Appunti di Algebra I

Dalle lezioni dei proff.
Roberto Dvornicich e Filippo Callegaro

Simone Cappellini

A.a. 2015/2016

31 gennaio 2016

http://poisson.phc.unipi.it/~cappellini

Indice

Capitolo 1

Teoria sui Gruppi

1.1 Richiami di Aritmetica

Definizione: Un insieme G dotato di un'operazione associativa, per cui esista un elemento neutro e tale che per ogni elemento esista un inverso si definisce *gruppo*.
Se per ogni coppia di elementi vale la proprietà commutativa il gruppo si dice *commutativo* o *abeliano*.

Teorema: Se G è un gruppo ciclico, allora

$$G \cong \begin{cases} \mathbb{Z} \\ \mathbb{Z}/n\mathbb{Z} & \text{con } n \geq 1 \end{cases}$$

Teorema: Se G è un gruppo ciclico allora è abeliano.

Definizione: Sia S un sottoinsieme di G gruppo. Si dice che S genera il sottogruppo H se H è il più piccolo sottogruppo di G che contiene S, e si scrive $H = \langle S \rangle$.
In particolare, se $S = \{s_i\}_{i \in I}$, $S^{-1} = \left\{s_i^{-1}\right\}_{i \in I}$ e $T = S \cup S^{-1}$ allora
$H = \{\prod_{i=1}^{n} t_i | \, t_i \in T \ \forall i, n \geq 0\}$.

Teorema (Teorema di Lagrange): Se $|G| = n$ e $H < G$ con $|H| = d$, allora $d \mid n$.

Dato G gruppo, $|G| = n$ e $d \mid n$. Esiste $H < G$ tale che $|H| = d$?

- Se G è *ciclico*, allora ne esiste uno e uno solo;
- Se G è *abeliano*, allora ne esiste almeno 1;
- Se $d = p$ con p primo, allora esiste;
- Se G è un gruppo qualsiasi non è detto.

Definizione: Un sottogruppo $H < G$ si dice *normale* (e si indica con $H \triangleleft G$) se per ogni elemento x di G le classi laterali xH e Hx coincidono.

Proposizione: Dato n gruppo G e un sottogruppo H di G,

$$H \triangleleft G \Leftrightarrow \forall \ x \in G \ xHx^{-1} \subseteq H$$

Osservazione. Se $H \triangleleft G$ allora G/H (l'insieme delle classi laterali) è un gruppo, detto gruppo *quoziente*, con operazione $xH \cdot yH := xyH$.

Definizione: Una funzione $f : G \to G'$ si dice *omomorfismo* tra gruppi se $f(xy) = f(x)f(y)$ per ogni $x, y \in G$.

Teorema: I sottogruppi normali di un gruppo G sono tutti e soli i nuclei di omomorfismi di gruppi da G in un altro gruppo G'.

Teorema (Teorema di Isomorfismo): Sia $f : G \to G'$, $K = \operatorname{Ker} f$. Allora esiste un'unica funzione $\varphi : G/K \to G'$ iniettiva che renda commutativo il seguente diagramma:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & G' \\ & G/K \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

Inoltre φ è surgettiva $\Leftrightarrow$ f lo è.

Osservazione. Se $K = \operatorname{Ker} f$, allora $f(x) = f(y) \Leftrightarrow xK = yK$.

Teorema (Teorema di Isomorfismo - Variante): Sia $f : G \to G'$, $K = \operatorname{Ker} f$, $H \triangleleft G$ e $H \subseteq K$. Allora esiste un'unica funzione $\varphi : G/H \to G'$ (non necessariamente iniettiva) che renda commutativo lo stesso diagramma (con H al posto di K) di cui sopra.

Esempio: Studiare come sono fatte tutte le $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ dato un omomorfismo $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ che rendano commutativo il seguente diagramma:

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, dashed, "f"] \arrow[dr, "\pi"'] & & \mathbb{Z}/n\mathbb{Z} \\ & \mathbb{Z}/m\mathbb{Z} \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Consideriamo $H = m\mathbb{Z}$. $H \subseteq \operatorname{Ker} f$. Essendo $m\mathbb{Z} = \langle m \rangle$ le f cercate sono tutti gli omomorfismi tali per cui $m \in \operatorname{Ker} f$, cioè $f(m) = 0$.

Teorema (Corrispondenza tra Sottogruppi): Sia $f : G \to G'$ un omomorfismo surgettivo. Allora:

- $H < G \Rightarrow f(H) < G'$;
- $H' < G' \Rightarrow f^{-1}(H') < G$;
- $H \triangleleft G \Rightarrow f(H) \triangleleft G'$;
- $H' \triangleleft G' \Rightarrow f^{-1}(H') \triangleleft G$.

Inoltre se $K = \operatorname{Ker} f$, i sottogruppi $H < G$ che contengono K sono in corrispondenza biunivoca con i sottogruppi $H' < G'$.
Analogamente vale per gli $H \triangleleft G$.

1.2 Teoremi, Proposizioni, Esercizi sui Gruppi

In questa sezione sono raccolti sia teoremi che esercizi sui gruppi svolti durante le lezioni e le esercitazioni. È quindi possibile che una dimostrazione qui proposta necessiti di definizioni, risultati e proposizioni analizzate in altre sezioni e capitoli.

Definizione: In un gruppo G, definiamo una relazione di equivalenza detta coniugio, tale che $x \sim y \Leftrightarrow \exists g \in G \ : \ y = gxg^{-1}$.

Osservazione. La classe di equivalenza di un elemento x per coniugio sarà $cl(x) = \{y \in G \mid \exists g \in G \ y = gxg^{-1}\} = \{gxg^{-1} \mid g \in G\}$.

Caratterizzazione Sottogruppi Normali: Sia $N < G$. Allora:

$$\begin{aligned} N \triangleleft G \Leftrightarrow & \quad N \text{ è nucleo di omomorfismo} \\ \Leftrightarrow & \quad N \text{ è invariante per coniugio con el. di } G \\ \Leftrightarrow & \quad N \text{ è unione di classi di coniugio di } G \\ & \left(G = \bigsqcup_{x \in \mathcal{R}} cl(x) \text{ quindi } N = \bigsqcup_{x \in \mathcal{R}'} cl(x) \right) \end{aligned}$$

Teorema: Sia G gruppo e siano H, K due sottogruppi normali di G tali che:

- $H \cap K = \{e\}$;
- $G = HK = \{hk \mid h \in H, k \in K\}$.

Allora $G \cong H \times K$.

Dimostrazione. Definiamo $f : H \times K \to G$ tal che $f(h,k) = hk$. Dimostriamo che si tratta di un isomorfismo di gruppi.

- Linearità:
  $f((h,k)(h',k')) = f(hh',kk') = hh'kk'$
  $f(h,k)f(h',k') = hkh'k'$.
  Basta dimostrare quindi che $h'k = kh' \ \forall h' \in H, \forall k \in K$.

  $$\begin{aligned} h'k = kh' &\Leftrightarrow (h'kh'^{-1})k^{-1} = e \\ &\Leftrightarrow h'(kh'^{-1}k^{-1}) = e \end{aligned}$$

  Ma $h'kh'^{-1} \in K$, poiché $K \triangleleft G$, e analogamente $kh'^{-1}k^{-1} \in H$. Quindi $h'kh'^{-1}k^{-1} \in H \cap K = \{e\}$, cioè $h'kh'^{-1}k^{-1} = e$.

- Iniettività:
  $\operatorname{Ker} f = \{(h,k) \mid hk = e\} = \{(h,k) \mid h = k^{-1}\} = \{(e,e)\}$.
  L'ultima uguaglianza deriva dall'ipotesi che $H \cap K = \{e\}$.

- Surgettività:
  Ovvia per la seconda ipotesi ($G = HK = \{hk \mid h \in H, k \in K\} = \operatorname{Im} f$).

$\square$

Osservazione. Se $|G| < \infty$, come seconda ipotesi del teorema precedente è sufficiente avere che $|G| = |H| \cdot |K|$. Infatti $HK \subseteq G$ e $|HK| = \frac{|H|\cdot|K|}{|H\cap K|} = |G|$, quindi $G = HK$.

Esempio: $G = \mathbb{C}^*$, $H = \mathbb{R}^+$, $K = \{z \in \mathbb{C}^* | \, |z| = 1\}$.
$\Rightarrow \mathbb{C}^* = HK$ e quindi $\mathbb{C}^* \cong H \times K$, con l'isomorfismo $z = \rho e^{i\theta} \mapsto (\rho, \theta)$.

Proposizione: Sia G un gruppo abeliano finito, $H \triangleleft G$ ciclico, G/H ciclico e siano $|H|$ e $|G/H|$ coprimi. Allora G è ciclico.

Dimostrazione. Sia $H = \langle y \rangle$, $ord(y) = m$.
Sia $|G/H| = n$, $G/H = \langle \bar{x} \rangle$ con $ord(\bar{x}) = n$.
Sia $x \in G$ tale che $\bar{x} = xH$.
Allora $\bar{x}^n = eH = H = x^n H, \Rightarrow x^n \in H \Rightarrow x^n = y^c$.
Poiché n è coprimo con m (l'ordine di y), allora per Bézout esistono s e t tali che $ns+mt = c$. Dunque $y^c = y^{ns+mt} = y^{ns}y^{mt} = y^{ns}(y^m)^t = y^{ns}$.
Sia $x' = xy^{-s}$. Allora $(x')^n = x^n y^{-ns} = y^c y^{-c} = e$.
Vediamo che $ord(x') = n$. Infatti x e x' stanno nella stessa classe laterale, che ha ordine n; quindi $(x')^i \notin H \ \forall \ i < n$.
Per concludere la dimostrazione bisogna dimostrare che $ord(x'y) = mn$.
Sia $ord(x'y) = k$:
$(x'y)^k = (x')^k y^k = e \Rightarrow (x')^k = y^{-k}$, cioè $(x')^k \in H$. Allora $(x')^k = e$ e $y^k = e$, e dunque $n \mid k, m \mid k$.
$\Rightarrow nm \mid k$. Ma dato che l'ordine di G è mn, si ha l'uguaglianza. $\square$

Proposizione: Sia G un gruppo finito tale che per ogni $g \in G$ $g^2 = e$. Allora G è abeliano e $G \cong (C_2)^n$ con $n \in \mathbb{N}$.

Dimostrazione. Per induzione su n.
Intanto vediamo che G è abeliano, poiché $\forall \ a, b \in G$ $(ab)^2 = e = a^2b^2$ e dalle regole di cancellazione segue che $ba = ab$.

Sia poi $g \in G$, $g \neq e$. $g^2 = e \Rightarrow H = \langle g \rangle \cong C_2$. Quindi per ipotesi induttiva $G/H \cong (C_2)^{n-1}$.
Costruiamo un omomorfismo iniettivo f:

$$\begin{tikzcd} G \arrow[r, "\pi"] & G/H \cong (C_2)^{n-1} \arrow[l, dashed, bend left, "f"] \end{tikzcd}$$

che associ ad ogni classe un rappresentante di tale classe. Allora $\operatorname{Im} f = K \cong (C_2)^{n-1}$ e $K \triangleleft G$.
Dato che $H \triangleleft G$, $H \cap K = \{e\}$ e $|H|\cdot|K| = |G|$ allora $G \cong H \times K = C_2 \times (C_2)^{n-1} = (C_2)^n$. $\square$

Proposizione: Sia G un gruppo tale che $|G| = 2p$ con p primo dispari. Allora $G \cong C_{2p}$ oppure $G \cong D_p$.

Dimostrazione. Sia $g \in G$, $ord(g) = p$, e sia $H = \langle g \rangle \cong C_p$. Allora $H \triangleleft G$ (ha indice 2).
$\exists k \in G$ tale che $ord(k) = 2$, e quindi $K = \langle k \rangle \cong C_2$.

- Se gli elementi di C_2 commutano con quelli di C_p: allora $Z(C_2) \supseteq C_2 \cup C_p$, e per motivi di cardinalità di sottogruppi $Z(C_2) = G$. Quindi $C_2 \triangleleft G$. Poiché $C_2 \cap C_p = \{e\}$ e $|G| = |C_2| \cdot |C_p|$ allora $G \cong C_{2p}$.

- Se gli elementi di C_2 non commutano con quelli di C_p: prendiamo l'azione di coniugio di C_2, $\phi : C_2 \to Aut(C_p) \cong C_{p-1}$ che associa a g l'omomorfismo $\phi_g : C_p \to C_p$.

$$ord(g) = 2 \Rightarrow ord(\phi_g) \mid 2 \Rightarrow$$

$$\Rightarrow \begin{cases} \phi_g = id & \Rightarrow & ghg^{-1} = h & \Rightarrow G \cong C_{2p} \text{ già visto} \\ \phi_g^2 = id & \Rightarrow & ghg^{-1} = h^{-1} & \Rightarrow G \cong D_p \end{cases}$$

$\square$

Proposizione: Sia G un gruppo finito di cardinalità maggiore di 2. Allora $|Aut(G)| > 1$.

Dimostrazione. Se G non è abeliano allora $G \neq Z(G)$, quindi $\exists g \notin Z(G)$ e questo elemento determina un automorfismo interno non banale.
Se invece G è abeliano, prendo $G \ni g \mapsto g^{-1} \in G$, che è un automorfismo banale se e solo se $g = g^{-1}\ \forall\ g \in G$. $\Rightarrow g^2 = e\ \forall\ g \in G\ \ \Rightarrow G \cong (C_2)^n$. Ma allora posso creare esplicitamente un automorfismo non banale, ad esempio quello che manda $(a,\ b,\ \ldots)$ in $(b,\ a,\ \ldots)$. $\square$

Proposizione: Sia G un gruppo di cardinalità $2n$ tale che esattamente metà degli elementi ha ordine 2 e tutti gli altri elementi formano un sottogruppo H. Allora n è dispari e H è abeliano.

Dimostrazione. Sia $a \in G \setminus H$. Dunque $a^2 = e$.
Sia ϕ_a tale che $\phi_a(g) = aga^{-1}$. Se $g \in H$, allora $ga \notin H$ e quindi $gaga = e$.
$\Rightarrow aga = g^{-1} = \phi_a(g)$. Dunque ϕ_a agisce su H mandando g in g^{-1}. Siano adesso $g_1, g_2 \in H$:
$g_1^{-1}g_2^{-1} = \phi_a(g_1)\phi_a(g_2) = \phi_a(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1}\ \Rightarrow g_2g_1 = g_1g_2\ \Rightarrow H$ è abeliano.
H non contiene elementi di ordine 2, $|H| = n\ \Rightarrow n$ è dispari per il Teorema di Cauchy per gruppi abeliani. $\square$

Osservazione. G è abeliano se e solo se $g \mapsto g^{-1}$ è un omomorfismo (e quindi un automorfismo).

1.3 Teorema di Cauchy

Teorema (Teorema di Cauchy): Sia G un gruppo di cardinalità n e sia p un primo tale che $p \mid n$. Allora $\exists\ x \in G$ tale che $ord(x) = p$.

Dimostrazione. Per la dimostrazione utilizziamo un'induzione su n ($n = mp$, quindi un'induzione su m) e la conoscenza del teorema nel caso di G abeliano.

Passiamo direttamente al passo induttivo: sapendo che

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

- Se $\exists\ x \in \mathcal{R}'$ tale che $p|\,|Z(x)|$, poiché $Z(x) < G$ allora si conclude grazie all'ipotesi induttiva;
- Se non esiste $x \in \mathcal{R}'$ tale che $p|\,|Z(x)|$, allora tutti gli addendi della sommatoria sono multipli di p. Allora $p|\,|Z(G)|$. Essendo $Z(G)$ abeliano, allora grazie al teorema nel caso abeliano si trova un $x \in Z(G)$ di ordine p.

$\square$

1.4 Sottogruppi in Gruppi Finiti

PROPOSIZIONE: In un gruppo G abeliano di ordine n per ogni $d \mid n$ esiste un sottogruppo di ordine d.

Dimostrazione. Sia $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ e sia $d = p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k}$ con $0 \leq \delta_i \leq \alpha_i$.
Sia inoltre $\delta = \delta_1 + \ldots + \delta_k$. Procediamo per induzione su δ.
Il passo base ($\delta = 1$) è dato dal teorema di Cauchy.
Passo induttivo:

Consideriamo un divisore $m = p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k}$ con $\delta + 1 = \delta_1 + \ldots + \delta_k$.
Senza perdita di generalità possiamo supporre $\delta_k > 0$. Prendiamo quindi $m' = p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k - 1}$.
Per ipotesi induttiva esiste un sottogruppo (normale) H di G di ordine m'. Nel gruppo quoziente G/H esiste $\bar{K} < G/H$ tale che $ord(\bar{K}) = p_k$ (per Cauchy), dunque $K = \pi^{-1}(\bar{K})$ ha l'ordine cercato. $\square$

PROPOSIZIONE: In un p-gruppo G di cardinalità p^n esiste un sottogruppo (normale) di ordine p^a per ogni $0 \leq a \leq n$.

Dimostrazione. Induzione su n.
Il caso $n = 1$ è banale.
Passo induttivo:
Poiché G è un p-gruppo, allora $Z(G) \neq \{e\}$. Sia quindi $|Z(G)| = p^k$.

- Se $a \leq k$, allora trovo il sottogruppo all'interno di $Z(G)$ (che è abeliano) grazie alla proposizione precedente;
- Se $a > k$ allora considero $G' = G/Z(G)$ che ha cardinalità $< p^n$. Quindi per ipotesi induttiva in G' esiste un sottogruppo (normale) $\bar{K}$ di ordine p^{a-k}. Allora $H = \pi^{-1}(\bar{K})$ è un sottogruppo di ordine voluto.

$\square$

In generale però non è vero che esiste sempre un sottogruppo di un certo ordine in un gruppo G. Infatti, prendendo il gruppo alterno (delle permutazioni pari) A_4 che ha ordine 12 si dimostra che non esiste un sottogruppo di ordine 6.

A_4 è costituito dall'identità, 8 3-cicli e 3 2-2-cicli.
Poiché, scelta una $\sigma \in S_n$,

$$|S_4| = |Z(\sigma)| \cdot |Cl(\sigma)|$$

allora

$$|A_4| = |Z(\sigma) \cap A_4| \cdot |Cl_{A_4}(\sigma)|$$

con $Cl_{A_4}(\sigma)$ la classe di coniugio di σ per elementi di A_4.

Lemma: Data $\sigma \in S_n$, $|Z(\sigma) \cap A_n| = \begin{cases} |Z(\sigma)| & \text{se } Z(\sigma) \subseteq A_n \\ \frac{|Z(\sigma)|}{2} & \text{se } Z(\sigma) \nsubseteq A_n \end{cases}$.

