e $N_q \cong \mathbb{Z}_q$. Poiché $[G : N_p] = q$ e q è il più piccolo primo che divide l'ordine di G, allora $N_p \triangleleft G$. Inoltre $p \neq q \implies N_p \cap N_q = \{e\}$. Si ha anche che, per questioni di cardinalità, $N_p N_q = G$. Per questo motivo dunque possiamo dire che $G \cong N_p \rtimes_{c_G} N_q$ dove:

$$\begin{aligned} c_G \colon N_q &\to Aut(N_p) \\ h &\mapsto \varphi_h \mid \varphi_h(k) = khk^{-1} \end{aligned}$$

Studiamo ora gli automorfismi $\tau \colon \mathbb{Z}_q \to Aut(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.

($q \nmid p - 1$) L'unico τ che posso costruire è quello che manda ogni elemento di $\mathbb{Z}_q$ in $[0]$ di $\mathbb{Z}_{p-1}$. Infatti l'immagine di un generatore di $\mathbb{Z}_q$ deve avere ordine che divide q, dunque o 1 o q. Ma poiché $q \nmid p - 1$ significa che in $\mathbb{Z}_{p-1}$ non ci sono elementi di ordine q e di conseguenza $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

($q \mid p - 1$) Allora ho diverse possibilità. Consideriamo un omomorfismo da $\mathbb{Z}_q \to \mathbb{Z}_{p-1} \cong Aut(\mathbb{Z}_p)$. Questo è completamente determinato dall'immagine di $[1]_q$ che può avere ordine 1 oppure q. Se ha ordine 1 siamo nel caso dell'automorfismo banale e dunque ci si riconduce al caso del prodotto diretto. Altrimenti possiamo scegliere l'immagine come:

$$\left[\frac{p-1}{q}\right]_{p-1}, 2\left[\frac{p-1}{q}\right]_{p-1}, \dots, (q-1)\left[\frac{p-1}{q}\right]_{p-1}$$

che sono tutti e soli gli elementi di ordine q in $\mathbb{Z}_{p-1}$. Abbiamo dunque $q - 1$ omomorfismi non banali che mi inducono un prodotto semidiretto, e li chiamiamo per comodità $\Phi_1, \dots, \Phi_{q-1}$. Prendiamo ora Φ_1, Φ_j con $1 \neq j$. Consideriamo $\alpha = id \in Aut(\mathbb{Z}_p)$ e $\forall j \in \{1, \dots, q-1\},\ B_j \in Aut(\mathbb{Z}_q) \mid B_j([1]_q) = [j]_q$.

Dobbiamo verificare che $\Phi_j([1]_q)$ e $\Phi_1(B_j([1]_q))$ coincidono e poi sfruttare questo lemma:

Lemma 2. *Dati due gruppi H, K, siano $\varphi, \psi \colon K \to Aut(H)$ due omomorfismi. Se esistono $\alpha \in Aut(H)$ e $\beta \in Aut(K)$ tali che:*

$$\alpha \circ \varphi(k) \circ \alpha^{-1} = \psi(\beta(k)) \quad \forall k \in K$$

allora $H \rtimes_\varphi K \cong H \rtimes_\psi K$.

Dimostrazione. Consideriamo la seguente mappa:

$$\begin{aligned} \Xi \colon H \rtimes_\varphi K &\to H \rtimes_\psi K \\ (h, k) &\mapsto (\alpha(h), \beta(k)) \end{aligned}$$

e mostriamo che si tratta di un isomorfismo. Innanzitutto facciamo vedere che è un omomorfismo:

$$\begin{aligned} \Xi((h,k)(h',k')) &= \Xi(h\varphi(k)(h'), kk') = (\alpha(h) \cdot (\alpha \circ \varphi(k))(h'), \beta(k)\beta(k')) \\ &= (\alpha(h) \cdot (\psi(\beta(k)) \circ \alpha)(h'), \beta(k)\beta(k')) \\ &= (\alpha(h), \beta(k))(\alpha(h'), \beta(k')) = \Xi(h,k) \cdot \Xi(h',k') \end{aligned}$$

L'iniettività segue da:

$$\Xi((h,k)) = (e_H, e_K) \iff (\alpha(h), \beta(k)) = (e_H, e_K) \iff (h,k) = (e_H, e_K)$$

dove l'ultima equivalenza vale per l'iniettività di α e di β. Analogamente la surgettività deriva dal fatto che α e β sono automorfismi. □

Abbiamo che:

$$\Phi_j([1]_p) = j\left[\frac{p-1}{q}\right]_{p-1} = \Phi_1([j]_q) = \Phi_1(\beta_j[1]_q))$$

Esistono dunque al più due gruppi di ordine pq. Uno è $\mathbb{Z}_p \times \mathbb{Z}_q$ e l'altro è $\mathbb{Z}_p \rtimes_\tau \mathbb{Z}_q$. Dimostriamo che sono distinti mostrando che $\mathbb{Z}_p \rtimes_\tau \mathbb{Z}_q$ non è abeliano con $\tau = \Phi_i$ per qualche i.

Siano $a \in \mathbb{Z}_p, b \in \mathbb{Z}_q$, allora:

$$(a,b)(0,b) = (a + \tau(b)(0), 2b) = (a, 2b)$$
$$(0,b)(a,b) = (0 + \tau(b)(a), 2b) = (\tau(b)(a), 2b)$$

Poiché τ non è banale, $\exists b \in \mathbb{Z}_q | \tau(b) \neq id \implies \exists a | \tau(b)(a) \neq a$. Dunque $(a,b)(0,b) \neq (0,b)(a,b) \implies \mathbb{Z}_p \rtimes_\tau \mathbb{Z}_q \ncong \mathbb{Z}_p \times \mathbb{Z}_q$ poiché non è abeliano.

□

Esercizio 6. $|Z_{S_n}(\sigma)| \cdot |Cl_{S_n}(\sigma)| = n!$

$$\sigma \in A_n \implies |Z_{A_n}(\sigma)| \cdot |Cl_{A_n}(\sigma)| = \frac{n!}{2} \qquad Z_{A_n}(\sigma) = \{\rho \in A_n | \rho\sigma\rho^{-1} = \sigma\} = Z_{S_n}(\sigma) \cap A$$

Lemma 3. $H < S_n \implies |H \cap A_n| = \begin{cases} |H| & \text{se } H \subset A_n \\ \frac{|H|}{2} & \text{se } H \not\subset A_n \end{cases}$

Dimostrazione.

$$H \hookrightarrow S_n \twoheadrightarrow {}^{S_n}\!/_{A_n} \cong \mathbb{Z}_2 \qquad (\varphi)$$