Dimostrazione. Se $Z(\sigma) \subseteq A_n$ la tesi è ovvia.
Se $Z(\sigma) \nsubseteq A_n$, sapendo che $|H| \cdot |K| = |H \cap K| \cdot |HK|$, allora

$$|Z(\sigma)| \cdot |A_n| = |Z(\sigma) \cap A_n| \cdot \underbrace{|Z(\sigma)A_n|}_{=|S_n|}$$

Da cui si giunge alla tesi. $\square$

Poiché $|A_4| = \frac{|S_4|}{2} = \frac{1}{2} \cdot |Z(\sigma)| \cdot |Cl(\sigma)|$, allora $Z(\sigma) \subseteq A_4 \Rightarrow \ |Cl_{A_4}(\sigma)| = \frac{|Cl(\sigma)|}{2}$; se invece $|Z(\sigma) \cap A_4| = \frac{|Z(\sigma)|}{2}$ allora $|Cl_{A_4}(\sigma)| = |Cl(\sigma)|$.

Dunque:

$$|Cl\left((a,\ b,\ c)\right)| = \binom{4}{3} \cdot 2! = 8 \Rightarrow |Z\left((a,\ b,\ c)\right)| = |Z\left((a,\ b,\ c)\right) \cap A_4| = 3$$

$$\Rightarrow |Cl_{A_4}\left((a,\ b,\ c)\right)| = 4$$

Cioè in A_4 (essendoci 8 cicli di ordine 3) ci sono 2 classi di coniugio diverse da 4 elementi ciascuna.

$$|Cl\left((a,\ b)(c, d)\right)| = \binom{4}{2} \cdot \frac{1}{2} = 3 = |Cl_{A_4}\left((a,\ b)(c,\ d)\right)| \Rightarrow$$

$$\Rightarrow |Z\left((a,\ b)(c,\ d)\right) \cap A_4| = 4$$

Cioè in A_4 c'è un unica classe di coniugio per i 2-2- cicli con 3 elementi.

Si ha quindi $12 = |A_4| = \bigcup_{\sigma \in \mathcal{R}_{A_4}} |Cl_{A_4}(\sigma)| = 1 + 4 + 4 + 3$. Dato che un sottogruppo di ordine 6 in A_4 ha indice 2 e quindi è normale, allora è unione di classi di coniugio. Ma è impossibile ottenere 6 sommando 1, 4, 4 e 3 e quindi non esiste un sottogruppo di ordine 6 in A_4.

Osservazione. Si ha che $Z(\sigma) \nsubseteq A_n$ quando:

1. La decomposizione in cicli di σ contiene almeno un ciclo di ordine pari;
2. σ contiene 2 cicli della stessa lunghezza:
   Ad esempio, in S_6 $\sigma = (1\ 2\ 3)(4\ 5\ 6)$, $Z(\sigma) \ni (1\ 4)(2\ 5)(3\ 6) \notin A_6$.
3. Esistono 2 elementi di $\{1, \ldots, n\}$ fissati da σ.

1.5 Teorema di Struttura per Gruppi Abeliani Finiti

TEOREMA (TEOREMA DI STRUTTURA PER GRUPPI ABELIANI FINITI): Se A è un gruppo abeliano finito, allora è isomorfo a un prodotto diretto di gruppi ciclici.

Dimostrazione. La dimostrazione si articola attraverso vari lemmi.

LEMMA 1: Per ogni $m \in \mathbb{N}$ la funzione $f : A \to A$ tale che $f(x) = mx$ è un endomorfismo di A.

Dimostrazione. Poiché A è abeliano, si ha che $f(x + y) = m(x + y) = mx + my = f(x) + f(y)$. □

Vediamo che $\operatorname{Ker} f = A_m = \{x \in A |\ mx = 0\}$ e che $\operatorname{Im} f = mA = \{mx |\ x \in A\}$.

Osservazione. A_m e mA sono sottogruppi caratteristici di A.

LEMMA 2: Se $|A| = mn$ con $(m, n) = 1$ allora $A \cong A_m \times A_n$ e anche $A \cong mA \times nA$.

Dimostrazione. $A \cong A_m \times A_n$:
Verifichiamo che $A_m \cap A_n = \{0\}$. Infatti, se $x \in A_m \cap A_n$ allora $mx = nx = 0$, e cioè $ord(x) \mid m$, $ord(x) \mid n$. $\Rightarrow$ $ord(x) \mid (m, n) = 1 \Rightarrow x = 0$.

$A_m \oplus A_n = A$: (il simbolo di somma diretta equivale, per gruppi finiti, a quello di prodotto diretto)
Un'inclusiione è ovvia, per l'altra utilizziamo Bézout che afferma che esistono s, t tali che $sm + tn = 1$. Quindi $smx + tnx = x$. Notando che $smx \in A_n$ e $tnx \in A_m$ si ottiene la tesi.
Dato che entrambi i sottogruppi sono normali (A è abeliano), allora $A \cong A_m \times A_n$.

L'altro isomorfismo è analogo. □

Osservazione. In realtà si ha che $A_m = nA$ e $A_n = mA$.

COROLLARIO: Sia $|A| = n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$. Allora $A \cong A_{p_1^{a_1}} \times \ldots \times A_{p_k^{a_k}}$.

Dimostrazione. Induzione su k.
Il passo base ($k = 1$ o 2) è banale o deriva dal LEMMA 2;
Per il passo induttivo si ha $A \cong A_{p_1^{a_1} \cdot \ldots \cdot p_{k-1}^{a_{k-1}}} \times A_{p_k^{a_k}} \cong A_{p_1^{a_1}} \times \ldots \times A_{p_k^{a_k}}$ □

Osservazione. $\left| A_{p_i^{a_i}} \right| = p_i^{a_i}$. Infatti $A_{p_i^{a_i}} < A$, e quindi $\left| A_{p_i^{a_i}} \right| \leq p_i^{a_i}$. Ma poiché $|A| = \left| A_{p_1^{a_1}} \right| \cdot \ldots \cdot \left| A_{p_k^{a_k}} \right|$ allora vale l'uguaglianza.

LEMMA 3: Sia A un p-gruppo abeliano. Allora A è isomorfo ad un prodotto diretto di gruppi ciclici.

Dimostrazione. Utilizziamo un ulteriore lemma:

LEMMA 4: Sia A un p-gruppo abeliano. Sia x di ordine massimo in A e sia $H =< x >$. Allora per ogni $\bar{y} \in A/H$ esiste $y \in A$ tale che $\pi(y) = \bar{y}$ e $ord(y) = ord(\bar{y})$.

Dimostrazione. Sia $z \in A$ tale che $\pi(z) = \bar{y}$. Cerchiamo $y \in z+H$, e cioè della forma $z+kx$.

Sia $ord(x) = p^a$ e $ord(\bar{y}) = p^b$ con $b \leq a$.
Allora $p^b \bar{y} = 0$, ovvero $p^b \pi(z) = \pi(p^b z) = 0 \Rightarrow p^b z \in H$. Chiamiamo $p^b z = sx$.
D'altronde poiché x ha ordine massimo possibile allora anche $p^a z = 0$, e quindi $p^a z = p^{a-b} p^b z = p^{a-b} sx = 0$. Allora $p^b \mid s \Rightarrow s = p^b t$.

Dunque $p^b z = p^b tx$, e quindi dovendo avere ordine p^b y avrà come proprietà che $p^b(z+kx) = 0$.

$$p^b(z+kx) = p^b z + p^b kx = p^b tx + p^b kx = 0 \Rightarrow k = -t$$

Siamo quindi riusciti a trovare l'y cercato. □

Dimostriamo adesso il Lemma 3 per induzione su $|A|$:
Passo induttivo: Prendendo $x \in A$ di ordine massimo possibile e $H =< x >$, per ipotesi induttiva

$$A/H \cong \bar{B}_1 \times \ldots \times \bar{B}_k$$

con $\bar{B}_i$ ciclici.
Siano $\bar{y}_1, \ldots, \bar{y}_k$ i generatori canonici di A/H (cioè $\bar{y}_1 = (\bar{1},\ 0, \ldots, 0)$ e analogamente gli altri). Per il Lemma 4 esistono $y_1, \ldots, y_k \in A$ tali che $ord(y_i) = ord(\bar{y}_i)$ e $\pi(y_i) = \bar{y}_i \forall\ i$.
Consideriamo $K =< y_1, \ldots, y_k >$. La proiezione $\pi|_K$ dà un isomorfismo tra K e $\bar{B}_1 \times \ldots \times \bar{B}_k \cong A/H$.
Infatti di sicuro è un omomorfismo, in più è surgettivo poichè nell'immagine di π ci stanno tutti i generatori di A/H e iniettivo per ragioni di cardinalità dovute ai generatori $y_1, \ldots, y_k$.

Concludiamo dunque la dimostrazione del Lemma 3 dimostrando che

$$A \cong H \times K$$

$H \cap K = \{0\}$: sia $H \cap K \ni m_1 y_1 + \ldots + m_k y_k \mapsto \pi(m_1 y_1 + \ldots + m_k y_k) = m_1 \bar{y}_1 + \ldots + m_k \bar{y}_k = (m_1, \ldots, m_k) = 0.$ $\Rightarrow m_i = 0\ \forall\ i$.
$H \oplus K = A$: sia $t \in A$, $\pi(t) = m_1 \bar{y}_1 + \ldots + m_k \bar{y}_k = \pi(m_1 y_1 + \ldots + m_k y_k)$. Dunque $t - \sum m_i y_i \in H$, cioè $t = \lambda x + \sum m_i y_i$.
Essendo A abeliano, tutti i sottogruppi sono normali, per cui $A \cong H \times K$. H è ciclico e K è prodotto di gruppi ciclici, dunque A è isomorfo ad un prodotto di gruppi ciclici. □

La dimostrazione del Teorema di Struttura consiste dunque nell'applicazione dei lemmi 1, 2, 3 e 4. □

Teorema (Unicità della Decomposizione in Gruppi Ciclici): Sia A un p-gruppo abeliano. La decomposizione di A nella forma $A \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$ con $a_1 \geq \ldots \geq a_k > 0$ è unica.

Dimostrazione. Sia $A \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{a_k}\mathbb{Z} \cong \mathbb{Z}/p^{b_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{b_h}\mathbb{Z}$ con $b_1 \geq \ldots \geq b_h > 0$.

Osservando che $A_p = \{x \in A |\ px = 0\}$ e

$$\begin{aligned} A_p &\cong p^{a_1-1}\mathbb{Z}/p^{a_1}\mathbb{Z} \times \ldots \times p^{a_k-1}\mathbb{Z}/p^{a_k}\mathbb{Z} \\ &\cong p^{b_1-1}\mathbb{Z}/p^{b_1}\mathbb{Z} \times \ldots \times p^{b_h-1}\mathbb{Z}/p^{b_h}\mathbb{Z} \end{aligned}$$

ha cardinalità p^k secondo la prima decomposizione e p^h per la seconda decomposizione si ha $h = k$.

Dimostriamo adesso che $a_i = b_i \ \forall\ i$ per induzione sull'ordine di A:

$$A/A_p \cong \mathbb{Z}/p^{a_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{a_k-1}\mathbb{Z} \cong \mathbb{Z}/p^{b_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{b_k-1}\mathbb{Z}$$

Per ipotesi induttiva tale decomposizione è unica, dunque per ogni $1 \leq j \leq k$ $a_j - 1 = b_j - 1 \Rightarrow a_j = b_j \ \forall\ j = 1, \ldots, k$. □

PROPOSIZIONE: Sia $G \cong H \times K$ con H, K caratteristici. Allora $Aut(G) \cong Aut(H) \times Aut(K)$.

Dimostrazione. Creiamo un isomorfismo da $Aut(H) \times Aut(K)$ in $Aut(G)$:

$$\begin{array}{rccc} f: & Aut(H) \times Aut(K) & \to & Aut(G) \\ & (\varphi, \psi) & \mapsto & \lambda \end{array}$$

con $\lambda(x, y) := (\varphi(x), \psi(y))$. Si tratta banalmente di un omomorfismo iniettivo. Vediamone la surgettività:
Sia $\lambda \in Aut(G)$, allora $\varphi = \lambda|_H \in Aut(H)$ e $\psi = \lambda|_K \in Aut(K)$. Dunque $\lambda(x, y) = \lambda(x, e)\lambda(e, y) = (\varphi(x), \psi(y))$. □

1.6 Abelianizzato di un Gruppo

DEFINIZIONE: Si dice *derivato* o *sottogruppo dei commutatori* il sottogruppo

$$G' = \left\{ ghg^{-1}h^{-1} \middle|\ g, h \in G \right\}$$

Osservazione. G' è caratteristico. Infatti, per ogni $\phi \in Aut(G)$,

$$\phi(ghg^{-1}h^{-1}) = \phi(g)\phi(h)\phi(g^{-1})\phi(h^{-1})$$

Osservazione. Se G è abeliano allora $G' = \{e\}$.

Osservazione. G/G' è abeliano.

DEFINIZIONE: Il gruppo quoziente G/G' si dice *abelianizzato* di G (G^{ab}).

PROPOSIZIONE: Se $N \lhd G$ tale che G/N è abeliano allora $N \supseteq G'$.

Dimostrazione. Considerando la proiezione $\pi : G \to G/N$, poiché G/N è abeliano si ha che $\forall\ g, h \in G$ $\pi(ghg^{-1}h^{-1}) = e$.
Dunque $ghg^{-1}h^{-1} \in \operatorname{Ker} \pi = N$. □

Osservazione. G' è il più piccolo sottogruppo normale tale per cui il quoziente risulti abeliano. Di conseguenza, G/G' è il più grande quoziente abeliano di G.

PROPOSIZIONE: Se $G' < H < G$ allora $H \lhd G$.

Dimostrazione.

$$\begin{array}{rccc} \pi: & G & \to & G/G' \\ & H & \mapsto & \bar{H} \end{array}$$

Poiché G/G' è abeliano, $\bar{H} \lhd G/G'$, e quindi $H \lhd G$. □

1.7 Teoremi di Sylow e Cayley

TEOREMA (1^{O} TEOREMA DI SYLOW): Sia G un gruppo di ordine $n = p^k m$ con $(p, m) = 1$ e $k > 0$. Allora esiste un sottogruppo di cardinalità p^k detto p-sottogruppo di Sylow oppure p-Sylow di G.

Dimostrazione. 1.
Induzione sull'ordine di G ($|G| = pl$, induzione su l).
Passo induttivo: se G possiede un sottogruppo di ordine $p^k m'$ con $m' < m$ allora la tesi segue per ipotesi induttiva. Se G è abeliano la tesi è banalmente vera.
Supponiamo G non abeliano e che non esista in G un sottogruppo di ordine $p^k m'$ con $m' < m$.
Dalla formula delle classi

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

si ha che $p^k \nmid |Z(x)| \ \ \forall\, x \in \mathcal{R}$, ovvero $p \mid \sum \frac{|G|}{|Z(x)|}$. Allora $p \big| \ |Z(G)|$, e quindi $\exists\, g \in Z(G)$ di ordine p. $H = < g >$ è un sottogruppo normale di G.

$ord(G/H) = p^{k-1}m$, e per ipotesi induttiva esiste un sottogruppo $\overline{K}$ in G/H di cardinalità p^{k-1}. Chiamando π la proiezione canonica al quoziente, si ha che $\pi^{-1}(\overline{K})$ ha cardinalità $|H| \cdot |\overline{K}| = p^k$. □

Dimostrazione. 2.
Sia $X = \left\{ A \subseteq G \Big| \ |A| = p^k \right\}$. Dunque $|X| = \binom{n}{p^k}$.
G agisce su X tramite moltiplicazione a sinistra:

$$\begin{array}{rccc} \varphi : & G & \to & S(X) \\ & g & \mapsto & T_g \end{array}$$

con $T_g(x) = gx$, e più in generale $T_g(A) = gA$. T_g è surgettiva; infatti $\forall\, x \in G$ $T_g(g^{-1}x) = gg^{-1}x = x$.

LEMMA 1: $\binom{n}{p^k} \equiv m \pmod p$.

Dimostrazione. Cerchiamo il coefficiente di $x^{n-p^k} y^{p^k}$ in $(x+y)^n$. Poiché $n = p^k m$ allora $(x+y)^n = (x+y)^{p^k m} \equiv (x^{p^k} + y^{p^k})^m \pmod p$.
$(x^{p^k} + y^{p^k})^m = x^{p^k m} + \binom{m}{1} x^{p^k(m-1)} y^{p^k} + \ldots = x^n + m x^{n-p^k} y^{p^k} + \ldots$. □

Poiché $p \nmid m$ allora esiste un'orbita di cardinalità non divisibile per p.
Sia $A \in X$ tale che $p \nmid |Orb(A)|$. Allora, chiamando $H = Stab(A)$, si ha $|H| \cdot |Orb(A)| = |G|$.
Quindi $p^k \ \big| \ |H|$, e cioè $p^k \leq |H|$.
Vediamo che, dato $a \in A$, $H \subseteq Aa^{-1}$. Infatti, poiché $H = Stab(A)$, $\forall\, x \in H$ $xA = A$. Cioè $\forall x \in H$ $xa = a_j \ \Rightarrow x = a_j a^{-1}$.
Dunque $|H| \leq |Aa^{-1}| = p^k \ \Rightarrow |H| = p^k$. □

COROLLARIO: Sia G un gruppo di cardinalità $p^k m$ con $(p, m) = 1$. Allora contiene sottogruppi di ordine p^i per ogni $i \leq k$.

Dimostrazione. Per il Primo Teorema di Sylow esiste un sottogruppo H di ordine p^k. Per l'esistenza di sottogruppi nei p-gruppi si ha che contenuti in H ci sono sottogruppi per ogni ordine possibile. □

Teorema (2° Teorema di Sylow): Sia $|G| = p^k m$ con $(p, m) = 1$. Se P è un p-Sylow di G e H è un p-sottogruppo di G (ovvero di cardinalità p^i per un certo i) allora H è contenuto in un coniugato di P, cioè $\exists\ g \in G$ tale che $H \subseteq gPg^{-1}$.

Dimostrazione. Osservazione preliminare:
Osservazione. Se $H \subseteq N(P)$ allora $H \subseteq P$. Infatti, HP è un sottogruppo di G di ordine una potenza di p che contiene P: ma allora $HP = P$, e cioè $H \subseteq P$.

Consideriamo $S = \{gPg^{-1} |\ g \in G\}$ l'insieme dei coniugati di P. G agisce su S tramite coniugio.
È una buona definizione: $\forall\ h \in G\ h(gPg^{-1})h^{-1} = (hg)P(hg)^{-1}\ \in S$.
Osserviamo che $Stab(P) = N(P)$. Dato che $N(P) \supseteq P$ e $[G : Stab(P)] = |Orb(P)| = |S|$ allora la cardinalità dell'orbita di P è coprima con p.

Restringiamo l'azione di coniugio al p-sottogruppo H: se un'orbita ha più di un elemento allora ha cardinalità divisibile per p (poiché $|H| = |Stab_H(P)| \cdot |Orb_H(P)|$). Dunque esiste un'orbita di cardinalità 1.
Sia $P' \in S$ tale che abbia orbita banale; allora $Stab_H(P') = H$. Cioè $\forall\ h \in H\ hP'h^{-1} = P' \ \Rightarrow H \subseteq N(P')$. Quindi per l'osservazione preliminare $H \subseteq P'$. □

Corollario: I p-Sylow di un gruppo G sono tutti coniugati tra di loro.

Dimostrazione. Basta applicare il Secondo Teorema di Sylow nel caso $H = P_i$ con P_i un p-Sylow. □

Teorema (3° Teorema di Sylow): Sia $|G| = p^k m$ con $(p, m) = 1$ e sia P un p-Sylow di G. Allora

$$\left|\left\{P' < G \;\middle|\; |P'| = p^k\right\}\right| = \left|\left\{gPg^{-1} \;\middle|\; g \in G\right\}\right| = [G : N(P)] \equiv 1 \pmod p$$

Dimostrazione. Consideriamo l'azione di coniugio di P sull'insieme $S = \{gPg^{-1} \mid g \in G\}$ dei coniugati di P.
Sia P' un punto fisso, cioè un elemento la cui orbita è banale; allora $\forall\ x \in P\ \ xP'x^{-1} = P' \Rightarrow x \in N(P')$.
Ma allora per l'osservazione preliminare del 2° Teorema di Sylow, essendo $P \subseteq N(P')$, allora $P \subseteq P'$, e cioè $P = P'$.

Dunque esiste solamente un'orbita banale ($Orb(P)$), mentre tutte le altre hanno cardinalità potenza di p (poiché divide l'ordine di P).
Allora

$$|S| = \sum_{P' \in \mathcal{R}} |Orb(P')| = 1 + p \cdot R \equiv 1 \pmod p$$

□

Teorema (Teorema di Cayley): Ogni gruppo finito è isomorfo ad un sottogruppo di un gruppo di permutazioni (S_n per un certo $n \in \mathbb{N}$).

Dimostrazione. Consideriamo l'azione di G su se stesso tramite moltiplicazione a sinistra:

$$\begin{array}{rccc} \varphi : & G & \to & S(G) \\ & g & \mapsto & T_g \end{array}$$

con $T_g(x) = gx$. Banalmente φ è iniettiva. Dunque $G \cong \operatorname{Im}\varphi < S(G) \cong S_n$ con $n = |G|$. □

Corollario: Sia $H < G$, $[G : H] = n$. Allora esiste $K \triangleleft G$ tale che $[G : K] \mid n!$.

Dimostrazione. Sia $X = \{gH \mid g \in G\}$ l'insieme delle classi laterali sinistre di H.
G agisce su X tramite moltiplicazione a sinistra $\phi : G \to S(X) \cong S_n$. ϕ è un omomorfismo, dunque ha un nucleo K che completa il seguente diagramma:

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, dashed, "\pi"'] & & S_n \\
& G/K \arrow[ur, dashed, hook, "\text{iniettiva}"'] &
\end{tikzcd}$$

$\square$

Osservazione. $K = \bigcap_{g \in G} gHg^{-1}$. Dunque $K \subseteq H$.

Capitolo 2

Gruppi Diedrali

2.1 Definizione e Costruzione

DEFINIZIONE: Dato un n-agono regolare, l'insieme delle isometrie del piano che mandano l'n-agono in se stesso formano un gruppo, detto *gruppo diedrale* (e si indica con D_n).

Osservazione. Il gruppo non è abeliano.

Poiché le isometrie che mandano l'n-agono in se stesso mandano vertici in vertici e il centro nel centro (è un punto fisso), tutte le isometrie in D_n sono:

- Rotazioni intorno al centro di angolo $\frac{2k\pi}{n}$;
- Riflessioni con asse passante per il centro e per un vertice o per il punto medio di un lato.

In totale esistono $2n$ isometrie distinte perchè, scelto un vertice, esso può essere mandato in n vertici, mentre i 2 vertici consecutivi ad esso possono essere scambiati o meno (2 possibilità).

Dunque $|D_n| = 2n$.

$$D_n = \underbrace{R}_{\text{rotazioni}} \cup \underbrace{S}_{\text{riflessioni}}$$

$$|R| = |S| = n, \qquad R < D_n$$

Poiché R ha indice 2, allora $R \triangleleft D_n$. In più, R è ciclico e $R = \langle r \rangle$ con $r^n = e$. Quindi $R \cong \mathbb{Z}/n\mathbb{Z}$ tramite l'isomorfismo $\frac{2k\pi}{n} \leftrightarrow \bar{k}$.

Possiamo riscrivere $D_n = R \cup R_s$ con $R_s = \left\{ r^k s | r \in R, k \in \mathbb{Z} \right\}$ scelta una $s \in S$, e quindi D_n come

$$D_n = \left\{ r^i s^j | 0 \leq i < n \ 0 \leq j \leq 1 \right\}$$

2.2 Regola di Scambio

Chiamando r una rotazione per l'origine (di angolo α) e s una riflessione (simmetria) rispetto ad una retta passante per l'origine e avente angolo β con l'asse x si ha la seguente relazione:

$$sr = r^{-1}s$$

Infatti, usando le oordinate polari per un punto $P = (\rho, \theta)$:

$$\begin{array}{rcl} r(P) = (\rho, \theta + \alpha) & \Rightarrow & s(r(P)) = (\rho, 2\beta - (\theta + \alpha)) \\ s(P) = (\rho, 2\beta - \theta) & \Rightarrow & r^{-1}(s(P)) = (\rho, 2\beta - \theta - \alpha) \end{array}$$

Quindi

$$srs = srs^{-1} = r^{-1}$$

$$\text{Allora} \begin{cases} r^n = e \\ s^2 = e \\ sr = r^{-1}s \end{cases} \qquad \text{e dunque} \begin{cases} r^i(r^{i'}s^{j'}) = r^{i+i'}s^{j'} \\ r^i s(r^{i'}s^{j'}) = r^{i-i'}s^{1+j'} \end{cases}$$

Adesso possiamo avere quindi una presentazione completa del gruppo D_n:

$$D_n = \left\{ r^i s^j | r^n = e,\ s^2 = e,\ srs^{-1} = r^{-1} \right\}$$

2.3 Sottogruppi di D_n

Sicuramente $\{e\}$ e D_n sono sottogruppi (banali).
Il gruppo delle rotazioni è un sottogruppo normale di D_n (chiamiamolo convenzionalmente C_n, ciclico di ordine n).

Proposizione: Se $C_m < C_n$ (in particolare $C_m \triangleleft C_n$) allora $C_m \triangleleft D_n$.

Dimostrazione. Poiché $C_m \triangleleft C_n$, $m \mid n$ ed $\exists\ h \in \mathbb{N}$ tale che $n = mh$. Quindi $C_m = \left\langle r^h \right\rangle$.
Sia $x \in C_m$, $x = \left(r^h\right)^k$. Verifichiamo che C_m sia normale.

$$(s^\epsilon r^i) r^{hk} (s^\epsilon r^i)^{-1} = \begin{cases} \text{se } \epsilon = 0 & \rightarrow & r^{hk} \\ \text{se } \epsilon = 1 & \rightarrow & r^{-i-hk+i} = r^{-hk} \end{cases}$$

Dato che $r^{\pm hk} \in C_m$, tesi. □

Osservazione. In generale non è vero che $H \triangleleft K \triangleleft G \Rightarrow H \triangleleft G$.
In questo caso però oltre ad essere normale C_m è anche l'unico sottogruppo di ordine m. Ciò significa che è caratteristico in C_n.

Definizione: Un sottogruppo H di G si dice *caratteristico* se per ogni automorfismo $\phi : G \to G$

$$\phi(H) = H$$

Quindi possiamo mostrare una dimostrazione alternativa alla proposizione precedente.

Dimostrazione. Sia $x \in D_n$. Vogliamo dimostrare che $xC_mx^{-1} = C_m$.
Sia $\phi_x : G \to G$ l'omomorfismo coniugio (con $x \in G$), tale che $\phi_x(g) = xgx^{-1}$.
Allora $\phi_x : D_n \to D_n$ è un automorfismo che fissa C_n.
Dunque $\phi_x|_{C_n} : C_n \to C_n$ è un automorfismo che fissa C_m, cioè $\phi_x|_{C_n}(C_m) = xC_mx^{-1} = C_m$. □

Tutti i sottogruppi di C_n sono quindi sottogruppi di D_n.
Cerchiamo adesso gli $H < D_n$ tali che $H \nless C_n$.

H contiene un elemento non appartenente a C_n, cioè contiene una riflessione di ordine 2 del tipo sr^k. Una possibilità è che $H = \left\{e, sr^k\right\} \cong C_2$.
È però possibile che $H \cap C_n \neq \{e\}$. In questo caso $H \cap C_n \cong C_m$, $m \mid n$, $C_m = \langle r^{\frac{n}{m}} \rangle$ (l'intersezione di gruppi è un gruppo).
Quindi $H = \langle sr^k, r^{\frac{n}{m}} \rangle \cong D_m$.

Dimostrazione. Evidentemente $\langle sr^k, r^{\frac{n}{m}} \rangle < H$.
Dimostriamo che $H \subseteq \langle sr^k, r^{\frac{n}{m}} \rangle$.
Se per assurdo $\exists \rho \in H \setminus \langle sr^k, r^{\frac{n}{m}} \rangle$, allora per costruzione $\rho \notin H \cap C_n$, quindi ρ è una riflessione.
Notiamo che il prodotto di 2 riflessioni di H è una rotazione, e dunque sta in C_m. Riscrivendo $\rho = sr^k(sr^k\rho)$ si ha che $sr^k \in \langle sr^k, r^{\frac{n}{m}} \rangle$ e $sr^k\rho \in C_m \subseteq \langle sr^k, r^{\frac{n}{m}} \rangle$. Quindi $\rho \in \langle sr^k, r^{\frac{n}{m}} \rangle$. Assurdo. $\square$

Abbiamo quindi visto:

PROPOSIZIONE: I sottogruppi di D_n sono:

- Un unico di tipo C_m per ogni $m \mid n$;
- $\frac{n}{m}$ di tipo D_m per ogni $m \mid n$.

ESEMPIO: I sottogruppi di D_6 sono:

$-C_1 = \{e\}$;	-6 di tipo $D_1 = \left\{e, sr^k\right\}$ con $k = 0, \dots, 5$;
$-C_2 = \langle r^3 \rangle$;	-3 di tipo $D_2 = \langle r^3, sr^k \rangle$ con $k = 0, 1, 2$;
$-C_3 = \langle r^2 \rangle$;	-2 di tipo $D_3 = \langle r^2, sr^k \rangle$ con $k = 0, 1$;
$-C_6 = \langle r \rangle$;	$-$Il sottogruppo banale D_6.

Osservazione. Tra tutti i sottogruppi di D_n gli unici ad essere abeliani sono quelli di tipo C_m e quelli di tipo D_1 (che ha ordine 2) e D_2 (poiché $D_2 = \left\{r^i s^j | r^2 = e, s^2 = e, srs^{-1} = r^{-1}\right\}$ e $srs^{-1} = r^{-1} = r \Rightarrow sr = rs$.).

Osservazione. I gruppi di tipo D_1 sono isomorfi a C_2.

PROPOSIZIONE: Ogni gruppo finito G in cui ogni elemento $\neq e$ ha ordine 2 è abeliano.

Dimostrazione. Siano $a, b \in G$, $a \neq e$, $b \neq e$.
Allora ci sono due possibilità:
– $ab = e \Rightarrow b = a^{-1}$, e quindi $ab = ba = e$;
– $ab \neq e \Rightarrow (ab)^2 = abab = e = aabb = a^2b^2 \Rightarrow ab = ba$. $\square$

2.4 Sottogruppi Normali di D_n

Usando la caratterizzazione per i sottogruppi normali

$$N \lhd G \Leftrightarrow N \text{ è unione di classi di coniugio di } G$$

possiamo studiare le classi di coniugio di D_n per studiarne i sottogruppi normali.

Le classi di coniugio per una rotazione r^h sono costituite dagli elementi ottenuti da xr^hx^{-1} al variare di $x \in D_n$:

- $\{e\}$ se $h = 0$;
- $\left\{r^h, r^{-h}\right\}$ con $h = 1, \dots, \frac{n}{2} - 1$ se n pari, con $h = 1, \dots, \frac{n-1}{2}$ se n dispari;
- $\left\{r^{\frac{n}{2}}\right\}$ se n pari.

Le classi di coniugio per una simmetria sr^k sono costituite dagli elementi ottenuti da xsr^kx^{-1} al variare di $x \in D_n$:

- Se n pari $\{sr^{2i}\}$ al variare di i (cioè tutte le simmetrie con rotazione ad esponente pari sono coniugate);
- Se n pari $\{sr^{2i+1}\}$ al variare di i (cioè tutte le simmetrie con rotazione ad esponente dispari sono coniugate);
- Se n dispari tutte le simmetrie sono coniugate.

Dunque tutti gli $N \triangleleft D_n$ sono:

- Gli $N < C_n$;
- Se $N \not< C_n$, allora contiene una riflessione e almeno tutta la sua classe di coniugio:
  - $\rightarrow$ Se n dispari allora N contiene tutte le riflessioni, in particolare s, sr e $ssr = r$ $\Rightarrow N = \langle s, r \rangle = D_n$;
  - $\rightarrow$ Se n pari allora N contiene almeno metà delle riflessioni (se le contiene tutte allora $N = D_n$) e cioè una delle 2 classi di coniugio. Quindi N è un sottogruppo del tipo $D_{\frac{n}{2}}$ (che sono 2).

2.5 Gruppi di Ordine 8

Quanti e quali sono i gruppi di ordine 8?

Classifichiamo dapprima tutti i gruppi abeliani di ordine 8. Sia G un gruppo abeliano tale che $|G| = 8$.

1. Se contiene un elemento di ordine 8 allora $G = C_8$;
2. Se non contiene un elemento di ordine 8, ma un elemento di ordine 4, allora $C_4 \triangleleft G$. Sia $g \in G \setminus C_4$ e sia $C_4 = \langle g' \rangle$. Allora:
   - $ord(g) = 2 \Rightarrow G = C_4 \times C_2$;
   - $ord(g) = 4$:
     - Se $g^2 \notin C_4 \Rightarrow \langle g^2 \rangle = C_2 \Rightarrow G = C_4 \times C_2$;
     - Se $g^2 \in C_4 \Rightarrow ord(gg') = 2$ e $gg' \notin C_4$. Quindi $\langle gg' \rangle = C_2 \Rightarrow G = C_4 \times C_2$.
3. Se G contiene solo elementi di ordine 1 e 2 allora $G = (C_2)^3$.

Classifichiamo adesso i gruppi non abeliani:

- G non contiene elementi di ordine 8 (altrimenti sarebbe ciclico);
- G non contiene solo elementi di ordine 1 e 2 (altrimenti sarebbe abeliano);

$\Rightarrow G$ contiene C_4, e poiché C_4 ha indice 2 allora è normale.
Sia $g \in G \setminus C_4$ e prendiamo l'omomorfismo di coniugio $\phi_g : C_4 \to C_4$. È ben definito poiché C_4 è normale (e quindi $gC_4g^{-1} \subseteq C_4$) ed è iniettivo e surgettivo. Dunque è un isomorfismo e l'immagine di un generatore è un generatore.
Dato che il numero di generatori di C_4 è 2, abbiamo 2 possibilità:

1. $\phi_g = id_{C_4}$ (cioè ogni generatore viene mandato in se stesso). Consideriamo il centralizzatore di C_4, $Z(C_4) = \{h \in G | hk = kh \ \forall \ k \in C_4\}$, che risulta essere un sottogruppo di G.
   Poiché $C_4 \subseteq Z(C_4)$ e C_4 ha indice 2, allora $C_4 = Z(C_4)$ o $G = Z(C_4)$. Ma essendo $g \in Z(C_4)$, $g \notin C_4$, allora $C_4 \neq Z(C_4)$.
   Dunque $G = Z(C_4)$. Ma allora non è difficile dimostrare (studiando come sono fatti gli elementi $h \in G \setminus C_4$) che il gruppo è abeliano e quindi $G = C_4 \times C_2$.

2. ϕ_g scambia i generatori, cioè $ghg^{-1} = h^{-1} \ \forall \ h \in C_4$. Se $ord(g) = 2$ allora $g^2 = e$ e $gh = h^{-1}g$, cioè $G = D_4$ con C_4 il gruppo delle rotazioni e g una simmetria.
   Se invece $ord(g) = 4$ allora $G = \{g^i h^j | g^4 = e,\ h^4 = e,\ ghg^{-1} = h^{-1}\} = Q_8$ e si dice gruppo dei quaternioni.

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

2.6 Omomorfismi tra Gruppi Diedrali

Quanti sono gli $Hom(D_m, D_n)$?
Per rispondere a questa domanda consideriamo il Teorema di Isomorfismo:

$$\begin{tikzcd}
D_m \arrow[rr, dashed, "\varphi"] \arrow[dr, "\pi"'] & & D_n \\
& D_m/\operatorname{Ker}\varphi \arrow[ur, hook, "\text{iniettiva}"'] &
\end{tikzcd}$$

Grazie al diagramma, trovare tutte le $\varphi \in Hom(D_m, D_n)$ è equivalente a cercare tutte le π surgettive e tutti gli omomorfismi iniettivi da $D_m/\operatorname{Ker}\varphi$ a D_n.
Le proiezioni al quoziente π sono tante quante i sottogruppi normali di D_m, i quali sono:

- Uno di tipo $C_{m'}$ per ogni $m' \mid m$;
- Se m è pari allora 2 sottogruppi del tipo $D_{\frac{m}{2}}$.

$\Rightarrow$ Tutti i gruppi quoziente $D_m/\operatorname{Ker}\varphi$ sono del tipo $D_m/C_{m'} \cong D_{\frac{m}{m'}}$ (la verifica di questo isomorfismo è semplice) con $m' \mid m$ e (se m è pari) 2 diversi gruppi isomorfi a C_2.

Poiché a questo punto dobbiamo cercare gli omomorfismi iniettivi da $D_m/\operatorname{Ker}\varphi$ in D_n, calcoliamo quanti sono i sottogruppi di D_n isomorfi ai gruppi quoziente $D_m/\operatorname{Ker}\varphi$:

- $H < D_n$ tali che $H \cong D_{\frac{m}{m'}}$: ne esistono se e solo se $\frac{m}{m'} \mid n$; in tal caso ce ne sono esattamente $\frac{nm'}{m}$ (+1 se n pari nel caso $m = m'$).

- $H < D_n$ tali che $H \cong C_2$: ce ne sono sempre n ($+1$ se n è pari nel caso $m = m'$).