$\operatorname{Ker}\varphi = H \cap A_n \implies {}^{H}\!/_{\operatorname{Ker}\varphi} \hookrightarrow \{\pm 1\} \implies \left|{}^{H}\!/_{H \cap A_n}\right| = \begin{cases} 1 & \text{se } H \subseteq A_n \\ 2 & \text{se } H \not\subset A_n \end{cases}$

Da cui segue che $Z_{A_n}(\sigma) = Z_{S_n}(\sigma) \ \vee$ ha cardinalità $\frac{|Z_{S_n}(\sigma)|}{2}$.
Supponiamo che $Z_{S_n} = Z_{A_n}$, allora $|Cl_{A_n}(\sigma)| = \frac{1}{2}|Cl_{S_n}(\sigma)|$;
Se invece $|Z_{S_n}(\sigma)| = 2|Z_{A_n}(\sigma)| \implies |Cl_{A_n}(\sigma)| = |Cl_{S_n}(\sigma)|$ e di conseguenza si ha $Cl_{A_n}(\sigma) = Cl_{S_n}(\sigma)$ poiché $Cl_{A_n}(\sigma) \subseteq Cl_{S_n}(\sigma)$ □

Esercizio 7. *I* $3-$*cicli sono tutti coniugati in* A_n *per* $n \geq 5$.

Esercizio 8. *I* $5-$*cicli non sono tutti coniugati in* A_5.

Esercizio 9. A_4 *non ha sottogruppi di ordine* 6.

Teoremi di Sylow e conseguenze.

Teorema 10 (Teorema di Sylow)**.** *Sia G un gruppo finito, p un numero primo, $|G| = p^n m,\ (m,p) = 1$. Allora valgono i seguenti fatti:*

Esistenza: $\forall\ 0 \leq \alpha \leq n\ \exists H < G \mid |H| = p^\alpha$*;*

Inclusione: Ogni p-sottogruppo di G è contenuto in un p-Sylow. (in generale vale anche che se $H < G \mid o(H) = p^\alpha\ 0 \leq \alpha \leq n \implies H$ è contenuto in un sottogruppo di G di ordine $p^{\alpha+1}$, ma non lo dimostriamo);

Coniugio: Due p-Sylow sono coniugati;

Numero: Se chiamo $n_p = \#p\text{-}Sylow \implies n_p | o(G) \wedge n_p \equiv 1 \mod (p)$.

Dimostrazione.

Esistenza: Fisso α e considero $\mathcal{M} = \{M \subset G \mid |M| = p^\alpha\}$.

$$|\mathcal{M}| = \binom{p^n m}{p^\alpha} = \frac{(p^n m)!}{p^\alpha!(p^n m - p^\alpha)!} = \frac{p^n m \cdot \prod_{i=1}^{p^\alpha - 1}(p^n m - i)}{p^\alpha \cdot \prod_{i=1}^{p^\alpha - 1}(p^\alpha - i)} = p^{n-\alpha} m \cdot \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$$

Abbiamo che $p^{n-\alpha} || \mathcal{M}|$ e non ci sono altri fattori: infatti, se indichiamo con v_p la valutazione p-adica, $\forall i \in \{1, \dots, p^{\alpha-1}\},\ v_p(p^n m - i) = v_p(p^\alpha - i) = v_p(i)$.

$$v_p\left(\frac{p^n m - i}{p^\alpha - i}\right) = 0 \implies p \not| \frac{p^n m - i}{p^\alpha - i} \implies p^{n-\alpha} \parallel |\mathcal{M}|$$

Consideriamo ora l'azione di G su $\mathcal{M}$ data da:

$$\begin{aligned} \Phi \colon G &\to S(\mathcal{M}) \\ g &\mapsto \varphi_g : M \mapsto gM \end{aligned}$$

Allora, chiamato R un insieme di rappresentanti:

$$|\mathcal{M}| = \sum_{M_i \in R} |orb(M_i)| = \sum_{M_i \in R} \frac{|G|}{|Stab(M_i)|}$$

Dico ora che esiste un M_i tale che $|Stab(M_i)| = p^\alpha$. Poiché $p^{n-\alpha} \parallel |\mathcal{M}| \implies$ non tutte le orbite hanno cardinalità multipla di $p^{n-\alpha+1}$. Dunque:

$$\exists i \text{ t.c. } p^{n-\alpha+1} \not| |orb(M_i)| = \frac{|G|}{|Stab(M_i)|} = \frac{p^n m}{|Stab(M_i)|} \implies p^\alpha \mid |Stab(M_i)|$$

Sia ora $x \in M_i$ e consideriamo la funzione:

$$\begin{aligned} f \colon Stab(M_i) &\to M_i \\ y &\mapsto yx \end{aligned}$$

e notiamo che chiaramente $yx \in M_i$ poiché y stabilizza M_i. Questa è una funzione iniettiva poiché, per la legge di cancellazione, $yx = y'x \iff y = y'$.
Ma allora $|M_i| = p^\alpha \implies |Stab(M_i)| \leq p^\alpha \wedge p^\alpha \mid |Stab(M_i)| \implies |Stab(M_i)| = p^\alpha$.

Inclusione: $H < G | o(H) = p^\alpha$, S p-Sylow di G. Definiamo X come ${}^{G}\!/_{S}$ che, notiamo bene, non è un gruppo ma solo l'insieme delle classi laterali di S in G. Definiamo ora:

$$\begin{aligned} F \colon H &\to S(X) \\ h &\mapsto \varphi_h : gS \mapsto hgS \end{aligned}$$

e notiamo che questa è una azione di H su X (verificare!).

$$m = |X| = [G : S] = \sum_{g_i \in R} |orb(g_i S)| = \sum_{g_i \in R} \frac{|H|}{|Stab(g_i S)|} = \sum_{g_i \in R} \underbrace{\frac{p^\alpha}{|Stab(g_i S)|}}_{p^{n_i}} \implies m = |X| = \sum_i p^{n_i}$$

E poiché $p \not| m,\ \exists i : n_i = 0, p^{n_i} = 1$. Dunque $|Stab(g_i S)| = p^\alpha \implies Stab(g_i S) = H$, inoltre $\forall h \in H, hg_i S = g_i S \implies \forall h \in H, h \in g_i S g_i^{-1} \iff H \subset g_i S g_i^{-1}$ che, essendo il coniugato di un p-Sylow, è ancora un p-Sylow.

Coniugio: H, S p-Sylow di G. Per la parte precedente applicata ad H ho che $\exists g \in G | H \subset gSg^{-1} \implies$ per cardinalità allora $H = gSg^{-1}$.