Per concludere basta notare che un omomorfismo iniettivo da $D_m/\operatorname{Ker}\varphi$ in D_n può essere scritto come composizione di un automorfismo $\psi \in Aut(D_m/\operatorname{Ker}\varphi)$ con l'inclusione in D_n. Nel caso in cui il quoziente abbia la forma di un C_2 il gruppo degli automorfismi è banale, quindi $\psi = id$. Nell'altro caso:

$$\begin{tikzcd}
D_m \arrow[r, "\varphi"] \arrow[d, "\pi"] & D_n \\
D_{\frac{m}{m'}} \arrow[r, "\psi"'] & D_{\frac{m}{m'}} \arrow[u, "\text{inclusione}"']
\end{tikzcd}$$

Dunque, ponendo $h = \frac{m}{m'}$ riepiloghiamo:

- Se m dispari e n dispari:

$$|Hom(D_m, D_n)| = \sum_{h|(m,n)} \underbrace{\phi(h) \cdot h}_{\#Aut(D_h)} \cdot \underbrace{\frac{n}{h}}_{\#\text{incl.}} = \sum_{h|(m,n)} \phi(h) \cdot n$$

- Se m dispari e n pari:

$$|Hom(D_m, D_n)| = \sum_{h|(m,n)} (\phi(h) \cdot n) + 1$$

- Se m pari e n dispari:

$$|Hom(D_m, D_n)| = \sum_{h|(m,n)} (\phi(h) \cdot n) + \underbrace{2n}_{\substack{\#\text{incl. per} \\ 2\text{ Ker}}}$$

- Se m pari e n pari:

$$|Hom(D_m, D_n)| = \sum_{h|(m,n)} (\phi(h) \cdot n) + 1 + 2(n+1)$$

Capitolo 3

Automorfismi e Azioni di Gruppi

Definizione: Un automorfismo di un gruppo G è un omomorfismo $f : G \to G$ bigettivo.

Definizione: Sia G gruppo. Si definisce

$$Aut(G) = \{\phi : G \to G \text{ isomorfismo di gruppi}\}$$

il gruppo degli *automorfismi* di G. È un gruppo rispetto alla composizione.

3.1 Esempi di Gruppi di Automorfismi

- G ciclico ($G \cong \mathbb{Z}$ o $G \cong \mathbb{Z}/m\mathbb{Z}$):

  $\rightarrow$ Caso $\mathbb{Z}$.

  $$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z} \\ & 1 & \mapsto & a \\ & x & \mapsto & ax \end{array}$$

  f è iniettiva se e solo se $a \neq 0$ ed è surgettiva se e solo se $a = \pm 1$.
  Dunque $Aut(\mathbb{Z}) \cong \{\pm id\}$.

  $\rightarrow$ Caso $\mathbb{Z}/m\mathbb{Z}$.
  f è iniettiva se e solo se è surgettiva, e cioè se e solo se $(a, m) = 1$.
  Dunque $Aut(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$.

  Costruiamo esplicitamente un isomorfismo ψ tra i 2 gruppi: $\forall\ f \in Aut(\mathbb{Z}/m\mathbb{Z})$ sia $\psi(f) := f(1) = a$.
  È un omomorfismo in quanto $(f \circ g)(1) = f(g(1)) = f(b) = ab = f(1)g(1)$ con $a = f(1)$ e $b = g(1)$.
  È iniettivo e surgettivo per costruzione. Quindi è un isomorfismo.

- $G = \mathbb{Q}$:
  Sia $f \in Aut(\mathbb{Q})$ e sia $a = f(1)$.
  Poiché $\underbrace{\frac{m}{n} + \ldots + \frac{m}{n}}_{n \text{ volte}} = m$, allora $\underbrace{f\left(\frac{m}{n}\right) + \ldots + f\left(\frac{m}{n}\right)}_{n \text{ volte}} = f(m) = am$ e quindi $f\left(\frac{m}{n}\right) = \frac{am}{n}$.
  $\Rightarrow f(x) = ax$ è bigettiva $\Leftrightarrow a$ è invertibile, cioè $a \neq 0$.
  Dunque $Aut(\mathbb{Q}) \cong \mathbb{Q}^*$.

- $G = (\mathbb{Z}/p\mathbb{Z})^n = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \ldots \times \mathbb{Z}/p\mathbb{Z}}_{n \text{ volte}}$.
  Definendo un prodotto per scalari (usando la somma) si ottiene uno spazio vettoriale con campo degli scalari $\mathbb{Z}/p\mathbb{Z}$.
  Quindi un omomorfismo ha anche la proprietà che $f(mv) = mf(v)$ con $m \in \mathbb{Z}/p\mathbb{Z}$.
  Sapendo che lo spazio delle applicazioni lineari è isomorfo allo spazio delle matrici si ottiene che $Aut\left((\mathbb{Z}/p\mathbb{Z})^n\right) \cong GL\left(n, \mathbb{Z}/p\mathbb{Z}\right)$.

  Osservazione. $Aut\left((\mathbb{Z}/p\mathbb{Z})^n\right)$ non è abeliano per ogni $n \geq 2$.

  Studiamo $|Aut\left((\mathbb{Z}/p\mathbb{Z})^n\right)|$:

$$\begin{array}{llll}
1^a \text{ colonna} & v_1 = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{n,1} \end{pmatrix} \neq 0 & \rightarrow \; p^n - 1 & \text{possibilità} \\
2^a \text{ colonna} & v_2 = \begin{pmatrix} a_{1,2} \\ \vdots \\ a_{n,2} \end{pmatrix} \neq \lambda_1 v_1 & \rightarrow \; p^n - p & \text{possibilità} \\
3^a \text{ colonna} & v_3 = \begin{pmatrix} a_{1,3} \\ \vdots \\ a_{n,3} \end{pmatrix} \neq \lambda_1 v_1 + \lambda_2 v_2 & \rightarrow \; p^n - p^2 & \text{possibilità} \\
\vdots & & & \vdots
\end{array}$$

  Con $\lambda_i \in \mathbb{Z}/p\mathbb{Z}$.
  $\Rightarrow |Aut\left((\mathbb{Z}/p\mathbb{Z})^n\right)| = \prod_{i=0}^{n-1} \left(p^n - p^i\right)$.

- $G = S_n$.
  $Aut(S_n) \cong S_n$ per $n \neq 2$ e per $n \neq 6$.
  Nel caso $n = 2$, dato che l'identità deve andare nell'identità esiste un solo automorfismo, mentre S_2 ha 2 elementi.
  Nel caso $n = 6$ vedremo in seguito che $|Aut(S_6)| = 2 \cdot 6!$.

- $G = D_n$.
  Dato che $D_n = \langle r, s\rangle$, vediamo come può essere fatta l'immagine di un generatore:
  $ord(r) = n \Rightarrow ord\left(f(r)\right) = n$, dunque $f(r)$ deve essere una rotazione (di ordine n).
  $ord(s) = 2 \Rightarrow ord\left(f(s)\right) = 2$, ma $f(s)$ non può essere una rotazione perché altrimenti $\langle f(r), f(s)\rangle \neq D_n$. Quindi $f(s) = sr^h$ con $h = 0, \ldots, n-1$.

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

3.2 Automorfismi Interni

Definizione: Un elemento $f \in Aut(G)$ si dice *automorfismo interno* di G se esiste $g \in G$ tale che $f(x) = gxg^{-1}$ per ogni $x \in G$.

Osservazione. $\forall\ g \in G$ la funzione $\phi : G \rightarrow G$ tale che $\phi(x) = gxg^{-1}$ è un automorfismo di G.
Infatti è un omomorfismo poiché $\phi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi(x)\phi(y)$;
è iniettiva: $gxg^{-1} = e \Rightarrow g^{-1}gxg^{-1}g = g^{-1}g = e$ cioè $x = e$;

è surgettiva: $\forall y \in G$ trovo $x \in G$ tale che $gxg^{-1} = y$, ovvero $x = g^{-1}yg$.

Definizione: Definiamo $Int(G)$ l'insieme degli automorfismi interni di G.

Definizione: Dato un gruppo G si dice *centro* di G

$$Z(G) = \{x \in G | xy = yx \ \forall \ y \in G\}$$

Proposizione: $Z(G) \triangleleft G$ e $Int(G) \cong G/Z(G)$.

Dimostrazione. Dato ϕ_g un automorfismo interno ($\phi_g(x) = gxg^{-1}$), consideriamo la funzione $\phi : G \to Int(G)$ tale che $\phi(g) = \phi_g$.
Verifichiamo che si tratti di un omomorfismo surgettivo:

- È un omomorfismo: $\forall \ x \in G \phi_{gh}(x) = ghxh^{-1}g^{-1} = g\phi_h(x)g^{-1} = (\phi_g \circ \phi_h)(x)$;
- È surgettivo per definizione.

Quindi per il teorema di isomorfismo

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & Int(G) \\ & G/\operatorname{Ker}\phi \arrow[ur, dashed, "\cong"'] & \end{tikzcd}$$

Cerchiamo $\operatorname{Ker}\phi = \{g \in G | \phi_g = id\} = \{g \in G | gxg^{-1} = x \ \forall \ x \in G\} =$
$= \{g \in G | gx = xg \ \forall \ x \in G\} = Z(G)$. Allora essendo un nucleo di un omomorfismo $Z(G) \triangleleft G$ e $G/Z(G) \cong Int(G)$. □

Corollario: $Int(G) \triangleleft Aut(G)$.

Dimostrazione. Le verifiche che $Int(G) < Aut(G)$ vengono tralasciate. Dimostriamo che $\psi Int(G) \psi^{-1} \subseteq Int(G) \ \forall \ \psi \in Aut(G)$.
$\forall \ g, x \in G$ abbiamo

$$\left(\psi \circ \phi_g \circ \psi^{-1}\right)(x) = \psi\left(\phi_g\left(\psi^{-1}(x)\right)\right) = \psi\left(g\psi^{-1}(x)g^{-1}\right) = \psi(g)x\psi(g^{-1}) \ \in Int(G)$$

□

Proposizione: Se G non è abeliano allora $G/Z(G)$ non è un gruppo ciclico.

Dimostrazione. Se $G/Z(G)$ fosse ciclico, allora

$$G/Z(G) = \langle xZ(G) \rangle \quad \Rightarrow G/Z(G) = \{x^m Z(G) \mid m \in \mathbb{Z}\}$$

Siano $g, h \in G$, $g \in x^m Z(G)$ e $h \in x^n Z(G)$. Allora $g = x^m z_1$ e $h = x^n z_2$ con $z_1, z_2 \in Z(G)$.

$$gh = x^m \underbrace{z_1 x^n}_{} z_2 = \underbrace{x^m x^n}_{} \underbrace{z_1 z_2}_{} = x^n \underbrace{x^m z_2}_{} z_1 = x^n z_2 x^m z_1 = hg$$

$\Rightarrow G$ è abeliano. Assurdo. □

Ricordiamo la definizione di sottogruppo caratteristico:
DEFINIZIONE: Un sottogruppo H di G si dice *caratteristico* se $\phi(H) = H \ \forall \ \phi \in Aut(G)$.

Osservazione. Questa condizione è più forte dell'essere un sottogruppo normale, perché $K \triangleleft G$ se $\phi(K) = K \ \forall \ \phi \in Int(G)$.

Osservazione. Dunque $H < G$, H caratteristico $\Rightarrow H \triangleleft G$.

ESERCIZIO: Siano $K < H < G$. Se $H \triangleleft G$ e K è un sottogruppo caratteristico di H, allora $K \triangleleft G$.

3.3 Azioni di Gruppo

Sia $S(X)$ il gruppo delle permutazioni degli elementi di X.

DEFINIZIONE: Un'azione di G su X è un omomorfismo $\phi : G \to S(X)$ che associa a $g \in G$ una permutazione $\phi_g : X \to X$.

Preso un elemento $x \in X$, possiamo studiare 2 oggetti ad esso correlati: un sottogruppo di G e un sottoinsieme di X.

DEFINIZIONE: Sia $\phi : G \to S(X)$ un'azione e sia $x \in X$. Si dice *stabilizzatore* di x il sottogruppo di G

$$Stab(x) = \{g \in G \mid \phi_g(x) = x\}$$

Osservazione. In generale tale sottogruppo non è normale.

DEFINIZIONE: Sia $\phi : G \to S(X)$ un'azione e sia $x \in X$. Si dice *orbita* di x il sottoinsieme di X

$$Orb(x) = \{y \in X \mid \exists \ g \in G \ : \ \phi_g(x) = y\}$$

PROPOSIZIONE: Sia $\phi : G \to S(X)$ un'azione e siano $x, y \in X$. La relazione $x \sim y \Leftrightarrow \exists \ g \in G$ tale che $\phi_g(x) = y$ è una relazione di equivalenza.

PROPOSIZIONE: Sia $\phi : G \to S(X)$ un'azione e sia $x \in X$.

$$\phi_g(x) = \phi_h(x) \Leftrightarrow gStab(x) = hStab(x)$$

Dimostrazione. $\Rightarrow$.
$\phi_g(x) = \phi_h(x) \Rightarrow \phi_{h^{-1}g}(x) = x \Rightarrow h^{-1}g \in Stab(x) \Rightarrow g \in hStab(x) \Rightarrow gStab(x) = hStab(x)$.
La prima implicazione deriva dall'applicazione ad entrambi i membri dell'omomorfismo $\phi_{h^{-1}} = (\phi_h)^{-1}$. □

Dimostrazione. $\Leftarrow$.
$gStab(x) = hStab(x) \Rightarrow g \in hStab(x)$, cioè $g = hk$ con $k \in Stab(x)$.
$\phi_g(x) = \phi_{hk}(x) = \phi_h(\phi_k(x)) = \phi_h(x)$. □

Osservazione. L'ultima proposizione permette di mettere in corrispondenza biunivoca le classi laterali sinistre di $Stab(x)$ con gli elementi dell'orbita di x.

Corollario: Se G è un gruppo finito (e quindi $Stab(x)$ è finito) allora

$$[G : Stab(x)] = |Orb(x)|$$

Dunque $|G| = |Stab(x)| \cdot |Orb(x)|$.

3.4 Azione di Coniugio

Sia G gruppo e $X = G$.

$$\begin{array}{rccc} \phi: & G & \to & S(X) \\ & g & \mapsto & \phi_g \end{array}$$

con $\phi_g(x) = gxg^{-1}$ l'automorfismo interno associato a g.

$$\operatorname{Ker} \phi = Z(G)$$

$$Stab(x) = \{g \in G \mid \phi_g(x) = x\} = \left\{g \in G \mid gxg^{-1} = x\right\} = \{g \in G \mid gx = xg\} = Z(x)$$

Osservazione. $Z(x)$ prende il nome di *centralizzatore* di x.

Osservazione. $Z(x) = G \Leftrightarrow x \in Z(G)$.

Osservazione. $Z(x) \supseteq Z(G)\ \forall\ x \in G$.

Osservazione. Se G è abeliano $Z(x) = G = Z(G)\ \forall\ x \in G$.

$$Orb(x) = \{\phi_g(x) \mid g \in G\} = \left\{gxg^{-1} \mid g \in G\right\} = \text{classe di coniugio di } x$$

3.5 Coniugio sui Sottogruppi di G

Sia G gruppo. Sia $X = \{H \mid H < G\}$. Prendendo ϕ l'azione di coniugio abbiamo che

$$Stab(H) = \{g \in G \mid \phi_g(H) = H\}$$

Osservazione. Se $H \triangleleft G$ allora $Stab(H) = G$ e $Orb(H) = \{H\}$ (anche se G non è finito); se $H \ntriangleleft G$, allora $Stab(H) \neq G$.

Definizione: Dato un gruppo G, si definisce *normalizzatore* di un sottogruppo H il suo stabilizzatore secondo l'azione di coniugio $Stab(H) = N(H) = \{g \in G \mid gHg^{-1} = H\}$.

Osservazione. Il normalizzatore di H è il più grande sottogruppo N di G tale che $H \triangleleft N$.

$$Orb(H) = \text{insieme dei sottogruppi coniugati ad } H$$

Osservazione. Se G è finito, si ha $|Orb(H)| = [G : N(H)]$.

Osservazione. Normalizzatore e centralizzatore di un sottogruppo sono due sottogruppi distinti secondo azioni distinte: il normalizzatore infatti è lo stabilizzatore di un elemento secondo l'azione di coniugio sui sottogruppi di G, il centralizzatore di un sottogruppo è l'intersezione dei centralizzatori dei suoi elementi (e l'azione in considerazione è il coniugio sugli elementi di G).

ESEMPIO: $G = D_4$.
Escludendo i sottogruppi banali, si ha che D_4 ha 3 diversi sottogruppi di ordine 4 e 5 sottogruppi di ordine 2. I sottogruppi di ordine 4 (avendo indice 2) sono tutti normali.
$Z(D_4)$ ha certamente non più di 2 elementi, altrimenti $D_4/Z(D_4)$ sarebbe ciclico e qunidi D_4 abeliano. Assurdo. È semplicemente verificabile che $Z(D_4) = \{e, r^2\}$.
Se un sottogruppo $H = \{e, x\}$ di ordine 2 è normale allora $x \in Z(D_4)$; quindi tra i sottogruppi di ordine 2 l'unico ad essere normale è $\langle r^2 \rangle$.
Come è fatto il normalizzatore di un altro generico sottogruppo $K = \langle g_K \rangle$ di ordine 2?
Sappiamo che $N(K) \supseteq K$, $N(K) \supseteq Z(G)$ e $N(H) \neq G$. Allora $N(K) = \langle r^2, g_K \rangle$ e $Orb(H) = \{g_K, rg_K r^{-1}\}$.

ESERCIZIO: Sia $X = \mathbb{Z}/m\mathbb{Z}$, $G = Aut(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Se $x \in \mathbb{Z}/m\mathbb{Z}$ allora $Orb(x) = \{y \in \mathbb{Z}/m\mathbb{Z} \mid ord(x) = ord(y)\}$.

3.6 Automorfismi di Gruppi Abeliani Finiti

Studiamo il gruppo degli automorfismi di un gruppo finito G abeliano. Per il Teorema di Struttura $G \cong G_{p_1} \times \ldots \times G_{p_k}$ con $p_i \big| |G|$ e ogni G_p è caratteristico. Dunque studiare $Aut(G)$ è equivalente a trattare gli automorfismi di ogni $G_{p_i} \cong \mathbb{Z}/p_i^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_i^{e_n}\mathbb{Z}$.

Sia dunque $G = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{e_n}\mathbb{Z}$ con p primo e $1 \leq e_1 \leq \ldots \leq e_n$.
Sia x_j un generatore di $\mathbb{Z}/p^{e_j}\mathbb{Z}\ \forall\ j$.
Sia $\varphi \in Aut(G)$, $\varphi(x_j) = \sum_{i=1}^n a_{ij}x_i$ con $a_{ij} \in \mathbb{Z}/p^{e_i}\mathbb{Z}$.

Condizione necessaria (e sufficiente) affinché φ sia un omomorfismo (e quindi un endomorfismo di G) è che $ord(\varphi(x_j)) \mid ord(x_j) = p^{e_j}$.
Poiché $ord(x_i) = p^{e_i}\ \forall i$, se $p^k \mid a_{ij}$ e $p^{k+1} \nmid a_{ij}$ con $k \leq e_i$ allora l'ordine di $a_{ij}x_i$ è uguale a $p^{e_i - k}$.

$$\Rightarrow p^{e_i - k} \leq p^{e_j} \Leftrightarrow p^{e_i - e_j} \mid a_{ij}$$

Dunque se per ogni i, j tali che $i > j$ si ha che $p^{e_i - e_j} \mid a_{ij}$ allora $\varphi \in End(G)$ e possiamo rappresentarlo matricialmente (grazie all'isomorfismo tra applicazioni lineari e matrici).
Definiamo

$$R = \left\{(a_{ij}) \in \mathcal{M}(n, \mathbb{Z}) \big|\ p^{e_i - e_j} \mid a_{ij}\ \forall i > j\ \wedge\ a_{ij} \in \mathbb{Z}/p^{e_i}\mathbb{Z}\ \forall\ i, j\right\}$$

Con semplici verifiche possiamo notare che $(R, +, \cdot)$ è un anello non commutativo.

Prendiamo l'omomorfismo di anelli $\pi : R \to End(G)$ che associa ad un elemento di R l'endomorfismo di G associato a tale matrice. Tale omomorfismo è surgettivo per come è stato definito R e iniettivo perché l'endomorfismo nullo $0(x_j) = \sum_{i=1}^n a_{ij}x_i = (a_{1j},\ a_{2j},\ \ldots,\ a_{nj}) = 0 \Leftrightarrow a_{ij} = 0\ \forall\ i, j$.
Dunque π è un isomorfismo di anelli.

Studiamo quando $A = (a_{ij}) \in R$ definisce un elemento di $Aut(G)$:

Sia $\bar{A} \in \mathcal{M}(n, \mathbb{F}_p)$.

Dimostriamo che:

Proposizione: $\pi(A) \in Aut(G) \Leftrightarrow \bar{A} \in GL(n, \mathbb{F}_p)$.

Dimostrazione. $\Rightarrow$.
Se $\pi(A) \in Aut(G) \Rightarrow \exists\ \pi(B) \in Aut(G)$ (e di conseguenza, vista la surgettività di π, $\exists\ B \in R$) tale che $\pi(A)\pi(B) = id_G$. Dunque $\pi(AB) = id_G$. Vista la bigettività di π, segue che $AB = id_R$ e quindi $\bar{A}\bar{B} = id_{GL(n,\mathbb{F}_p)}$, cioè $\bar{A}$ è invertibile. $\square$

Dimostrazione. $\Leftarrow$.
$\bar{A}$ ha inversa in $GL(n, \mathbb{F}_p)$. Sia $\bar{B}$ l'inversa. Poichè $GL(n, \mathbb{F}_p)$ è finito, $\bar{A}$ ha ordine finito. Quindi $\exists\ l \in \mathbb{N}$ tale che $\bar{A}^l = id_{GL(n,\mathbb{F}_p)} \Rightarrow \bar{B} = \bar{A}^{l-1} \Rightarrow B = A^{l-1}$ è un elemento di R.

Quindi $AB = id_R + pM$ per una certa matrice M.
$(AB)^{p^N} = id_R + p^{N+1}M'$ con $N \geq e_i\ \forall\ i$ e M' una certa matrice. Chiamando $C = B(AB)^{p^N-1}$ si ha che $\pi(AC) = \pi(id_R + p^{N+1}M') = \pi(id_R) + \pi(p^{N+1}M') = id_G$. Le ultime uguaglianze derivano dal fatto che π è un omomorfismo di anelli e che $\pi(p^{N+1}M') = 0$.
Dunque $\pi(AC) = \pi(A)\pi(C) = id_G \Rightarrow \pi(A)$ è invertibile in $End(G)$. $\square$

3.7 Automorfismi di Q_8

Ricordando che $Q_8 = \{g^i h^j | g^4 = e,\ h^4 = e,\ ghg^{-1} = h^{-1}\}$, studiamone gli automorfismi. Il primo generatore deve andare in un elemento di ordine 4 (per un totale di 6 modi); il secondo generatore deve andare in un altro elemento di ordine 4, ma non deve appartenere al sottogruppo generato dall'immagine del primo generatore. Dunque per h ci sono un totale di 4 possibilità di scelta.
Dunque $|Aut(Q_8)| \leq 24$.

Cerchiamo adesso una limitazione nell'altro verso. Poiché gli elementi di ordine 4 vanno in elementi di ordine 4 (che sono 6), potremmo analizzare $Aut(Q_8) \to S_6$, cioè le permutazioni degli elementi di ordine 4. In realtà però tali elementi vengono permutati a coppie $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$. Quindi possiamo considerare l'omomorfismo $\psi : Aut(Q_8) \to S_3$.

Prendendo $\varphi_1 : \begin{cases} i \mapsto j \\ j \mapsto\ k \\ k \mapsto i \end{cases}$, si ha che $\psi(\varphi_1) = (1,\ 2,\ 3)$.

Prendendo $\varphi_2 : \begin{cases} i \mapsto j \\ j \mapsto\ i \\ k \mapsto -k \end{cases}$, si ha che $\psi(\varphi_2) = (1,\ 2)$.

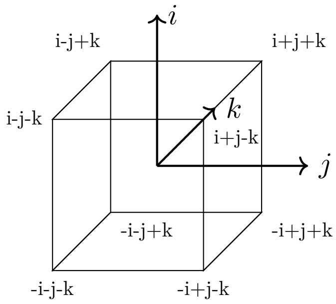
Dunque $\operatorname{Im}\psi$ ha almeno 4 elementi (il sottogruppo generato da $(1,\ 2,\ 3)$ e $(1,\ 2)$), e quindi $\operatorname{Im}\psi = S_3$.

Cerchiamo $\operatorname{Ker}\psi$: poiché $iji^{-1} = -j$ e $iki^{-1} = -k$, allora $Int(Q_8) < \operatorname{Ker}\psi$. Essendo $Int(Q_8) \cong Q_8/Z(Q_8) \cong Q_8/_{\{\pm 1\}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,

$$|Aut(Q_8)| = |\operatorname{Ker}\psi| \cdot |\operatorname{Im}\psi| = |\operatorname{Ker}\psi| \cdot |S_3| \geq 4 \cdot 6 = 24$$

Quindi $|Aut(Q_8)| = 24$.

Dimostriamo che $Aut(Q_8) \cong S_4$.
Prendiamo un cubo in $\mathbb{R}^3 = \langle i, j, k \rangle$:



Un automorfismo di Q_8 è una isometria di $\mathbb{R}^3$ che permuta i vertici del cubo (la base ortonormale $\{i, j, k\}$ subisce una trasformazione che permuta $\pm i, \pm j, \pm k$) pur conservando gli inversi. Possiamo quindi limitarci a osservare come si permutano le diagonali del cubo. Sia $\psi : Aut(Q_8) \to S_4$ e siano:

1. Diagonale 1: $\{i + j + k, -i - j - k\}$;
2. Diagonale 2: $\{i + j - k, -i - j + k\}$;
3. Diagonale 3: $\{i - j - k, -i + j + k\}$;
4. Diagonale 4: $\{i - j + k, -i + j - k\}$;

Prendendo $\varphi_1 : \begin{cases} i \mapsto j \\ j \mapsto k \\ (k \mapsto i) \end{cases}$ si ha che la prima diagonale resta fissa, la seconda va nella terza, la terza nella quarta e la quarta nella seconda. Poniamo dunque $\psi(\varphi_1) = (2\ 3\ 4)$.

Prendendo l'automorfismo di coniugio rispetto a i, $\varphi_2 : \begin{cases} i \mapsto i \\ j \mapsto iji^{-1} = -j \\ (k \mapsto -k) \end{cases}$ si ha che le diagonali 1 e 3 si scambiano così come le diagonali 2 e 4. Poniamo dunque $\psi(\varphi_2) = (1\ 3)(2\ 4)$.

Analogamente gli altri automorfismi di coniugio generano i 2-2-cicli. Dunque $Int(Q_8) \mapsto K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ detto gruppo di Klein.
Allora $\operatorname{Im}\psi$ contiene tutte le permutazioni pari, cioè A_4, e quindi $|\operatorname{Im}\psi| \geq 12$.

Prendendo infine $\varphi_3 : \begin{cases} i \mapsto j \\ j \mapsto i \\ (k \mapsto -k) \end{cases}$ si ha che le prime 2 diagonali si scambiano, mentre le altre 2 restano fisse, cioè $\psi(\varphi_3) = (1\ 2)$.

$\operatorname{Im}\psi$ contiene A_4 e almeno una permutazione dispari (contiene cioè almeno 13 elementi), quindi $\operatorname{Im}\psi = S_4$.
Da qui per cardinalità si conclude che ψ è un isomorfismo.

Capitolo 4

Gruppo delle Permutazioni S_n

Sia $G = S_n$ e $X = \{1, \dots, n\}$. Parlando dell'azione di G su X abbiamo che $\varphi : G \to S(X)$ è l'identità, e per ogni $x \in X$ $Orb(x) = X$ e $Stab(x) \cong S_{n-1}$.

Restringiamoci invece a lavorare su un sottogruppo di G.
Sia $\sigma \in G$ e $H = \langle \sigma \rangle$.
L'azione di H su X determina una partizione di X in orbite

$$X = \bigsqcup_{x \in \mathcal{R}} Orb(x)$$

Sia Y un'orbita: $Y = Orb(x)$ con $x \in X$.
Poiché H è ciclico, $Y = \{\sigma^m(x) \mid m \in \mathbb{Z}\}$.
Y è finito, quindi esistono m, m' ($m > m'$ tali che $\sigma^m(x) = \sigma^{m'}(x)$; $\Rightarrow \sigma^{m-m'}(x) = x$. Sia h il più piccolo esponente positivo tale che $\sigma^h(x) = x$.

Proposizione: $\sigma^a(x) = \sigma^b(x) \Leftrightarrow a \equiv b \pmod h$

Dimostrazione. $\Rightarrow$.
Supponiamo $a \geq b$.
$\sigma^a(x) = \sigma^b(x) \Rightarrow \sigma^{a-b}(x) = x$. Dividendo per h si ha che $a - b = qh + r$
$\sigma^{a-b}(x) = (\sigma^r \circ \sigma^{qh})(x) = \left(\sigma^r \circ (\sigma^h)^q\right)(x) = \sigma^r(x) = x \;\Rightarrow r = 0.$ □

Dimostrazione. $\Leftarrow$.
Supponiamo $a = b + th$. $\sigma^a(x) = (\sigma^b \circ \sigma^{ht})(x) = \sigma^b(x)$ □

Abbiamo quindi dimostrato che $Orb(x) = \left\{x, \sigma(x), \dots, \sigma^{h-1}(x)\right\}$ ha h elementi.

Definizione: Un ciclo è una permutazione che ha una sola orbita non banale (con più di un elemento).

Osservazione. Dunque ogni permutazione $\sigma \in S_n$ si decompone in modo unico (a meno dell'ordine) come prodotto di cicli disgiunti.

Corollario: I cicli sono un insieme di generatori di S_n.

Definizione: Si definisce *lunghezza* di un ciclo la cardinalità dell'orbita del ciclo.

Definizione: Una trasposizione è un ciclo di lunghezza 2.

Osservazione. È sempre possibile scrivere un ciclo come prodotto di trasposizioni.

Esempio: $\sigma = (1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$
In generale $(a_1\ a_2\ \dots\ a_k) = \underbrace{(a_1\ a_k)\cdots(a_1\ a_2)}_{k-1 \text{ trasp.}}$

Osservazione. Dunque ogni permutazione si può scrivere come prodotto di trasposizioni (ma in generale non in modo unico).

Corollario: Le trasposizioni sono un insieme di generatori di S_n.

Proposizione: Data una permutazione $\sigma \in S_n$ per ogni scrittura $\sigma = \tau_1 \cdot \ldots \cdot \tau_k$ con τ_i una trasposizione $\forall\ i$, k ha sempre la stessa parità.

Dimostrazione. Consideriamo la funzione $\phi : S_n \to \{\pm 1\}$ data da

$$\phi(\sigma) = \prod_{\{a,b\} \subseteq \{1,\ldots,n\}} \frac{\sigma(a) - \sigma(b)}{a - b}$$

Sicuramente $|\varphi(\sigma)| = 1$ poiché sia al numeratore che al denominatore appaiono tutte le coppie $\{a, b\} \subseteq \{1, \ldots, n\}$.

Dimostriamo che φ è un omomorfismo:

$$\begin{aligned}\varphi(\sigma \circ \tau) &= \prod_{\{a,b\} \subseteq \{1,\ldots,n\}} \frac{(\sigma \circ \tau)(a) - (\sigma \circ \tau)(b)}{a - b} = \\ &= \prod_{\{a,b\} \subseteq \{1,\ldots,n\}} \frac{\sigma(\tau(a)) - \sigma(\tau(b))}{\tau(a) - \tau(b)} \ \frac{\tau(a) - \tau(b)}{a - b} = \varphi(\sigma) \cdot \varphi(\tau)\end{aligned}$$

Consideriamo la trasposizione $\tau = (x\ y)$ e calcoliamo quanto vale $\varphi(\tau)$.
Distinguiamo le coppie $\{a, b\}$ in 3 casi:

1. $\{a, b\} \cap \{x, y\} = \emptyset$;
2. $\{a, b\} \cap \{x, y\} = \{x\}$ oppure $\{y\}$;
3. $\{a, b\} = \{x, y\}$

Caso 1:

$$\varphi(\tau) = \prod_{\{a,b\} \cap \{x,y\} = \emptyset} \frac{a - b}{a - b} = 1$$

Caso 2: Ci sono due possibilità.

$$\varphi(\tau) = \prod_{\{a,x\} \subseteq \{1,\ldots,n\}} \frac{\tau(a) - \tau(x)}{a - x} = \prod_{\{a,x\} \subseteq \{1,\ldots,n\}} \frac{a - y}{a - x}$$

$$\varphi(\tau) = \prod_{\{a,y\} \subseteq \{1,\ldots,n\}} \frac{\tau(a) - \tau(y)}{a - y} = \prod_{\{a,y\} \subseteq \{1,\ldots,n\}} \frac{a - x}{a - y}$$

Moltiplicando tra loro i risultati derivanti da questi tipi di coppie si ha

$$\varphi(\tau) = \prod_{\{a,b\}\cap\{x,y\}=\{x\} \text{ oppure } \{y\}} \frac{\tau(a)-\tau(b)}{a-b} = 1$$

Caso 3: $\varphi(\tau) = \frac{\tau(x)-\tau(y)}{x-y} = \frac{y-x}{x-y} = -1$.
$\Rightarrow \varphi(\tau) = -1$.
Prendendo quindi una $\sigma \in S_n$, $\sigma = \tau_1 \cdot \ldots \cdot \tau_k$ allora $\varphi(\sigma) = \varphi(\tau_1) \cdot \ldots \cdot \varphi(\tau_k) = (-1)^k$.
Quindi se $\varphi(\sigma) = (-1)^k$ allora la parità di k è determinata. $\square$

4.1 Classi di Coniugio di Permutazioni

Prendiamo un ciclo $c = (a_1 \ \ldots \ a_k)$ e studiamone la classe di coniugio secondo elementi di S_n.

$$\sigma(a_1 \ \ldots \ a_k)\sigma^{-1}$$

Poniamo $\sigma(a_i) = b_i$ per ogni i.
Dividiamo il problema in 2 casi:

- $\sigma c \sigma^{-1}(x)$ con $x \in \{b_1, \ldots, b_k\}$. Allora

$$b_i \xrightarrow{\sigma^{-1}} a_i \xrightarrow{c} a_{i+1} \xrightarrow{\sigma} b_{i+1}$$

- $\sigma c \sigma^{-1}(x)$ con $x \notin \{b_1, \ldots, b_k\}$ e $\sigma(y) = x$. Allora $y \notin \{a_1, \ldots, a_k\}$ e

$$x \xrightarrow{\sigma^{-1}} y \xrightarrow{c} y \xrightarrow{\sigma} x$$

$\Rightarrow \sigma(a_1 \ \ldots \ a_k)\sigma^{-1} = (b_1 \ \ldots \ b_k)$
Quindi la classe di coniugio di un ciclo di lunghezza k è formata da tutti e soli i cicli di lunghezza k.
Di conseguenza, poiché $\forall\ \alpha, \beta$ cicli si ha $\sigma\alpha\beta\sigma^{-1} = \sigma\alpha\sigma^{-1}\ \sigma\beta\sigma^{-1}$ allora i coniugati di una permutazione τ sono tutte e sole le permutazioni che si decompongono in prodotto di cicli della stessa lunghezza dei cicli di τ.

4.2 Formula delle Classi e p-gruppi

Sia G un gruppo; l'azione di coniugio permette di identificare lo stabilizzatore di un elemento con il centralizzatore.

Abbiamo già visto che

- Se G è infinito, possiamo soltanto dire che G è unione (disgiunta) di orbite di elementi di G;
- Se G è un gruppo finito, allora $|G| = |Z(x)| \cdot |Orb(x)|$.

Possiamo però riscrivere la relazione per i gruppi finiti utilizzando proprio che G è unione di orbite:

$$|G| = \sum_{x\in\mathcal{R}} |Orb(x)| = \sum_{x\in\mathcal{R}} \frac{|G|}{|Z(x)|}$$

Suddividiamo adesso la somma in 2 casi distinti:

1. $x \in Z(G)$, cioè $Z(x) = G$. $\Rightarrow \frac{|G|}{|Z(x)|} = 1$;
2. $x \notin Z(G)$, cioè $Z(x) \neq G$. $\Rightarrow \frac{|G|}{|Z(x)|} \neq 1$.

Quindi

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

DEFINIZIONE: Sia p un primo. Un p-gruppo è un gruppo finito di ordine p^n per un certo $n \in \mathbb{N}$.

La formula delle classi ha un'immediata applicazione nel caso dei p-gruppi. Infatti

$$p^n = |Z(G)| + \sum_{x\in\mathcal{R}'} \frac{p^n}{|Z(x)|} = |Z(G)| + \textit{ multiplo di } p \;\Rightarrow\; p \mid |Z(G)|$$

Ovvero $Z(G) \neq \{e\}$.

COROLLARIO: Se $|G| = p^2$ con p primo, allora G è abeliano.

Dimostrazione.

$$|Z(G)| = \begin{cases} 1 \to \text{impossibile, visto sopra} \\ p \\ p^2 \end{cases}$$

Se $|Z(G)| = p$, allora il quoziente $G/Z(G)$ è ciclico perchè di cardinalità p. Ma allora G è abeliano, e quindi $G = Z(G)$. Assurdo.

$\Rightarrow |Z(G)| = p^2 = |G| \;\Rightarrow G = Z(G) \Rightarrow G$ è abeliano. $\square$

PROPOSIZIONE: Sia G un p-gruppo e sia $H < G$ con $H \neq G$. Allora $N(H) \supsetneq H$.