Numero: Sia S un p-Sylow. $n_p = \#p\text{-Sylow} = \#\text{coniugati di } S \text{ in } G = [G : N_G(S)] \mid |G|$ che è un divisore di $|G|$ coprimo con p. Se denotiamo con Y l'insieme dei coniugati di S in G, allora possiamo considerare questa azione:

$$\begin{aligned} g &\colon S \to S(Y) \\ g &\mapsto \varphi_g : xSx^{-1} \mapsto gxSx^{-1}g^{-1} \end{aligned}$$

Dico che l'orbita di S è l'unica orbita banale di questa azione: se $H \in Y$ e $orb(H) = \{H\} \implies Stab(H) = \{s \in S | sHs^{-1} = H\} = S \iff S \in N_G(H) \iff SH = HS \iff HS < G$, impossibile poiché S era un p-gruppo massimale:

$$|HS| = \frac{|H||S|}{|H \cap S|} = \frac{p^n p^n}{|H \cap S|} \qquad HS < G \implies |HS| \mid |G| \implies H = S$$

Dunque:

$$|Y| = n_p = \sum_{H \in R} |orb(H)| = |orb(S)| + \sum_{H \in R \setminus \{S\}} |orb(H)| = 1 + \sum_{H \in R \setminus \{S\}} \frac{|S|}{|Stab(H)|}$$

Poiché $|S| = p^n$ e $|Stab(H)| = p^{\alpha_i}$ poiché l'orbita è non banale, segue che $n_p = pk + 1 \implies n_p \equiv 1 \mod (p)$.

□

Teorema 11. *G gruppo abeliano finito $\implies$ G è prodotto diretto dei suoi p-Sylow.*

Dimostrazione. $|G| = p_1^{e_1} \dots p_r^{e_r}$. Proseguiamo per induzione su r.

- Se $r = 1$, G è un p_1-gruppo.
- Passo induttivo: Sia $d \mid |G|$ e definiamo $G_d = \{x \in G | dx = 0\}$. Consideriamo la seguente applicazione:

$$\begin{aligned} \varphi_d &\colon G \to G \\ x &\mapsto dx \end{aligned}$$

Poiché $G_d = \mathrm{Ker}(\varphi_d) \implies G_d < G$. Denotiamo per comodità $G_{p_r}^{e_r}$ come G_{p^e}. Allora $|G| = p_e m$ e dunque m ha $r - 1$ fattori primi distinti. Sicuramente G_{p^e} è un p-gruppo poiché $G_{p^e} = \{g \in G | p^e g = 0\}$. Notiamo inoltre che se $q || G_{p^e}$ per Cauchy $\exists y \in G_{p^e}, o(y) = q \implies q = p$.

G_{p^e} è un p-Sylow. Se S è un p-Sylow di $G \implies |S| = p^e \implies S \subset G_{p^e} \implies S = G_{p^e}$

Voglio ora dimostrare che $G \cong G_{p^e} \times G_m$ e applicare l'ipotesi induttiva su G_m. $G_{p^e}, G_m \triangleleft G$ è banale poiché G è abeliano. Inoltre $G_{p^e} \cap G_m = \{0\}$. Dobbiamo dunque verificare che $G_{p^e} + G_m = G$ (sto usando la notazione additiva come è solito fare nei gruppi abeliani). La prima inclusione è ovvia, dimostriamo invece che $G \subset G_{p^e} + G_m$.

Poiché $(p^e, m) = 1$ si ha che $\exists a, b \in \mathbb{Z} | ap^e + bm = 1$. Allora $g \in G, g = ap^e g + bmg = ax + by$. Chiaramente $x \in G_m$ poiché $mx = 0 = \underbrace{mp^e}_{o(G)} g$ e $y \in G_{p^e}$ perché $p^e y = p^e mg = 0$. Allora ho finito poiché:

$$G \cong G_{p^e} \times G_m = G_{p_1}^{e_1} \times G_{p_2}^{e_2} \times \dots \times G_{p_r}^{e_r}$$

□

Esempio 15. *Se $G \cong S_4$, $|G| = 2^3 \cdot 3$. Sia P un 2-Sylow di S_4. Allora $|P| = 8$ e necessariamente $P \cong D_4$ poiché tutti i p-Sylow sono isomorfi tra loro e D_4 si immerge naturalmente in S_4.*

Classificazione dei gruppi di ordine 12.
$|G| = 12 = 2^2 \cdot 3$.

$$n_3 \equiv 1 \mod (3) \wedge n_3 | 12 \implies n_3 = 1, 4; \quad n_2 \equiv 1 \mod (2) \wedge n_2 | 12 \implies n_2 = 1, 3.$$

G ha almeno un sottogruppo normale tra i 2-Sylow e i 3-Sylow. Siano P_2 e P_3 rispettivamente un 2-Sylow e un 3-Sylow. Allora:

$$P_2 \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} \\ \text{oppure} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases} \qquad P_3 \cong \mathbb{Z}/3\mathbb{Z}$$

Analizziamo i diversi casi:

Abeliani: $G \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$
$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$

Non abeliani:

- **2-Sylow normale.**

  $G = \mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_3$
  $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \rtimes_\varphi \mathbb{Z}_3$

  Nel primo caso notiamo che esiste un unico omomorfismo da $\mathbb{Z}_3$ in $Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$ ed è proprio quello che manda il generatore nell'identità, dunque φ è l'automorfismo banale e ci in realtà questo è il prodotto diretto $\mathbb{Z}_4 \times \mathbb{Z}_3$ già visto sopra.

  Nel secondo caso considero gli automorfismi da $\mathbb{Z}_3 \to Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$ e noto che posso mandare 1 in σ, σ^2. I gruppi che otteniamo con le due scelte sono isomorfi. Infatti consideriamo l'immersione di G in S_4 e facciamo agire G sui 3-Sylow (ricordiamo infatti che $n_3 = 4$). $P_3 = N(P_3)$, infatti $\varphi_g(P) = gPg^{-1} = P \iff g \in P$. $\varphi_g(P) = P \ \forall P$3-Sylow $\implies g \in \bigcap P = \{e\}$.
  Poiché A_4 è l'unico sottogruppo di ordine 12 di S_4, allora $\mathbb{Z}_2 \times \mathbb{Z}_2 \rtimes_\varphi \mathbb{Z}_3 \cong A_4$.

- **3-Sylow normale.**

  $G \cong Z_3 \rtimes_\varphi \mathbb{Z}_4$
  $G \cong \mathbb{Z}_3 \rtimes_\varphi (\mathbb{Z}_2 \times \mathbb{Z}_2)$

  Nel primo caso consideriamo gli omomorfismi da $\mathbb{Z}_4 \to Aut(\mathbb{Z}_3) \cong \mathbb{Z}_2$, e poiché abbiamo già escluso il caso banale, siamo costretti a mandare 1 in $-id$ ottenendo così un nuovo gruppo, $Z_3 \rtimes_\varphi \mathbb{Z}_4$.

  Nel secondo caso invece devo considerare gli omomorfismi da $\mathbb{Z}_2 \times \mathbb{Z}_2 \to Aut(\mathbb{Z}_3) \cong \{\pm id\}$. Nonostante io abbia due scelte per i tre elementi di ordine due, ho solo due casi disponibili: se mando i generatori nell'identità chiaramente ottengo di nuovo $\mathbb{Z}_6 \times \mathbb{Z}_2$, mentre in ogni altro caso avrò sempre che due elementi saranno mandati in $-id$ e un altro in id e di conseguenza ottengo che $G \cong \mathbb{Z}_6 \rtimes_\varphi \mathbb{Z}_2 \cong D_6$.

Il teorema di struttura, lemmi ed esercizi.

Teorema 12 (Teorema di struttura per gruppi abeliani finiti)**.** *Sia G un gruppo abeliano finito. Allora G è prodotto diretto di gruppi ciclici:*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

con $n_s \mid n_{s-1} \mid \ldots \mid n_1$. Inoltre tale scrittura è unica.

Esempio 16. $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$.

Proposizione 15. *Sia G finitamente generato e abeliano, definiamo $T = \{x \in G | o(x) < \infty\}$. Gli elementi di T sono detti di torsione. Si ha:*

- *$T < G$ se G è abeliano;*
- *Se G non è abeliano G/T non ha elementi di torsione e $G \cong T \times G/T$ con $G/T \cong \mathbb{Z}^k$*

Dimostrazione. $\forall p \mid |G| \implies G_{(p)} = \{x \in G \mid p^k x = 0 \text{ per qualche } k\}$ è un p-Sylow, $G_{(p)} \triangleleft G$ perché nucleo dell'omomorfismo moltiplicazione per p^k (che è un omomorfismo poiché G è abeliano). Poiché G è abeliano si ha che questo è l'unico p-Sylow (tutti gli elementi verificano $p^k x = 0$). □

Teorema 13 (1)**.** *G gruppo, G abeliano finito $\implies G \cong G_{(p_1)} \times \cdots \times G_{(p_m)}$.*

Dimostrazione. La decomposizione è unica a meno dell'ordine dei fattori: c'è un solo p-Sylow $\forall p_i, i = 1, \ldots, m$ perché G è abeliano. □

Teorema 14 (2)**.** *Sia G un p-gruppo abeliano. Esistono e sono univocamente determinati $r_1 \geq r_2 \geq \cdots \geq r_t$ tali che:*

$$G \cong \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_t}}$$

Dimostrazione. Proseguiamo per induzione su n con $|G| = p^n$.

Esistenza: $|G| = p^n$; se $n = 1$ allora $|G| = p$ e $G \cong \mathbb{Z}_p$. Se invece $n > 1$ considero $x_1 \in G$ tale che $ord(x_1) = p^{r_1}$ con p^{r_1} massimo ordine possibile in G. Considero ora $\langle x_1 \rangle < G$ e il quoziente $G/\langle x_1 \rangle$. Per ipotesi induttiva:

$$G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \cdots \times \langle \overline{x_s} \rangle$$

con $ord(\overline{x_i}) = p^{r_i}$. Consideriamo ora la proiezione $\pi \colon G \to G/\langle x_1 \rangle$.

Claim: $\forall\, \overline{x} \in G/\langle x_1 \rangle\ \exists y \in \pi^{-1}(\overline{x})$ t.c. $o(y) = o(\overline{x})$ e questo è vero perché p^{r_1} è l'ordine massimo.

□

Dimostrazione del teorema di struttura. **Esistenza:** Per il teorema (1) si ha che $G \cong G_{(p_1)} \times \cdots \times G_{(p_m)}$. Utilizziamo il teorema (2) per decomporre ulteriormente G. Otteniamo:

$$\begin{array}{rccccc}
G \cong & G_{(p_1)} & \times & \ldots & \times & G_{(p_m)} \\
\cong & \mathbb{Z}/p_1^{r_{11}}\mathbb{Z} & \times & \ldots & \times & \mathbb{Z}/p_1^{r_{1t_1}}\mathbb{Z} \\
& \ldots & \times & \ldots & \times & \ldots \\
& \mathbb{Z}/p_m^{r_{m_1}}\mathbb{Z} & \times & \ldots & \times & \mathbb{Z}/p_m^{r_{mt_m}}\mathbb{Z} \\
& \downarrow \text{TCR} & & \downarrow \text{TCR} & & \downarrow \text{TCR} \\
& \mathbb{Z}/n_1\mathbb{Z} & \times & \ldots & \times & \mathbb{Z}/r_m\mathbb{Z}
\end{array}$$

Dove nella seconda riga abbiamo $r_{i_1} \geq r_{i_2} \geq \ldots r_{i_{t_i}}$ e nell'ultima $n_m \mid n_{m-1} \mid \ldots \mid n_1$.

Unicità: Se avessi due scritture diverse potrei spezzarle al massimo ripercorrendo gli isomorfismi al contrario e avrei due scritture diverse per almeno uno dei p-Sylow. Ma questo è assurdo proprio per il teorema (2). □

Esempio 17. $G \cong \mathbb{Z}_{16} \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_{120} \times \mathbb{Z}_{12} \times \mathbb{Z}_4 \times \mathbb{Z}_2$

Dimostrazione teorema (2). Procediamo per induzione su n con $|G| = p^n$.

Esistenza: $|G| = p^n$. Se $n = 1$ allora $|G| = p$ e $G \cong \mathbb{Z}_p$.

Sia dunque $n > 1$. Sia $x_1 \in G$ tale che $o(x_1) = p^{r_1}$ con p^{r_1} massimo ordine possibile in G. Consideriamo $\langle x_1 \rangle < G$ e il quoziente, $G/\langle x_1 \rangle$. Per ipotesi induttiva:

$$G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \cdots \times \langle \overline{x_s} \rangle \qquad \text{dove } o(\overline{x_i}) = p^{r_i}$$

Consideriamo la proiezione $\pi \colon G \to G/\langle x_1 \rangle$.

Claim: $\forall \overline{x} \in {}^{G}\!/_{\langle x_1 \rangle}\ \exists y \in \pi^{-1}(\overline{x}) \mid o(y) = o(\overline{x})$ e questo è vero poiché p^{r_1} è l'ordine massimo.

Sia dunque $p^r = o(\overline{x}), \pi(y) = \overline{x}$. Si ha $\pi(p^r y) = p^r \overline{x} = \overline{0}, p^r y \in \langle x_1 \rangle$. Dunque $\exists a \in \mathbb{Z} \mid p^r y = a x_1$.

$$0 = p^{r_1} y = p^{r_1 - r}(p^r y) = \underbrace{p^{r_1 - r} a x_1}_{p^{r_1} | p^{r_1 - r} a}$$

Ma $o(x_1) = p^{r_1}$ è l'ordine massimo in G e dunque $p^r | a = p^r a'$. Considero ora $y - a' x_1$. $\pi(y - a' x_1) = \pi(y) = x, p^r(y - a' x_1) = p^r y - a x_1 = 0 \implies o(y - a' x_1) = p^r$.