Dimostrazione. Suddividiamo la dimostrazione in 2 casi:

- $H \not\supseteq Z(G)$. Allora $\exists\ z \in Z(G)$ tale che $z \notin H$. Ma $z \in N(H)$, quindi abbiamo la tesi;
- $H \supseteq Z(G)$. Procediamo per induzione sull'ordine di H.
  Consideriamo
  $$\begin{array}{rccc} \pi: & G & \to & G/Z(G) \\ & H & \mapsto & \bar{H} \end{array}$$
  Poiché in un p-gruppo $Z(G)$ non è mai banale, allora $|\bar{H}| < |H|$, e quindi per ipotesi induttiva $N(\bar{H}) \supsetneq \bar{H}$ e $N(\bar{H}) \triangleright \bar{H}$.
  Ma allora $H \triangleleft\ \pi^{-1}\left(N(\bar{H})\right)$.
  Guardando le cardinalità di H e di $\pi^{-1}\left(N(\bar{H})\right)$ si ha dunque che $H \subsetneq \pi^{-1}\left(N(\bar{H})\right) \subseteq N(H)$ (perché $N(H)$ è il più grande sottogruppo in cui H è normale).

□

Proposizione: Sia G un p-gruppo e $H \triangleleft G$ con $H \neq \{e\}$. Allora $H \cap Z(G) \neq \{e\}$.

Dimostrazione. Utilizzando la caratterizzazione di un sottogruppo normale come unione di classi di coniugio possiamo riscrivere la formula delle classi restringendola ad H.

$$|H| = |H \cap Z(G)| + \sum_{x \in \mathcal{R}'_H} \frac{|G|}{|Z(x)|}$$

Dato che p divide tutta la sommatoria e p divide anche $|H|$, allora $p \big| |H \cap Z(G)|$. □

4.3 Cardinalità del Normalizzatore di un Sottogruppo Ciclico

Ricordiamo la definizione di normalizzatore:

Definizione: Dato un gruppo G, si definisce *normalizzatore* di un sottogruppo H il sottogruppo $N(H) = \{g \in G \mid gHg^{-1} = H\}$.

Osservazione. La differenza tra $N(H)$ e $Z(H)$ sta nel fatto che il centralizzatore fissa gli elementi di H puntualmente, mentre il normalizzatore fissa l'insieme H in generale.

Proposizione: Per ogni $\sigma \in S_n$

$$|N(<\sigma>)| = |Z(\sigma)| \cdot |Aut(<\sigma>)|$$

Dimostrazione. Costruiamo un omomorfismo

$$\begin{array}{cccc} \varphi : & N(<\sigma>) & \to & Aut(<\sigma>) \\ & \tau & \mapsto & \varphi_\tau \end{array}$$

con $\varphi_\tau(\sigma^a) = \tau\sigma^a\tau^{-1}$.
Si può notare immediatamente che $\operatorname{Ker}\varphi = Z(\sigma)$. Per giungere alla tesi dobbiamo verificare che l'omomorfismo sia surgettivo.

Sia $\alpha \in Aut(<\sigma>)$. Sia $\alpha(\sigma) = \sigma^d$ con $(ord(\sigma), d) = 1$.
Se $\sigma = c_1 \cdot \ldots \cdot c_k$ decomposizione in cicli allora $\sigma^d = c_1^d \cdot \ldots \cdot c_k^d$ è una decomposizione in cicli di lunghezze uguali a quelle di σ.

Cerchiamo quindi una permutazione τ che coniughi σ con σ^d. Ma, una volta stabilito il primo elemento di ogni ciclo, τ esiste ed è unica (poiché esplicitamente determinata a partire da σ e σ^d).

Abbiamo quindi trovato che per ogni $\alpha \in Aut(<\sigma>)$ esiste una τ_α tale che $\varphi_{\tau_\alpha} = \alpha$, cioè φ è surgettiva.

Per il teorema di isomorfismo, infine, $|N(<\sigma>)| = |\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi| = |Z(\sigma)| \cdot |Aut(<\sigma>)|$. □

Osservazione. Se σ è un ciclo di ordine n, allora

$$\sigma^d \begin{cases} \text{se } (d,n) = 1 & \text{è un } n\text{-ciclo} \\ \text{se } (d,n) = m & \text{è prodotto di } m \ \frac{n}{m}\text{-cicli} \end{cases}$$

4.4 Semplicità di A_n

DEFINIZIONE: Un gruppo si dice *semplice* se non ha sottogruppi normali non banali.

PROPOSIZIONE: A_n è semplice per ogni $n \geq 5$.

Dimostrazione. Per induzione su n:
Passo base $n = 5$.
A_5 è costituito dall'identità, dai 5-cicli, dai 3-cicli e dai 2-2-cicli.
Sia $H \triangleleft A_5$.

- Se H contiene un 3-ciclo, allora per normalità li contiene tutti (20 elementi). Ma allora, poiché $(a\ b\ c)(b\ d\ a) = (b\ d)(a\ c)$, contiene anche tutti i 2-2-cicli (altri 15 elementi), e quindi per cardinalità genera tutto A_5.

- Se H contiene un 2-2-ciclo, allora per normalità li contiene tutti (15 elementi). Ma poiché $(a\ b)(c\ d)(c\ d)(a\ e) = (a\ e\ b)$, contiene tutti i 3-cicli (20 elementi) e quindi genera A_5.

- Se H contiene un 5-ciclo, allora per normalità contiene tutta la sua classe di coniugio (212 elementi). Ma poiché $(a\ b\ c\ d\ e)(a\ c\ b\ d\ e) = (a\ d)(b\ e)$, allora contiene anche tutti i 2-2-cicli (ulteriori 15 elementi); inoltre $(a\ b\ c\ d\ e)(a\ b\ e\ d\ c) = (a\ c\ b)$ e dunque contiene altri 20 elementi (i 3-cicli). Quindi genera A_5.

Dunque $H = A_5$, cioè A_5 è semplice.
Passo induttivo $n > 5$.
Sia $A_n > G_i := \{\sigma \in A_n \mid \sigma(i) = i\} \cong A_{n-1}$. Per ipotesi induttiva G_i è semplice per ogni i.
Sia $N \triangleleft A_n$. Allora $N \cap G_i \triangleleft G_i$, quindi o $N \cap G_i = G_i$ o $N \cap G_i = \{e\}$.

- Se esiste i tale che $G_i \cap N = G_i$ allora N contiene i 3-cicli e i 2-2-cicli di G_i; allora per ipotesi di normalità contiene tutti i 3-cicli e i 2-2-cicli, che generano A_n.

- Se $N \cap G_i = \{e\}$ per ogni i, allora nessun elemento di N fissa un elemento di $\{1, \ldots, n\}$. Quindi se $\sigma(i) = \tau(i)$, con $\sigma, \tau \in N$, allora $\sigma^{-1}\tau(i) = i$, cioè $\sigma = \tau$.

  Preso $N \ni \sigma = c_1 \cdot \ldots \cdot c_k$ cicli disgiunti di ordini $r_1 \geq \ldots \geq r_h$:

  - Se $r_1 \geq 3$, $c_1 = (i_1\ \ldots\ i_{r_1})$:
    Coniugando σ con $\rho = (i_3\ j\ k)$ tale che $(j\ k) \neq (i_1\ i_2)$. N è normale, quindi il coniugato sta in N.
    $\tau = \rho\sigma\rho^{-1}$; $\tau(i_1) = i_2$ e $\sigma(i_1) = i_2$. Ma $\tau(i_2) = j$ e $\sigma(i_2) = i_3$. Assurdo.
  - Se $r_i = 2$ per ogni i:
    Allora σ è composizione di trasposizioni disgiunte $\sigma = (i\ j)(k\ l)\ldots$.
    Coniugando σ con $\rho = (l\ p\ q)$ tale che $p, q \neq \{i,\ j,\ k,\ l\}$, si ottiene un elemento $\tau = \rho\sigma\rho^{-1}$ tale che $\tau(k) = l$, $\sigma(k) = p \neq l$, ma $\tau(i) = \sigma(i) = j$. Assurdo.

Dunque $N = A_n$, cioè A_n è semplice. □

Capitolo 5

Prodotti Semidiretti

Siano G_1, G_2 gruppi. Sia $X = G_1 \times G_2$. Sia

$$\begin{array}{rccc} \varphi: & G_2 & \to & Aut(G_1) \\ & g_2 & \mapsto & \varphi_{g_2} \end{array}$$

Definiamo una moltiplicazione in X in questo modo:

$$(x_1, x_2)(y_1, y_2) := (x_1\varphi_{x_2}(y_1), x_2y_2)$$

Allora X è un gruppo con questa operazione.
Infatti:

- L'operazione è associativa:

$$\begin{aligned} ((x_1, x_2)(y_1, y_2))\,(z_1, z_2) &= (x_1\varphi_{x_2}(y_1), x_2y_2)(z_1, z_2) = \\ &= (x_1\varphi_{x_2}(y_1)\varphi_{x_2y_2}(z_1), x_2y_2z_2) \end{aligned}$$

$$\begin{aligned} (x_1, x_2)\,((y_1, y_2)(z_1, z_2)) &= (x_1, x_2)(y_1\varphi_{y_2}(z_1), y_2z_2) = \\ &= (x_1\varphi_{x_2}(y_1)\varphi_{x_2y_2}(z_1), x_2y_2z_2) \end{aligned}$$

- (e_1, e_2) è l'elemento neutro;
- Elemento inverso:

$$(x_1, x_2)(y_1, y_2) = (e_1, e_2) = (x_1\varphi_{x_2}(y_1), x_2y_2) \Rightarrow \begin{cases} y_2 = x_2^{-1} \\ \varphi_{x_2}(y_1) = x_1^{-1} \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} y_2 = x_2^{-1} \\ y_1 = \varphi_{x_2}^{-1}(x_1^{-1}) = \varphi_{x_2^{-1}}(x_1^{-1}) \end{cases}$$

Tale gruppo si dice *prodotto semidiretto* di G_1 e G_2 e si denota con $G_1 \rtimes_\varphi G_2$.

Osservazione. Il prodotto diretto è un caso particolare del prodotto semidiretto, quando φ associa l'identità ad ogni elemento di G_2 (ovvero è l'omomorfismo nullo).

Osservazione. $G_1 \rtimes_\varphi \{e\} \lhd G_1 \rtimes_\varphi G_2$. Infatti è il nucleo dell'omomorfismo di proiezione $\pi_2 : G_1 \rtimes_\varphi G_2 \to G_2$.

Osservazione. $\{e\} \rtimes_\varphi G_2$ in generale non è normale. Infatti:

$$(x_1, x_2)(e, y_2)(x_1, x_2)^{-1} = (x_1, x_2y_2)(\varphi_{x_2}^{-1}(x_1^{-1}), x_2^{-1}) = (x_1\varphi_{x_2y_2x_2^{-1}}(x_1^{-1}), x_2y_2x_2^{-1})$$

Scegliendo (x_1, x_2) in modo tale che $\varphi_{x_2 y_2 x_2^{-1}}$ sia non banale e che x_1^{-1} non sia un punto fisso si ottiene la tesi.

Osservazione. $G_1 \rtimes_\varphi G_2$ non è un gruppo abeliano.

Esempio: $G_1 = \mathbb{Z}/n\mathbb{Z} =< x >$, $G_2 = \mathbb{Z}/2\mathbb{Z} =< y >$.

$$\begin{array}{cccc} \varphi: & \mathbb{Z}/2\mathbb{Z} & \to & Aut(\mathbb{Z}/n\mathbb{Z}) & \cong (\mathbb{Z}/n\mathbb{Z})^* \\ & e_2 & \mapsto & id & \\ & y & \mapsto & (x \mapsto x^{-1}) & \end{array}$$

Siano $g = (x, e)$ e $h = (e, y)$. Allora $ord(g) = n$, $ord(h) = 2$ e

$$(e, y)(x, e)(e, y)^{-1} = (x^{-1}, e) = (x, e)^{-1}$$

cioè $hgh^{-1} = g^{-1}$. $\Rightarrow \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \cong D_n$.

Proposizione: Sia G un gruppo e siano H, K due sottogruppi di G tali che:

1. $H \triangleleft G$;
2. $H \cap K = \{e\}$;
3. $HK = G$ (o equivalentemente $|H| \cdot |K| = |G|$ nel caso in cui $|G| < \infty$);

Allora $G \cong H \rtimes_\varphi K$ con $\varphi_k(h) = khk^{-1}$.

Dimostrazione. Sia $f : H \rtimes_\varphi K \to G$ tale che $f((h, k)) = hk$. Dimostriamo che è un isomorfismo.

- È un omomorfismo:

$$f\left((h, k)(h', k')\right) = f\left(\left(hkh'k^{-1}, kk'\right)\right) = hkh'k'$$

$$f\left((h, k)\right) f\left((h', k')\right) = hkh'k'$$

- È surgettivo per l'ipotesi 3.
- È iniettivo:

$$\mathrm{Ker}(f) = \{(h, k) | hk = e\} = \left\{(h, h^{-1}) \middle| h \in H \cap K\right\} = \{e\}$$

□

Esempio: $G = \{f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} | f(x) = ax + b,\ a \in (\mathbb{Z}/n\mathbb{Z})^*,\ b \in \mathbb{Z}/n\mathbb{Z}\}$
G è un gruppo (il gruppo delle affinità) con l'operazione di composizione.

Prendiamo

$$\begin{array}{cccc} \psi: & G & \to & (\mathbb{Z}/n\mathbb{Z})^* \\ & (x \mapsto ax + b) & \mapsto & a \end{array}$$

$H = \mathrm{Ker}\,\psi = \{f \in G | f(x) = x + b,\ b \in \mathbb{Z}/n\mathbb{Z}\} \cong \mathbb{Z}/n\mathbb{Z}$ è il sottogruppo delle traslazioni.
Un K tale che $K \cap H = \{e\}$ è il sottogruppo delle omotetie

$$K = \{f \in G | f(x) = ax,\ a \in (\mathbb{Z}/n\mathbb{Z})^*\} \cong (\mathbb{Z}/n\mathbb{Z})^*$$

Essendo $G = HK$ allora $G \cong H \rtimes_\psi K$ con $\psi_k(h) = k \circ f \circ k^{-1}$.

Vediamo che, ponendo $h(x) = x + b$ e $k(x) = cx$, $\psi_k(h) = c((c^{-1}x) + b) = x + cb$ e quindi

$$G \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\psi (\mathbb{Z}/n\mathbb{Z})^* \quad \text{con} \quad \begin{array}{rccc} \psi : & (\mathbb{Z}/n\mathbb{Z})^* & \to & Aut\,(\mathbb{Z}/n\mathbb{Z}) \\ & k & \mapsto & k \end{array}$$

con $k \in Aut\,(\mathbb{Z}/n\mathbb{Z})$ intesa come la moltiplicazione per k.
Quindi ψ è l'isomorfismo identico.

Proposizione: Sia G un gruppo di ordine pq con p, q primi e $p < q$. Allora $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ dove $\varphi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

Dimostrazione. Per Cauchy esiste un elemento di ordine p e uno di ordine q, quindi esistono K e H di quelle due cardinalità.

Dimostriamo che il sottogruppo di ordine q è unico.
Se per assurdo esistessero $H_1 \neq H_2$, $|H_1| = |H_2| = q$ allora

$$|H_1 H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|} = |H_1| \cdot |H_2| = q^2 > pq = |G|$$

che è assurdo.
Dunque H è caratteristico in G e anche normale.
Inoltre, poiché p e q sono primi, $H \cap K = \{e\}$. Allora $G \cong H \rtimes_\varphi K \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ dove $\varphi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. □

Osservazione. Il prodotto diretto (ovvero con φ banale) esiste sempre; in questo caso G è ciclico di ordine pq.

Osservazione. Un prodotto semidiretto non banale esiste se e solo se $p \mid q-1$. Tutti questi semidiretti sono isomorfi tra loro, a prescidere dalla definizione di φ.

5.1 Gruppi di Ordine p^3

Sia p un primo diverso da 2. Cerchiamo di caratterizzare tutti i gruppi di ordine p^3.

Per il Teorema di Struttura se G è abeliano allora è della forma

$$\mathbb{Z}/p^3\mathbb{Z} \qquad \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \qquad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Se invece G non è abeliano, cerchiamo 2 sottogruppi di ordine p e p^2 per poter applicare il teorema di decomposizione in prodotto semidiretto.

Essendo G un p-gruppo allora di sicuro esiste un sottogruppo $H < G$ di ordine p^2, quindi abeliano ($H \cong \mathbb{Z}/p^2\mathbb{Z} \vee H \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$) e normale poiché $H \subsetneq N(H)$.

Dimostriamo che, quando $p \neq 2$, è sempre possibile trovare un $K < G$, $|K| = p$ e tale che $H \cap K = \{e\}$. Sia $x \in G \setminus H$; se $ord(x) = p$ allora abbiamo concluso prendendo $K = \langle x \rangle$. Se $ord(x) = p^2$, consideriamo $R = \langle x \rangle \cong \mathbb{Z}/p^2\mathbb{Z}$.
Osserviamo che in questo caso possiamo supporre $H \cong \mathbb{Z}/p^2\mathbb{Z}$ poiché in $H \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ci sono $p+1$ sottogruppi distinti di ordine p e quindi se ne troverebbe almeno uno con

intersezione banale con R e dunque avremmo concluso la ricerca.

Consideriamo adesso l'omomorfismo $\phi : H \to Aut(R)$ tale che $\phi(h) = \phi_h : \ r \mapsto hrh^{-1}$. Notiamo dapprima che $\operatorname{Im}\phi = \phi(H) \neq \{id\}$: se per assurdo così fosse allora $\forall h \in H$, $\forall r \in R$ $hr = rh \Rightarrow H \subseteq Z(r), R \subseteq Z(r) \Rightarrow G = HR \subseteq Z(r)$ $\forall r \in R \Rightarrow R \subseteq Z(G)$. Ma allora $|Z(G)| = p^3$ (assurdo perchè G non è abeliano) o $Z(G) = R$ (assurdo perché $G/Z(G)$ sarebbe ciclico).
Dunque $|\phi(H)| \mid |H| = p^2 \wedge |\phi(H)| \mid |Aut(R)| = p(p-1) \Rightarrow |\phi(H)| \mid p$ e $|\phi(H)| \neq 1 \Rightarrow |\phi(H)| = p$. Dal momento che $Aut(R)$ è ciclico si ha che $\phi(H)$ è l'unico sottogruppo di ordine p di $Aut(R)$. Sia $y \in H$ un generatore di H e prendiamo un generatore del sottogruppo di ordine p di $Aut(R)$, $\phi_h : x \to x^{1+p}$ (possiamo considerare questo senza perdita di generalità).

Ricapitolando, abbiamo queste relazioni: $G = \langle x, y\rangle$, $x^{p^2} = y^{p^2} = e$, $yxy^{-1} = x^{1+p}$. Cerchiamo adesso, se esiste, un j tale che $xy^j \notin H$ e $ord(xy^j) = p$. Se trovato, ponendo $K = \langle xy^j \rangle$ allora $HK = G$ e $H \cap K = \{e\}$.

Dimostriamo per induzione su n che $(xy^j)^n = x^{n+jp\frac{n(n-1)}{2}}y^{jn}$: il passo base è ovvio; per dimostrare il passo induttivo utilizziamo prima altri 2 risultati.