$\exists x_2, \dots, x_s \in G \mid o(x_i) = o(\overline{x_i}) = p^{r_i} \forall i = 2, \dots, s$.

$$\pi \colon G \to {}^{G}\!/_{\langle x_1 \rangle} \cong \langle \overline{x_2} \rangle \times \cdots \times \langle \overline{x_s} \rangle$$

Sia ora $\langle x_2, \dots, x_s \rangle = H < G$ e consideriamo la proiezione canonica π_H. π_H è bigettiva: è surgettiva poiché otteniamo tutti i generatori dei prodotti diretti ed è iniettiva perché:

$$\pi(a_2 x_2 + \cdots + a_s x_s) = (a_2 \overline{x_2}, \dots, a_s \overline{x_s}) = (\overline{0}, \dots, \overline{0}) \iff p^{r_i} | a_i\ \forall i \implies p^{r_i} x_i = 0 \implies \sum_{i=2}^{s} a_i x_i = 0$$

e di conseguenza $H = \langle x_2, \dots, x_s \rangle \cong \langle \overline{x_2} \rangle \times \cdots \times \langle \overline{x_s} \rangle$.

Claim: $G \cong \langle x_1 \rangle \times H$.

1) $\langle x_1 \rangle H = G$ oppure in notazione additiva $\langle x_1 \rangle + H = G$;

2) $\langle x_1 \rangle \cap H = \{e\}$ oppure in notazione additiva $\langle x_1 \rangle \cap H = \{0\}$.

1] $\forall g \in G, g = a_1 x_1 + h, h \in H, a \in Z$. Proietto in ${}^{G}\!/_{\langle x_1 \rangle}$ e ottengo $\overline{g} = \underbrace{a\overline{x_1}}_{=0} + \overline{h}$.

$$\forall g \in G, \overline{g} \in {}^{G}\!/_{\langle x_1 \rangle} = \langle \overline{x_2} \rangle \times \cdots \times \langle \overline{x_s} \rangle$$

$h = a_2 x_2 + \cdots + a_s x_s \implies \overline{g - h} = \overline{0} \implies g - h \in \langle x_1 \rangle \implies g = a x_1 + h$

2] $\langle x_1 \rangle \cap H = \{0\}$:

$$a_1 x_1 = a_2 x_2 + \dots a_s x_s \implies 0 = (a_2 \overline{x_2}, \dots, a_s \overline{x_s}) \implies p^{r_i} | a_i\ \forall i = 2, \dots, s$$
$$\implies a_i x_i = 0\ \forall i = 2, \dots, s \implies a_1 x_1 = 0 \implies G \cong \langle x_1 \rangle \times \cdots \times \langle x_s \rangle$$

dove ogni $\langle x_i \rangle$ ha cardinalità p^{r_i} con $r_2 \geq \cdots \geq r_s$. Poiché p^{r_1} è l'ordine massimo, $r_1 \geq r_2 \geq \cdots \geq r_s$.

Unicità: Procediamo per induzione su n.

Passo base) $G \cong \mathbb{Z}_p$

Passo induttivo) $G \cong \mathbb{Z}_{p^n} \implies G \cong \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_s}} \quad r_1 \geq r_2 \geq \cdots \geq r_s$. Supponiamo che si abbia anche $G \cong \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_t}}$ con $k_1 \geq k_2 \geq \cdots \geq k_t$. Dimostriamo dunque che si deve avere $s = t$.

$$G_p = \{x \in G \mid o(x) = p\} \qquad (\mathbb{Z}_p)^s \cong (\mathbb{Z}_p)^t \implies s = t$$

$$G \cong \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_s}} \cong \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_s}}$$

$$pG \cong \frac{p\mathbb{Z}}{p^{r_1}\mathbb{Z}} \times \cdots \times \frac{p\mathbb{Z}}{p^{r_s}\mathbb{Z}} \cong \mathbb{Z}_{p^{r_1 - 1}} \times \cdots \times \mathbb{Z}_{p^{r_s - 1}}$$
$$pG \cong \frac{p\mathbb{Z}}{p^{k_1}\mathbb{Z}} \times \cdots \times \frac{p\mathbb{Z}}{p^{k_s}\mathbb{Z}} \cong \mathbb{Z}_{p^{k_1 - 1}} \times \cdots \times \mathbb{Z}_{p^{k_s - 1}}$$

Per ipotesi induttiva si ha che pG ha scrittura unica, di conseguenza $r_i - 1 = k_i - 1\ \forall i \implies r_i = k_i\ \forall i$

□

Classificazione dei gruppi di ordine 30.

Quando n è square-free, c'è un unico gruppo ciclico di ordine n, in questo caso $\mathbb{Z}_{30}$. Sia dunque G tale che $|G| = 30 = 2 \cdot 3 \cdot 5$ e dimostriamo che se non è ciclico è isomorfo ad uno di questi tre gruppi: $D_{15}, D_5 \times \mathbb{Z}_3, D_3 \times \mathbb{Z}_5$.

$$n_5 | 6 \quad n_5 \equiv 1 \mod (5) \implies n_5 = 1, 6;$$
$$n_3 | 10 \quad n_3 \equiv 1 \mod (3) \implies n_3 = 1, 10;$$

Se P_5 non è normale, $n_5 = 6$. Di conseguenza ho $6 \cdot \varphi(5) = 24$ elementi di ordine 5. Necessariamente P_3 è normale per questioni di cardinalità. $P_3 \triangleleft G \implies P_5P_3 < G$.

In generale vale che se un sottogruppo è contenuto nel normalizzatore dell'altro, allora il loro prodotto è un sottogruppo. Inoltre $P_5P_3 \triangleleft G$ poiché ha indice 2 in G. Dunque P_5P_3 è un sottogruppo di ordine 15 e di conseguenza è ciclico.

$$x \in G, o(x) = 15 \implies G = \langle x \rangle \rtimes_\varphi \langle y \rangle \quad y \in G, o(y) = 2$$

$$\varphi \colon \langle y \rangle \to Aut(\langle x \rangle) \cong (\mathbb{Z}_{15})^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2$$
$$y \mapsto \varphi_y : x \mapsto yxy^{-1} = x^a$$

$\varphi_y^2 = id,\ \varphi_y^2(x) = x^{a^2} = x \implies a^2 \equiv 1 \mod (15) \implies a = \pm 1, \pm 4 \mod (15)$.

- $a = 1 \implies G \cong \mathbb{Z}_{30}$
- $a = -1 \implies G \cong D_{15}$
- $a = 4 \implies$ l'automorfismo fissa $\mathbb{Z}_3 \implies G \cong D_5 \times \mathbb{Z}_3$
- $a = -4 \implies$ l'automorfismo fissa $\mathbb{Z}_5 \implies G \cong D_3 \times \mathbb{Z}_5$

Esercizio 10.
- $H \triangleleft K, K \triangleleft G \implies H \triangleleft G$?
- *$H < K < G$ con H caratteristico in K e K caratteristico in $G \implies H < G$ caratteristico?*
- *$H < K \triangleleft G$ con H caratteristico in $K \implies H \triangleleft G$?*
- *$H \triangleleft K < G$ con K caratteristico in $G \implies H \triangleleft G$?*

Esercizio 11. *G gruppo, $o(G) = 2d$, d dispari. Allora $\exists H \triangleleft G \mid o(H) = d$. In particolare G non è semplice.*

Dimostrazione. Per il teorema di Cayley abbiamo un'immersione $G \hookrightarrow S_{2d}$ che ha come azione la moltiplicazione sinistra. Preso un generico elemento $g \in G$ conosciamo la decomposizione in cicli di φ_g che deve essere prodotto di cicli del tipo $(x, gx, g^2x, \ldots, g^{m-1}x)$ dove $m = o(g)$ e x varia in un insieme di rappresentanti. Per il teorema di Cauchy esiste un elemento y di ordine 2, dunque φ_y sarà prodotto di d cicli di lunghezza 2. Essendo questa una permutazione dispari, $\varphi_y \notin A_{2d} \implies |H| = d \wedge [G : H] = 2$ dove $H = G \cap A_{2d}$. □

Esercizio 12. *Sia G un gruppo semplice finito. Se $\exists H < G \mid [G : H] = n \implies G$ si immerge in A_n.*

Dimostrazione. Facendo agire G per moltiplicazione sinistra sui laterali di H otteniamo un omomorfismo $\Phi : G \to A_{2d}$ il cui nucleo deve essere banale per non contraddire la semplicità del gruppo. Di conseguenza, poiché l'omomorfismo non è sicuramente banale, questa è proprio un'immersione. □

Esercizio 13. *G gruppo, $H < G \mid [G : H] = n \implies \exists N \triangleleft G \mid |{}^{G}\!/_{N}| | n!, N \subset H$.*

Esercizio 14. *Un gruppo di ordine 112 non è semplice.*

Esercizio 15. *Un gruppo di ordine 144 non è semplice.*

Esercizio 16. *Dato un gruppo G di ordine p^3 non abeliano:*
- *Dimostrare che $|Z(G)| = p$;*
- *Dimostrare che $G' = Z(G)$;*
- *Contare il numero delle classi di coniugio.*

Esercizio 17. *Quanti sono i p-Sylow di $GL_n(\mathbb{F}_p)$?*

Esercizio 18. *Dimostrare che A_n è generato dai 3-cicli, che S_n può essere generato da un n-ciclo e un 2-ciclo e che A_n è il sottogruppo dei commutatori di S_n.*

Anelli e ideali.

Definizione 14. *Sia A un anello commutativo con identità. Allora, preso $x \in A$ si dice che:*

- *x è divisore di 0 se $\exists y \in A, y \neq 0$ tale che $(yx) = xy = 0$;*
- *x è nilpotente se $\exists n \in \mathbb{N}$ tale che $x^n = 0$;*
- *x è invertibile se $\exists y \in A$ tale che $xy = yx = 1$.*

Definizione 15 (Dominio d'integrità)**.** *A anello commutativo con unità si dice dominio di integrità se l'insieme D dei divisori di 0 di A è composto dal solo 0.*

Definizione 16 (Anello ridotto)**.** *A si dice ridotto se l'insieme degli elementi nilpotenti è composto dal solo 0.*

Proposizione 16. *Denotiamo con A^* l'insieme degli elementi invertibili di A. Allora vale che:*

1. *A^* è un gruppo moltiplicativo;*
2. *$A^* \cap D = \emptyset$;*
3. *Se A è finito, $A = A^* \cup D$.*

Dimostrazione. 2. $x \in A^* \cap D \implies \exists y, z, z \neq 0$ tali che $xy = 1, xz = 0$. Ma allora: $0 = 0 \cdot y = (zx)y = z(xy) = z \cdot 1 = z$, assurdo.

3. $x \in A, x \notin D$. Consideriamo $\varphi_x \colon A \to A$ tale che $\varphi_x(a) = xa$. Ma poiché $x \notin D$ si ha che $Ker(\varphi_x) = \{0\}$ dunque φ_x è surgettivo per cardinalità e quindi $1 \in Im(\varphi_x)$.

□

Corollario 3. *A è un dominio di integrità $\implies$ A è un campo.*

Esempio 18. *Consideriamo $\mathbb{K}[x]/(f(x))$ dove $(f(x)) = \{p(x)f(x) | p(x) \in \mathbb{K}[x]\}$.*
Ogni classe è del tipo $r(x) + (f(x))$ con $r(x) = 0 \vee deg(r) < deg(f)$.

$$\overline{r(x)} \text{ è divisore dello } 0 \iff (r(x), f(x)) \neq 1 \qquad \overline{r(x)} \text{è invertibile} \iff (r(x), f(x)) = 1$$

Definizione 17 (Ideale)**.** *$I \subset A$ è un ideale se $(I, +)$ è un sottogruppo e $\forall a \in A, aI \subset I$.*

Definizione 18 (Ideale generato)**.** *Sia $S \subset A$ non vuoto e consideriamo*

$$(S) = \left\{ \sum_{i=1}^{n} s_i a_i \mid n \in N, s_i \in S, a_i \in A \right\}$$

Si verifica che (S) è un ideale di A e si chiama ideale generato da S in A.

Osservazione 23.
- *Se A non è commutativo, si definisce ideale sinistro o ideale destro un sottogruppo additivo che assorbe la moltiplicazione per elementi di A rispettivamente a sinistra o a destra.*
- $(f(x)) = f(x)\mathbb{K}[x]$;
- $(s) = sA$.

Operazioni tra ideali. Siano $I, J \subset A$ ideali.

- $I \cup J$ in generale non è un ideale;
- $I \cap J$ è sempre un ideale;
- $I + J = \{i + j \mid i \in I, j \in J\}$ è un ideale;
- $IJ = \langle \{ij \mid i \in I, j \in J\} \rangle = \{\sum_{\alpha=1}^{n} i_\alpha j_\alpha \mid i_\alpha \in I, j_\alpha \in J\}$;
- $\sqrt{I} = r(I) = \{x \in A \mid x^n \in I \text{ per qualche } n \in \mathbb{N}\}$.

Osservazione 24. $\sqrt{\{0\}} = N$.