- $yx^n = x^{n(1+p)}y$. Dimostriamolo per induzione su n.
  Il passo base deriva dall'identità $yxy^{-1} = x^{1+p}$.
  Passo induttivo: $yx^{n+1} = yx^n x = x^{n(1+p)}yx = x^{n(1+p)}x^{1+p}y = x^{(n+1)(1+p)}y$.
- $y^n x = x^{1+np}y^n$. Dimostriamolo per induzione su n.
  Il passo base deriva dall'identità $yxy^{-1} = x^{1+p}$.
  Passo induttivo: $y^{n+1}x = yy^n x = yx^{1+np}y^n = x^{(1+np)(1+p)}y^{n+1} = x^{1+(n+1)p}y^{n+1}$.

Dimostriamo adesso il passo induttivo della prima uguaglianza:

$$\begin{aligned}(xy^j)^{n+1} = (xy^j)^n xy^j &= x^{n+jp\frac{n(n-1)}{2}}y^{jn}xy^j = \\ &= x^{n+jp\frac{n(n-1)}{2}}(y^{jn}x)y^j = \\ &= x^{n+jp\frac{n(n-1)}{2}}(x^{1+jnp}y^{jn})y^j = \\ &= x^{n+1+jp\frac{n(n+1)}{2}}y^{j(n+1)}\end{aligned}$$

Dunque $(xy^j)^p = x^{p+j\frac{p^2(p-1)}{2}}y^{jp}$; ciò significa che se $p \neq 2$ si ha $p^2 \mid \frac{p^2(p-1)}{2}$ ovvero $(xy^j)^p = x^p y^{jp}$. A questo punto $x^p, y^p \in H \cap R$, e in particolare $x^{-p} \in H \cap R = \langle y^p \rangle$. Quindi esiste $j \in \{1, \dots, p-1\}$ tale che $(y^p)^j = x^{-p}$ da cui $(xy^j)^p = x^p y^{jp} = x^p (y^p)^j = x^p x^{-p} = e$.

Abbiamo così dimostrato l'esistenza di due sottogruppi $H \triangleleft G$, $K < G$ tali che $|H| = p^2$, $|K| = p$, $G \cong H \rtimes K$.

- Caso 1: $G \cong \mathbb{Z}/p^2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$. L'omomorfismo $\varphi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^*$ è definito da $\varphi(y) = \varphi_y : \ x \longmapsto yxy^{-1}$. Se $H = \langle x \rangle$, $K = \langle y \rangle$ allora possiamo considerare $\varphi_y : \ x \longmapsto yxy^{-1} = x^{1+p}$.
- Caso 2: $G \cong (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$. Vediamo come è fatto l'omomorfismo $\varphi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \cong GL(2, \mathbb{F}_p)$. Definiamo $\varphi_y(x) = M^y x$ con $M \in$

$GL(2, \mathbb{F}_p)$ di ordine p. Ad esempio, possiamo prendere $M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

Verifichiamo che $ord(M) = p$: sia $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$; allora $M = I + N \Rightarrow M^p = (I + N)^p = I^p + p \cdot \ldots + N^p$ dato che $p \mid \binom{p}{i}$ $\forall\ i = 1, \ldots, p-1$. Ma poiché $N^2 = 0$ allora anche $N^p = 0 \Rightarrow M^p = I^p = I$, e cioè $ord(M) = p$.

Capitolo 6

Teoria degli Anelli

Definizione: Si definisce *anello* un insieme A dotato di 2 operazioni ($+$ e $\cdot$) tale che:

1. $(A, +)$ è un gruppo abeliano;
2. La moltiplicazione è associativa;
3. Valgono le proprietà distributive della moltiplicazione con l'addizione e viceversa.

Definizione: In un anello A si dice *divisore di zero* un elemento $x \in A$ tale per cui esiste $y \in A \setminus \{0\}$ tale che $xy = 0$ oppure $yx = 0$. Poniamo D l'insieme dei divisori di zero.

Tipi di Anelli:

- Anello commutativo: $\forall\ x, y\ \in A\ xy = yx$;
- Anello con unità: $\exists 1 \in A$ tale che $\forall\ x \in A\ x \cdot 1 = 1 \cdot x = x$;
- Anello privo di divisori di zero;
- Dominio di integrità: anello commutativo con 1 privo di divisori di zero;
- Campo (o corpo commutativo): anello commutativo con 1 in cui $\forall\ x \neq 0\ \exists x^{-1} \in A$ tale che $xx^{-1} = x^{-1}x = 1$;
- Corpo non commutativo (o anello di divisione): anello non commutativo con 1 in cui $\forall\ x \neq 0\ \exists x^{-1} \in A$ tale che $xx^{-1} = x^{-1}x = 1$

Osservazione. Se A è un corpo $A \setminus \{0\}$ è un gruppo con la moltiplicazione.

Osservazione. Se $|A| \geq 2$ e $1 \in A$ allora $0 \neq 1$.

Osservazione. Se $1 \in A$, allora $A^* = \{x \in A \mid x \text{ è invertibile}\}$ è un gruppo con la moltiplicazione.

Proposizione: Sia A un anello commutativo con unità. Sia D l'insieme dei divisori di zero. Allora:

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

Dimostrazione. 1.
Sia $x \in D \cap A^*$: allora, poiché $x \in D$, $\exists y \neq 0$ tale che $xy = 0$, e poiché $x \in A^*$ $\exists z$ tale che $zx = 1$. Dunque $y = 1 \cdot y = zxy = z \cdot 0 = 0$ assurdo. □

Dimostrazione. 2.
Se $x \notin D$ vale la proprietà di cancellazione:
$xa = xb \Rightarrow xa - xb = 0 \Rightarrow x(a - b) = 0 \Rightarrow a = b$.
Supponiamo quindi $x \notin D$ e consideriamo l'insieme $\{1, x, x^2, \ldots, x^n, \ldots, x^m, \ldots\}$. Poiché $|A| < \infty$ allora esistono n, m (con $m > n$) tali che $x^m = x^n$. Ma allora $x^{m-n} = 1$, e cioè $x \cdot x^{m-n-1} = 1$, ovvero $x^{-1} = x^{m-n-1}$. □

Corollario: Un dominio di integrità finito è un campo.

Teorema (Teorema di Wedderburn): Un anello di divisione finito privo di divisori di zero è un campo.

Definizione: Un *ideale* I di un anello A è un sottoinsieme di A tale che:

1. I è un sottogruppo di A per l'addizione;
2. $\forall a \in A$ $\forall i \in I$ $ai \in I$ (ideale sinistro) oppure $ia \in I$ (ideale destro).

Osservazione. Se A è un anello commutativo ogni ideale è bilatero.

Proposizione: Sia A un anello commutativo con unità e sia I un ideale di A. Allora A/I è un anello commutativo con le operazioni:

- $(x + I) + (y + I) := (x + y) + I$;
- $(x + I)(y + I) := xy + I$.

Dimostrazione. Per la somma non c'è niente da dimostrare, dato che vale per i gruppi.
Dimostriamo che si tratta di una buona definizione per la moltiplicazione:
Se $x + I = x' + I$ e $y + I = y' + I$ allora vediamo che $xy + I = x'y' + I$. Infatti $x \in x' + I$, e quindi $x = x' + i_1$; $y \in y' + I$, e quindi $y = y' + i_2$.
$xy = (x' + i_1)(y' + i_2) = x'y' + i_1y' + x'i_2 + i_1i_2 \ \in x'y' + I \ \Rightarrow xy + I = x'y' + I$.

L'operazione è associativa perché lo è in A.
L'operazione è commutativa perché lo è in A.
Le proprietà di distributività valgono perché valgono in A. □

Osservazione. A/I è con unità $(1 + I)$, a meno che $I = A$ e quindi $A/I = \{0\}$.

Osservazione. L'intersezione di 2 ideali di A è un ideale di A.

Definizione: Sia S un sottoinsieme di A anello commutativo con unità. Si dice ideale generato da S (notazione: (S)) il più piccolo ideale di A contenente S.

Primo caso: $S = \{x\}$.
$(S) = (x) = Ax = \{ax \mid a \in A\}$. Infatti $Ax \subseteq (S)$ per la proprietà di assorbimento; $(S) \subseteq Ax$ poiché Ax è un ideale (semplice verifica).

Definizione: Un ideale si dice principale se è generato da un solo elemento.

Osservazione. $(x) = \{0\} \Leftrightarrow x = 0$.

Osservazione. $(x) = A \Leftrightarrow x \in A^*$.

Secondo caso: $S = \{x_1, \dots, x_n\}$ finito.
$(S) = (x_1, \dots, x_n) = Ax_1 + \dots + Ax_n = \{a_1x_1 + \dots + a_nx_n \mid a_i \in A\ \forall i\}$. Le due inclusioni sono analoghe a sopra.

Caso generale: S qualsiasi. $S = \{x_\lambda\}_{\lambda \in \Lambda}$.
$(S) =$ combinazioni lineari finite degli $x_\lambda =$
$= \{a_1x_{\lambda_1} + \dots + a_nx_{\lambda_n} \mid n \in \mathbb{N}\ \lambda_i \in \Lambda, a_i \in A\ \forall i\}$

Proposizione: Gli ideali di $\mathbb{Z}$ sono tutti e soli gli ideali della forma $m\mathbb{Z} = (m)$ con $m \geq 0$.

$$m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$$

$$S = m\mathbb{Z} \cup n\mathbb{Z} \Rightarrow (S) = (m, n) = (d) = m\mathbb{Z} + n\mathbb{Z}$$

Osservazione. Un anello A è un campo se e solo se i suoi unici ideali sono $\{0\}$ e A.

6.1 Operazioni tra Ideali

Sia A un anello commutativo con unità, e siano I, J due ideali di A.
Allora possiamo definire delle operazioni tra ideali come segue.

Definizione: $I \cap J$ è il più grande ideale contenuto in I e in J.

Definizione: $I + J = \{i + j \mid i \in I, j \in J\}$ è il più piccolo ideale che contiene I e J.

Definizione: $I \cdot J = \{a_1i_1j_1 + \dots + a_ni_nj_n \mid n \in \mathbb{N}, a_k \in A, i_k \in I, j_k \in J\}$ è un ideale (banale verifica). Possiamo anche scrivere $I \cdot J = (ij)_{i \in I, j \in J}$.

Osservazione. La definizione di $I \cdot J$ è diversa da quella naturale perché se fosse stata $\{ij \mid i \in I, j \in J\}$ non sarebbe stato un ideale.
Esempio: Nell'anello $\mathbb{R}[x, y]$, $I = J = (x, y) = \{f \cdot x + g \cdot y \mid f, g \in \mathbb{R}[x, y]\}$.
$x^2 \in I \cdot J, y^2 \in I \cdot J$, ma $x^2 + y^2$ non è prodotto di un elemento di I per un elemento di J; dunque nella definizione di $I \cdot J$ c'è la necessità di aggiungere le combinazioni lineari in generale e non i singoli prodotti elemento per elemento.

Osservazione. $I \cdot J \subseteq I \cap J$. Infatti un insieme di generatori di $I \cdot J$ è dato dagli ij con $i \in I, j \in J$. Ma $ij \in I \cap J$, e dunque vale l'inclusione.

Definizione: I, J si dicono relativamente primi se $I + J = A = (1)$.

Proposizione: Se $I + J = A$ allora $I \cdot J = I \cap J$.

Dimostrazione. $\subseteq$. Ovvia. □

Dimostrazione. $\supseteq$. Per ipotesi $\exists\ x \in I, \exists\ y \in J$ tali che $x + y = 1$. Sia $a \in I \cap J$; allora $a = a \cdot 1 = a(x + y) = ax + ay \in I \cdot J$. □

Definizione: $I : J = \{x \in A \mid xJ \subseteq I\}$ è un ideale.

Esempio: In $\mathbb{Z}$, $I = (m)$, $J = (n)$.
$m = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ con $a_i > 0$; $n = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k} \cdot q_1^{c_1} \cdot \ldots \cdot q_s^{c_s}$ con $b_i \geq 0$, $c_i > 0$.
Allora $I : J = (p_1^{x_1} \cdot \ldots \cdot p_k^{x_k})$ con $x_i = \max\{a_i - b_i, 0\}$.

Definizione: Ann(I)= $\{x \in A \mid xI = (0)\}$ è un ideale bilatero se I è un ideale bilatero o sinistro di A.
Verifica:
È banalmente un sottogruppo additivo; vediamo la proprietà di assorbimento.
$x \in$Ann(I), $b \in A$; $(xb)a = x(ba) = 0$ perché $a \in I \Rightarrow ba \in I$ (essendo I un ideale sinistro).
Dunque $xb \in$Ann(I). $(bx)a = b(xa) = b \cdot 0 = 0$, quindi $bx \in$Ann(I).

Definizione: $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\}$ è un ideale. Verifichiamolo:

È un gruppo additivo abeliano: infatti $0 \in \sqrt{I}$; se $x \in \sqrt{I}$ allora $x^m \in I$, dunque $(-x)^m \in I \Rightarrow -x \in \sqrt{I}$; se $x^m, y^n \in I$ allora $(x + y)^{m+n-1} = \sum_{i=1}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i} \in I$, poiché per ogni monomio $i \geq m$ oppure $m + n - 1 - i \geq n$.
La regola di assorbimento è banale.

Osservazione. $\sqrt{(0)} = \{$elementi nilpotenti di $A\}$.

Esempio: In $\mathbb{Z}/m\mathbb{Z}$ con $m = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ $\sqrt{(0)} = (p_1 \cdot \ldots \cdot p_k) = p_1 \cdot \ldots \cdot p_k\mathbb{Z}/m\mathbb{Z}$.

6.2 Omomorfismi di Anelli

Definizione: Una funzione $f : A \to B$ con A e B anelli si dice omomorfismo di anelli se vengono conservate le operazioni, cioè:

- $f(x + y) = f(x) + f(y)$;
- $f(xy) = f(x)f(y)$.

Esempio: Gli unici omomorfismi $f : \mathbb{Z} \to \mathbb{Z}$ sono quello nullo e l'identità, infatti:

$$b = f(1) = f(1 \cdot 1) = f(1)f(1) = b^2$$

Osservazione. È sempre vero che $f(0) = 0$, ma non è vero che $f(1) = 1$. Infatti:
Esempio: $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ tale che $f(x) = 3x$. Allora $f(xy) = 3xy$ e $f(x)f(y) = 3x3y = 3^2xy = 3xy$.

Come deve essere fatto dunque $f(1)$?

Se $f(1) = b$, allora $f(x) = f(1 \cdot x) = f(1)f(x) = b \cdot f(x)$. Quindi b deve essere unità in $f(A)$, ovvero nell'immagine dell'omomorfismo.

Proposizione: Se B è un dominio di integrità e $f \neq 0$ allora $f(1) = 1$.

Dimostrazione. Sia $b = f(1)$. Allora per come visto sopra $b = b^2$, cioè $b(b-1) = 0$. Poiché B è un dominio di integrità, $b = 0 \vee b = 1$. $\square$

Osservazione. Se $f(1) = 1$ allora $f(x^{-1}) = f(x)^{-1}$.

Proposizione: Sia $\operatorname{Ker} f = \{x \in A \mid f(x) = 0\}$. Allora:

1. $\operatorname{Ker} f$ è un ideale di A;

2. $f(x) = f(y) \;\Leftrightarrow\; x + \operatorname{Ker} f = y + \operatorname{Ker} f$.

Dimostrazione. 1.
$x \in \operatorname{Ker} f \Rightarrow f(ax) = f(a)f(x) = f(a) \cdot 0 = 0 \Rightarrow ax \in \operatorname{Ker} f$. $\square$

Dimostrazione. 2. Deriva dal fatto che f è un omomorfismo di gruppi. $\square$

Osservazione. Gli ideali di A sono tutti e soli i nuclei di omomorfismi $f : A \to B$ con B un anello qualsiasi.

Teorema (Teorema di Isomorfismo per Anelli): Sia $f : A \to B$ un omomorfismo di anelli, sia $I = \operatorname{Ker} f$. Allora esiste un unico omomorfismo $\varphi : A/I \to B$ che rende commutativo il seguente diagramma:

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & B \\
& A/I \arrow[ur, dashed, "\varphi"'] &
\end{tikzcd}$$

φ è iniettiva. Inoltre è surgettiva $\Leftrightarrow$ f lo è.

Dimostrazione. Se φ esiste, allora è unica perchè deve essere in particolare un omomorfismo di gruppi. Quindi, dato il teorema di isomorfismo per gruppi, resta da vedere che φ conserva il prodotto. $\varphi(x + I) = f(x) \Rightarrow \varphi((x + I)(y + I)) = \varphi(xy + I) = f(xy) = f(x)f(y) = \varphi(x + I)\varphi(y + I)$. $\square$

Proposizione: Siano I, J ideali di A con $I \subseteq J$. Allora

$$A/J \cong (A/I)\,/\,(J/I)$$

Dimostrazione. Siano $\pi_1 : A \to A/I$ e $\pi_2 : A/I \to (A/I)\,/\,(J/I)$ le proiezioni canoniche tali che $\pi_1(x) = x + I$ e $\pi_2(x + I) = \overline{x + I}$. Allora $\pi_2 \circ \pi_1$ è surgettiva perché composizione di funzioni surgettive; inoltre $\operatorname{Ker}(\pi_2 \circ \pi_1) = J$, dato che $\overline{x + I} = \bar{0} \Leftrightarrow x + I \in J \Leftrightarrow x \in J$. Quindi per il teorema di isomorfismo si conclude. $\square$

Proposizione: Siano I, J due ideali di A. Allora

$$I/\,(I \cap J) \cong (I + J)\,/J$$

Dimostrazione. Sia $f : I \to (I + J)\,/J$ tale che $f(x) = x + J$. È un omomorfismo surgettivo e $\operatorname{Ker} f = \{x \in I \mid x + J \subseteq J\} = \{x \in I \mid x \in J\} = I \cap J$.
Dunque si conclude per il teorema di isomorfismo. $\square$

Teorema (Corrispondenza biunivoca tra Ideali): Sia $f : A \to B$ un omomorfismo di anelli surgettivo. Sia $I = \operatorname{Ker} f$. Allora esiste una corrispondenza biunivoca tra gli ideali di A che contengono I e gli ideali di B.

Osservazione. Per dire che J ideale di $A \Rightarrow f(J)$ ideale di B serve che f sia surgettiva.
Esempio: $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ l'inclusione. $i((2))$ non è un ideale, dato che $\mathbb{Q}$ è campo.

Definizione: Siano A e B anelli, con A sottoanello di B e sia $b \in B$. Si definisce omomorfismo di sostituzione l'omomorfismo $\varphi_b : A[x] \to B$ tale che $\varphi_b(f) = f(b)$.