Definizione 19 (Ideale proprio)**.** *Sia $I \subset A$ un ideale. I si dice proprio se $I \neq A$.*

Proposizione 17. *I è un ideale proprio se e solo se $I \cap A^* = \emptyset$.*

Dimostrazione. $\implies$) I proprio $\implies I \subsetneq A \implies \exists a \in A \setminus I$. Se $\exists u \in I \cap A^* \implies 1 = \underbrace{u}_{\in I} \cdot \underbrace{u^{-1}}_{\in A} \in I \implies 1 \cdot a \in I$, assurdo.
$\impliedby$) $I \cap A^* = \emptyset \implies I \subsetneq A$ perché $1 \notin I$. □

Corollario 4. *In un campo $\mathbb{K}$ gli unici ideali sono $\{0\}$ e $\mathbb{K}$.*

Definizione 20 (Omomorfismo di anelli)**.** *Siano A, B anelli commutativi con identità. Si dice che $f\colon A \to B$ è un omomorfismo di anelli se $\forall a_1, a_2 \in A$:*

- $f(a_1 + a_2) = f(a_1) + f(a_2)$;
- $f(a_1 a_2) = f(a_1) f(a_2)$;
- $f(1_a) = 1_b$.

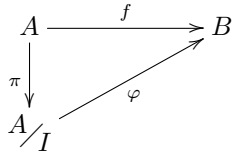
Definizione 21 (Quoziente)**.** *Se $I \subset A$ è un ideale, ${}^{A}\!/_{I}$ è un anello con la seguente operazione:*

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

Proposizione 18. *Gli ideali di A sono tutti e soli i nuclei degli omomorfismi.*

Dimostrazione. $I \subseteq A$ ideale $\implies I = Ker(\pi)$, dove $\pi\colon A \to {}^{A}\!/_{I}$ è la proiezione al quoziente. Prendiamo ora una generica $f\colon A \to B$ con A e B anelli e f omomorfismo. Notiamo che $Ker(f) = \{a \in A \mid f(a) = 0\}$ è un ideale di A: infatti se $a \in A$ e $x \in Ker(f)$ si ha $ax \in Ker(f)$ poiché $f(ax) = f(a)f(x) = 0$. □

Teorema 15 (Teorema di omomorfismo)**.** *Sia $f\colon A \to B$ un omomorfismo di anelli e sia $I = Ker(f)$. Allora $\exists!\ \varphi\colon {}^{A}\!/_{I} \to B$ tale che il seguente diagramma commuti:*



Inoltre φ è iniettivo e $\varphi\left({}^{A}\!/_{I}\right) = f(A)$.

Dimostrazione. C'è solo da verificare che l'unico omomorfismo di gruppi è anche omomorfismo di anelli, ossia che $\varphi(\overline{a}\overline{b}) = \varphi(\overline{a})\varphi(\overline{b})$. Ma vale:
$\varphi(a + I) = \varphi(\pi(a)) = f(a) \implies \varphi(\overline{a}\overline{b}) = \varphi(\pi(ab)) = f(ab) = f(a)f(b) = \varphi(\overline{a})\varphi(\overline{b})$.

□

Teorema 16 (Teorema di corrispondenza)**.** *Sia $\pi\colon A \to {}^{A}\!/_{I}$ la proiezione al quoziente. Allora π induce una corrispondenza biunivoca tra gli ideali di ${}^{A}\!/_{I}$ e gli ideali di A che contengono I. Inoltre questa corrispondenza conserva l'ordinamento, l'indice e gli ideali primi e massimali.*

$$\begin{aligned} \Phi\colon \{J \subset A \mid J \supset I\} &\longrightarrow \{J \subset {}^{A}\!/_{I}\} \\ J &\longmapsto {}^{J}\!/_{I} \\ \pi^{-1}(J) &\longleftarrow J \end{aligned}$$

Lemma 4. *Sia $f\colon A \to B$ un omomorfismo di anelli. Siano $I \subset A$ e $J \subset B$ due ideali. Allora:*

1) $f^{-1}(J)$ è un ideale di A;

2) $f(I)$ p un ideale di B se f è surgettiva.

Dimostrazione. Sappiamo già che $f^{-1}(J) < A$.

1) Sia $a \in A$. Devo dimostrare che $af^{-1}(J) \subset f^{-1}(J)$. Sia x un elemento di A tale che $f(x) \in (J)$. Si ha che: $ax \in f^{-1}(J) \implies f(ax) = \underbrace{f(a)}_{\in B}\underbrace{f(x)}_{\in J} \in J$ poiché J è un ideale.

2) $\forall y \in f(I),\ y = f(x),\ x \in I$ e $\forall b \in B,\ b = f(a),\ a \in A$ si ha che $by = f(a)f(x) = f(\underbrace{ax}_{\in I}) \in f(I)$.

□

Dimostrazione del teorema di corrispondenza. Sia $I \subset J \subset A$ un ideale. Allora:

$$\Phi(J) = {}^{J}\!/_{I} \subset {}^{A}\!/_{I} \qquad \text{Lemma (2)}$$

$$J \subset {}^{A}\!/_{I} \text{ ideale} \implies \Phi^{-1}(J) = \pi^{-1}(J) \subset A \text{ ideale} \qquad \text{Lemma (1)}$$

□

Osservazione 25. *I, J ideali, $IJ = \langle xy \mid x \in I, y \in J\rangle$. Notiamo che $IJ \subset I \cap J$ poiché $\forall i \in I, y \in Y$ si ha $xy \in I \cap J$.*

Esempio 19. *$I = J = 2\mathbb{Z}$. Allora $IJ = 4\mathbb{Z}$ e $I \cap J = 2\mathbb{Z}$.*

Lemma 5. *Se I, J sono ideali di A e $I + J = (1) = A$ allora $IJ = I \cap J$. In tal caso I e J si dicono comassimali.*

Dimostrazione. $\exists i \in I, j \in J$ tali che $1 = i + j$. Sia allora $x \in I \cap J$. Allora:

$$x = x \cdot 1 = x(i + j) = \underbrace{xi}_{\in IJ} + \underbrace{xj}_{\in IJ} \in IJ$$

. □

Teorema 17 (Teorema cinese)**.** *Siano $I, J \subset A$ ideali. Allora la mappa:*

$$\begin{aligned} f\colon A &\longrightarrow {}^{A}\!/_{I} \times {}^{A}\!/_{J} \\ a &\longmapsto (a + I, a + J) \end{aligned}$$

è un omomorfismo di anelli.

Si ha che $Ker(f) = I \cap J$ e che f è surgettiva $\iff I + J = A$. In tal caso si ha che:

$${}^{A}\!/_{IJ} \cong {}^{A}\!/_{I} \times {}^{A}\!/_{J}$$

Dimostrazione.

- f è un omomorfismo perché lo è sulle singole coordinate;
- $Ker(f) = \{a \in A \mid f(a) = (a + I, a + J) = (I, J) = (\overline{0}, \overline{0})\} = \{a \in A \mid a \in I \wedge a \in J\} = I \cap J$;
- Dimostriamo ora la doppia implicazione.

$\Longleftarrow$) Sia $1 = i + j,\ i \in I,\ j \in J$. $\forall (x + I, y + J)\ \exists a \in A$ tale che $(x + I, y + J) = (a + I, a + J)$ dove $a \equiv x \mod (I) \wedge a \equiv y \mod (J)$ con I e J ideali coprimi o comassimali. Sia allora $a = xj + yi$.

$$\begin{aligned} a = x(1 - i) + yi = x + ix + yi \equiv x \mod (I) \\ a = xj + (1 - j)y = xj + (1 - j)y = xj + y - yj \equiv y \mod (J) \end{aligned}$$

$\Longrightarrow$) $\exists a \mid f(a) = (1 + I, J) \wedge \exists b \mid f(b) = (I, 1 + J)$.

Allora: $\begin{cases} a \equiv 1 \mod (I) \\ a \equiv 0 \mod (J) \end{cases} \implies \begin{cases} a - 1 \in I \\ a \in J \end{cases} \implies \begin{cases} a - 1 = i \in I \\ 1 = a - i \in I + J \end{cases}$

Dunque ${}^{A}\!/_{Ker(f)} \cong {}^{A}\!/_{I} \times {}^{A}\!/_{J}$.

□

Definizione 22 (Ideale primo)**.** *$I \subsetneq A$ ideale. I si dice primo se $\forall x, y \in A$ vale che $xy \in I \implies x \in I \vee y \in I$.*

Osservazione 26. *$\{0\}$ è chiaramente un ideale primo di $\mathbb{Z}$: $xy = 0 \iff x = 0 \vee y = 0$ poiché $\mathbb{Z}$ è un dominio.*

Definizione 23 (Ideale massimale)**.** *$I \subsetneq A$ ideale si dice massimale se è massimale rispetto all'inclusione tra gli ideali propri ossia se $I \subset J \subsetneq A \implies I = J$.*

Definizione 24. *Sia $\mathcal{F}$ una famiglia e $\leq$ un ordinamento parziale. Allora:*

- *$I \subset \mathcal{F}$: $X \in \mathcal{F}$ si dice massimo per $\mathcal{F}$ se $\forall A \in \mathcal{F}$ si ha $A \leq X$;*
- *$I \subset \mathcal{F}$: $M \in \mathcal{F}$ si dice maggiorante per I se $\forall A \in I, A \leq M$;*
- *$\mathcal{C} \subseteq \mathcal{F}$ si dice catena se $\mathcal{C}$ è totalmente ordinato (ovvero se in $\mathcal{C}$ tutti gli elementi sono confrontabili);*
- *$(\mathcal{F}, \leq)$ si dice induttivo se ogni catena ammette un maggiorante.*

Teorema 18 (Lemma di Zorn)**.** *Sia $(\mathcal{F}, \leq)$ parzialmente ordinato. Se $\mathcal{F} \neq \emptyset$ e $\mathcal{F}$ è induttivo, allora $\exists M \in \mathcal{F}$ massimale.*

Osservazione 27. *$(\{I \subsetneq A \mid I \text{ è un ideale proprio}\}, \subseteq)$ è parzialmente ordinato. Infatti $\mathcal{C} = \{I_\lambda\}_{\lambda \in \Lambda}$ è una catena e $I = \bigcup I_\lambda$ è un ideale di $A \in \mathcal{F}$. Poiché $\mathcal{F}$ è induttivo, allora esistono elementi massimali.*

Proposizione 19. *Ogni ideale proprio di A è contenuto in un ideale massimale di A.*

Dimostrazione. $\mathcal{F} = \{I \subseteq A \mid J \supseteq I\} \neq \emptyset$ (ad esempio c'è I). $(\mathcal{F}, \subseteq)$ è induttivo e dunque, per Zorn, $\exists M \in \mathcal{F}$ massimale. Chiaramente $I \subset M$. Osservo che M è un ideale massimale di A: se $M \subseteq M' \subset A \implies M' \supseteq I \implies M' \in \mathcal{F}$ ma M è massimale in $\mathcal{F} \implies M = M'$. □

Corollario 5. *$\forall x \in A, x \notin A^* \implies x$ è contenuto in un ideale massimale.*

Dimostrazione. $I = (x)$ è un ideale proprio di A e si applica la proposizione precedente. □

Proposizione 20. *Sia $I \subsetneq A$ proprio. Allora:*

- *I è primo $\iff$ A/I è un dominio;*
- *I è massimale $\iff$ A/I è un campo.*

Dimostrazione. • Consideriamo $\pi\colon A \to A/I$. Allora:

$$I \text{ primo} \underset{\iff x \in I \vee y \in I}{\iff} \underbrace{xy \in I}_{} \iff \pi(xy) = \overline{0} \iff \pi(x)\pi(y) = \overline{0} \underbrace{\iff}_{A/I \text{ è un dominio}} \pi(x) = 0 \vee \pi(y) = 0$$

- I è massimale $\iff$ in A/I ci sono solo gli ideali banali $\iff$ A/I è un campo (per il teorema di corrispondenza).

□

Corollario 6. • *A dominio $\iff$ $\{0\}$ è un ideale proprio;*

- *A è un campo $\iff$ $\{0\}$ è massimale;*
- *Ogni campo è un dominio (massimale $\implies$ primo);*

Esempio 20. *Sia $I \subset \mathbb{Z}$ un ideale, $I = (m)$. Allora $\sqrt{(m)} \subset \mathbb{Z}$ e in particolare, poiché $x \in \sqrt{I} \iff \exists n \in \mathbb{N}$ tale che $x^n \in I$ si ha che se $m = p_1^{a_1} \cdots p_n^{a_n}$ con $a_i > 0$ allora $\sqrt{(m)} = (p_1 \cdots p_n)$.*

Definizione 25 (Divisione tra ideali)**.** *Siano $I, J \subset A$ ideali. Definiamo $I : J = \{x \in A \mid xJ \subset I\}$.*

Esempio 21. *Siano $(3), (9)$ ideali di $\mathbb{Z}$. Allora si ha che $(3) : (9) = \mathbb{Z}$ e $(9) : (3) = (3)$.*

Proposizione 21. *Se p è un numero primo, allora $(p^a) : (p^b) = \begin{cases} p^{a-b} & \text{se } a \geq b \\ \mathbb{Z} & \text{se } a < b \end{cases}$*

In generale, se $m = p_1^{a_1} \cdots p_n^{a_n}$ e $n = p_1^{b_1} \cdots p_n^{a_n}$ (posso supporre la fattorizzazione fatta dagli stessi primi se ammetto che gli esponenti possano anche essere 0) si ha che $(m) : (n) = (p_1^{max(a_1-b_1,0)} \cdot p_2^{max(a_2-b_2,0)} \cdots p_n^{max(a_n-b_n,0)})$.