Teorema (Teorema Cinese del Resto per Anelli): Sia A un anello commutativo con unità, siano I, J ideali di A relativamente primi. Allora

$$A/IJ \cong A/(I \cap J) \cong A/I \times A/J$$

Dimostrazione. Consideriamo l'omomorfismo $f : A \to A/I \times A/J$ tale che $f(x) = (x + I, x + J)$.
$\operatorname{Ker} f = \{x \in A |\, x + I = I, x + J = J\} = \{x \in A \mid x \in I, x \in J\} = I \cap J = IJ$.
Per vedere che sia surgettivo è sufficiente mostrare che $(\bar{1}, \bar{0}) = (1 + I, J) \in \operatorname{Im} f$ e $(\bar{0}, \bar{1}) = (I, 1 + J) \in \operatorname{Im} f$.
Poiché $I + J = A$, esistono $x \in I$, $y \in J$ tali che $x + y = 1$. Dunque $x = 1 - y$, e cioè $x \in I$ e $x \in 1 + J$; analogamente $y = 1 - x \in J \cap (1 + I)$.
$\Rightarrow f(x) = (\bar{0}, \bar{1})$ e $f(y) = (\bar{1}, \bar{0})$. □

6.3 Ideali Primi e Massimali

Definizione: Si dice *caratteristica* di un anello A (char(A)) il minimo intero positivo m (se esiste) tale che $mx = 0 \ \forall\, x \in A$.
Se non esiste nessun intero positivo con questa proprietà, allora definiamo $\operatorname{char} A = 0$.

Osservazione. Se A è commutativo con unità allora

$$char(A) = \begin{cases} ord_+(1) & \text{se è finito} \\ 0 & \text{se } ord_+(1) = +\infty \end{cases}$$

Osservazione. I multipli di 1 (sottogruppo additivo generato da 1) è un sottoanello di A che si dice sottoanello fondamentale.
$(m \cdot 1)(n \cdot 1) = \underbrace{(1 + \ldots + 1)}_{m \text{ volte}} \underbrace{(1 + \ldots + 1)}_{n \text{ volte}} = \underbrace{1 + \ldots + 1}_{mn \text{ volte}} = mn \cdot 1$.

Osservazione. Chiamando F il sottoanello fondamentale, si ha che $F \cong \mathbb{Z}$ o $F \cong \mathbb{Z}/m\mathbb{Z}$.

Osservazione. Se A è un dominio di integrità allora char(A)= 0 oppure char(A)= p con p primo.

Definizione: Sia A un anello commutativo con unità e sia P un ideale proprio di A ($P \neq A$). P si dice *primo* se $xy \in P \Rightarrow x \in P \lor y \in P$.

Definizione: Sia A un anello commutativo con unità e sia M un ideale proprio di A ($M \neq A$). M si dice *massimale* se, per ogni ideale I tale che $M \subseteq I \subseteq A$, allora

$I = M \vee I = A$.

Osservazione. A/P è dominio di integrità se e solo se P è un ideale primo. Infatti al quoziente vale $\overline{xy} = \overline{x} \cdot \overline{y} = \overline{0} \Rightarrow \overline{x} = \overline{0} \vee \overline{y} = \overline{0}$ se e solo se P è un ideale primo.

Osservazione. A/M è campo se e solo se M è un ideale massimale. Infatti, grazie alla corrispondenza tra ideali possiamo dire che gli unici ideali nel quoziente sono $\overline{I} = \{\overline{0}\}$ e $\overline{I} = A/M$ se e solo se M è un ideale massimale.

COROLLARIO: Se I è un ideale massimale allora è anche un ideale primo.

Osservazione. A è un dominio di integrità se e solo se $\{0\}$ è un ideale primo.

Osservazione. A è un campo se e solo se $\{0\}$ è un ideale massimale.

DEFINIZIONE: Un elemento $p \in A$, $p \neq 0$ e $p \notin A^*$ si dice *primo* se $p \mid xy \Rightarrow p \mid x \vee p \mid y$ o, equivalentemente, se (p) è un ideale primo.

DEFINIZIONE: Sia A un dominio di integrità. Un elemento $m \in A$, $m \neq 0$ e $m \notin A^*$ si dice *irriducibile* se $m = xy \Rightarrow x \in A^* \vee y \in A^*$.

Osservazione. m irriducibile NON è equivalente a $M = (m)$ massimale. Invece è equivalente alla proprietà che $M = (m)$ è massimale all'interno dell'insieme degli ideali principali.

PROPOSIZIONE: Sia A un dominio di integrità. Se p è un elemento primo allora p è irriducibile.

Dimostrazione. $p = xy \Rightarrow p \mid xy \Rightarrow p \mid x \vee p \mid y$.
Se $p \mid x$ allora $x = pa$, e quindi $p = pay \Rightarrow ay = 1 \Rightarrow y \in A^*$.
Se $p \mid y$ allora $y = pb$, e quindi $p = xpb \Rightarrow xb = 1 \Rightarrow x \in A^*$. $\square$

Osservazione. p irriducibile $\not\Rightarrow p$ primo.
ESEMPIO: $A = \mathbb{Z}[\sqrt{-5}]$. $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
Vediamo che 2 è irriducibile: $2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \Rightarrow$ passando alle norme al quadrato $4 = (a^2 + 5b^2)(c^2 + 5d^2) = 1 \cdot 4 = 2 \cdot 2$.
Ma $2 \neq a^2 + 5b^2 \ \forall a, b \in \mathbb{Z}$. Se invece $1 = a^2 + 5b^2$ e $4 = c^2 + 5d^2$, allora $a = 1, b = 0, c = 2, d = 0$. Ma allora $2 = 1 \cdot 2$, e 1 è invertibile.
Dunque 2 è irriducibile.

Vediamo però che 2 non è primo: $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ ma $2 \nmid (1 \pm \sqrt{-5})$.

DEFINIZIONE: Sia A un anello commutativo con unità. Un ideale Q si dice *primario* se $xy \in Q \Rightarrow x \in Q \vee \exists n \in \mathbb{N}$ tale che $y^n \in Q$.

DEFINIZIONE: Sia A un anello commutativo con unità. Un ideale Q si dice *quasi primario* se $xy \in Q \Rightarrow \exists n \in \mathbb{N}$ tale che $x^n \in Q \vee y^n \in Q$.

PROPOSIZIONE: Sia A un anello commutativo con unità. Q primario $\Rightarrow \sqrt{Q}$ primo.

Dimostrazione. $ab \in \sqrt{Q} \Rightarrow (ab)^n \in Q$ per un certo $n \in \mathbb{N}$.
Se $a \notin \sqrt{Q}$ allora $a^m \notin Q \ \forall m \in \mathbb{N} \Rightarrow b^n \in Q$. Dunque $\sqrt{Q}$ è primo. $\square$

Proposizione: Sia A un anello commutativo con unità. Q è primario se e solo se i divisori di zero in A/Q sono nilpotenti.

Dimostrazione. $\Leftarrow$.
Ovvia utilizzando la definizione di ideale primario. □

Dimostrazione. $\Rightarrow$.
Sia $\overline{a} \in A/Q$ un divisore di zero, cioè $\exists \overline{b} \in A/Q,\ \overline{b} \neq 0$ tale che $\overline{ab} = 0$. Dunque $ab \in Q$. Ma $a \notin Q$, dato che $\overline{a} \neq 0$. Quindi $b^n \in Q$ per un certo $n \in \mathbb{N} \Rightarrow \overline{b}^n = 0$.
Ma poiché A è un anello commutativo $ab = ba$, ed essendo $b \notin Q$ allora deve essere $a^n \in Q$ per un certo $n \in \mathbb{N}$ e dunque $\overline{a}$ nilpotente. □

Proposizione: Sia A un anello commutativo con unità. $\sqrt{Q}$ massimale $\Rightarrow Q$ primario.

Dimostrazione. Sia $M = \sqrt{Q}$ massimale (e dunque primo).
$A/Q \supseteq \overline{M} = \sqrt{0}$. Dunque $\overline{M}$ è l'intersezione di tutti gli ideali primi di A/Q, ma essendo massimale si ha che A/Q ha un solo ideale primo, $\overline{M}$.
Quindi in A/Q ogni elemento è invertibile o nilpotente. Ciò significa che i divisori di zero in A/Q sono nilpotenti. Allora per la proposizione precedente Q è primario. □

Osservazione. In generale $\sqrt{Q}$ primo $\not\Rightarrow Q$ primario. Infatti:
Esempio: $A = \mathbb{K}[x, y, z]/\left(xy - z^2\right)$, $P = (x, z)$.
$A/P \cong \mathbb{K}[y]$ è un dominio di integrità $\Rightarrow P$ è primo.
Sia $Q = P^2$ (ovvero $P = \sqrt{Q}$). Q non è primario. Infatti $xy = z^2 \in Q$, $x \notin Q$ ma $y^n \notin Q\ \forall n \in \mathbb{N}$.

6.4 L'anello $S^{-1}A$

Definizione: Un sottoinsieme S di A si dice moltiplicativamente chiuso se $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$.

Definizione: Sia A un dominio di integrità e S un sottoinsieme moltiplicativamente chiuso tale che $0 \notin S$ e $1 \in S$. Allora si definisce $S^{-1}A$ l'anello $\left\{\frac{a}{s} \mid a \in A, s \in S\right\}/_\sim$ con la relazione di equivalenza definita come $\frac{a}{s} \sim \frac{b}{t} \Leftrightarrow at = bs$ e le seguenti operazioni:

- $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$;
- $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$.

Osservazione. Occorre verificare che le operazioni siano ben definite. Lasciamo come esempio la dimostrazione della buona definizione dell'addizione:
$\frac{a}{s} \sim \frac{a'}{s'}$, $\frac{b}{t} \sim \frac{b'}{t'}$. Dunque $as' = a's$ e $bt' = b't$.

$$\frac{at+bs}{st} \overset{?}{\sim} \frac{a't'+b's'}{s't'}$$
$$(at+bs)s't' \overset{?}{=} (a't'+b's')st$$
$$\underbrace{as'}\,tt' + \underbrace{bt'}\,ss' \overset{?}{=} a'stt' + b'tss'$$
$$a'stt' + b'tss' = a'stt' + b'tss'$$

Proposizione: La funzione $\varphi : A \to S^{-1}A$ definita da $\varphi(x) = \frac{x}{1}$ è un omomorfismo iniettivo di anelli.

Dimostrazione. Verifichiamo le proprietà di omomorfismo:
$\varphi(x+y) = \frac{x+y}{1} = \frac{x}{1} + \frac{y}{1} = \varphi(x) + \varphi(y)$.
$\varphi(xy) = \frac{xy}{1} = \frac{x}{1} \cdot \frac{y}{1} = \varphi(x)\varphi(y)$.
Verifichiamo l'iniettività: $\varphi(x) = \frac{x}{1} = \frac{0}{1} \Leftrightarrow x \cdot 1 = 0 \cdot 1 = 0 \Leftrightarrow x = 0$. $\square$

Osservazione. Se $S = A \setminus \{0\}$ allora $S^{-1}A$ è un campo detto campo dei quozienti di A (o campo delle frazioni).

Osservazione. Se I è un ideale di A allora $S^{-1}I$ è un ideale di $S^{-1}A$. Inoltre $S^{-1}I \neq S^{-1}A \Leftrightarrow S \cap I = \emptyset$.

Osservazione. Se J è un ideale di $S^{-1}A$ allora esiste un ideale I di A tale che $J = S^{-1}I$. Basta infatti prendere

$$I = \{\text{numeratori degli elementi di } J\} = \left\{ x \in A \;\middle|\; \exists j \in J, \exists s \in S \;:\; j = \frac{x}{s} \right\}$$

PROPOSIZIONE: Siano A, B domini di integrità e sia $f : A \to B$ un omomorfismo di anelli. Sia inoltre $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso tale che $f(S) \subseteq B^*$. Allora esiste un'unica $\overline{f} : S^{-1}A \to B$ che estende f.

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, hook, "i"'] & & B \\ & S^{-1}A \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

Dimostrazione. Se tale $\overline{f}$ esiste allora è unica perché deve commutare il diagramma. Poiché $f = \overline{f} \circ i$, allora $\forall a \in A$, $\forall s \in S$ $f(a) = \overline{f}(\frac{a}{1}) = \overline{f}(\frac{sa}{s}) = \overline{f}(\frac{s}{1})\overline{f}(\frac{a}{s}) = f(s)\overline{f}(\frac{a}{s})$.
Dunque definiamo $\overline{f}(\frac{a}{s}) := f(s)^{-1}f(a)$.
Si verifica facilmente che si tratta di una buona definizione e che è un omomorfismo. $\square$

SCELTE USUALI DI S:

- $S = A \setminus \{0\}$; implica che $S^{-1}A$ è un campo (campo dei quozienti).
- $S = A \setminus P$ con P un ideale primo;
- $S = A \setminus \bigcup_{i \in I} P_i$ con P_i ideale primo $\forall i$.

PROPOSIZIONE: Sia A un dominio di integrità, P un ideale primo e $S = A \setminus P$. Allora $S^{-1}P$ è un ideale proprio di $S^{-1}A$ ed è l'unico ideale massimale di $S^{-1}A$.

Dimostrazione. $S^{-1}P$ è un ideale proprio perché $S \cap P = \emptyset$.
Ogni elemento $\frac{x}{s} \notin S^{-1}P$ è tale che $s \in S$, $x \notin P \Rightarrow x \in S$. Dunque $\frac{x}{s}$ è invertibile.
Allora $S^{-1}P$ è massimale perché ogni elemento nel suo complementare è invertibile, ed è unico perché $S^{-1}A$ è unione disgiunta di $S^{-1}P$ e dell'insieme degli elementi invertibili. $\square$

DEFINIZIONE: Un anello commutativo con unità si dice *anello locale* se possiede un unico ideale massimale.

TEOREMA (LEMMA DI ZORN): Sia X un insieme con una relazione d'ordine parziale, tale che ogni catena ascendente di X ammette un maggiorante. Allora X ammette un elemento massimale.

Osservazione. Equivalentemente, possiamo dire che il Lemma di Zorn afferma che $\forall x \in X \ \exists \ m$ massimale in X tale che $m \geq x$.

Corollario: In un anello commutativo con unità per ogni ideale proprio esiste un ideale massimale che lo contiene.

Dimostrazione. Utilizziamo il Lemma di Zorn con $X = \{\text{ideali propri di } A\}$. L'unione degli elementi di una catena $\{I_\lambda\}_{\lambda \in \Lambda}$ è ancora un ideale proprio perché $1 \notin I_\lambda \forall \lambda$ ed è un maggiorante. Dunque si giunge alla tesi tramite la seconda formulazione di Zorn. □

Osservazione. In un anello locale A, l'ideale massimale M è l'unione di tutti gli elementi non invertibili.

Esercizio: Sia A un dominio di integrità e sia S un insieme moltiplicativamente chiuso tale che $0 \notin S$ e $1 \in S$. Allora gli ideali primi di $S^{-1}A$ sono in bigezione con gli ideali primi di A contenuti in $A \setminus S$.

Proposizione: Sia A un dominio di integrità, P un ideale primo e $S = A \setminus P$. Sia $\overline{S}$ l'immagine di S in A/P attraverso la proiezione canonica. Allora

$$S^{-1}A/S^{-1}P \cong \overline{S}^{-1}(A/P)$$

Dimostrazione. Consideriamo l'applicazione:

$$\begin{array}{rccc} f: & S^{-1}A/S^{-1}P & \to & \overline{S}^{-1}(A/P) \\ & \left[\frac{a}{s}\right] & \mapsto & \frac{[a]}{[s]} \end{array}$$

È una buona definizione: siano $\left[\frac{b}{t}\right] = \left[\frac{a}{s}\right]$, cioè $\frac{a}{s} - \frac{b}{t} = \frac{c}{u}$ con $c \in P$. Allora $aut - bsu = cst$.
Voglio dimostrare che $\frac{[a]}{[s]} = \frac{[b]}{[t]}$, cioè $at - bs \in P$.
Dall'uguaglianza sopra si ha che $aut - bsu = (at - bs)u = cst \in P$ dato che $c \in P$. Allora, poiché $u \notin P$, $at - bs \in P$. Tesi.

La surgettività della funzione f è facilmente verificabile.

$\operatorname{Ker} f = \left\{ \left[\frac{a}{s}\right] \,\middle|\, f\left(\left[\frac{a}{s}\right]\right) = \frac{[0]}{[1]} \right\}$, dunque $\left[\frac{a}{s}\right] \in \operatorname{Ker} f \Leftrightarrow a \in P \Leftrightarrow \frac{a}{s} \in S^{-1}P \Leftrightarrow \left[\frac{a}{s}\right] = \left[\frac{0}{1}\right]$.
Quindi la funzione f è anche iniettiva, ed è l'isomorfismo cercato. □

6.5 Estensione e Contrazione di Ideali

Definizione: Siano $A \subseteq B$ due anelli commutativi.

- I ideale di A genera un ideale in B chiamato *estensione* di I che si denota con I^e;
- J ideale di B; $A \cap J$ è un ideale di A chiamato *contrazione* di J che si denota con J^c.

Proprietà con Operazioni tra Ideali

1. $(I_1 + I_2)^e = I_1^e + I_2^e$;

2. $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$;
   Controesempio altra inclusione: prendiamo $\mathbb{K}[x] \hookrightarrow \mathbb{K}[x,y]$ e gli ideali di $\mathbb{K}[x,y]$ $J_1 = (x+y) \Rightarrow J_1^c = (0)$, $J_2 = (y) \Rightarrow J_2^c = (0)$; allora $J_1^c + J_2^c = (0) \not\supseteq (J_1 + J_2)^c = (x,y)^c = (x)$.

3. $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$;
   Controesempio altra inclusione: prendiamo $\mathbb{Z}[x^2, x^3] \hookrightarrow \mathbb{Z}[x]$ e gli ideali di $\mathbb{Z}[x^2, x^3]$ $I_1 = (x^2) \Rightarrow I_1^e = (x^2)$, $I_2 = (x^3) \Rightarrow I_2^e = (x^3)$; allora $(I_1 \cap I_2)^e = (x^5, x^6)^e = (x^5) \not\supseteq I_1^e \cap I_2^e = (x^2) \cap (x^3) = (x^3)$.

4. $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$;

5. $(I_1 I_2)^e = I_1^e I_2^e$;

6. $(J_1 J_2)^c \supseteq J_1^c J_2^c$;
   Controesempio altra inclusione: prendiamo $\mathbb{Z}[xy] \hookrightarrow \mathbb{Z}[x,y]$ e gli ideali di $\mathbb{Z}[x,y]$ $J_1 = (x) \Rightarrow J_1^c = (xy)$, $J_2 = (y) \Rightarrow J_2^c = (xy)$; allora $(J_1 J_2)^c = (xy)^c = (xy) \not\subseteq J_1^c J_2^c = (xy)\,(xy) = (x^2 y^2)$.

7. $(I_1 : I_2)^e \subseteq I_1^e : I_2^e$;
   Controesempio altra inclusione: prendiamo $\mathbb{Z}[x^2, x^3] \hookrightarrow \mathbb{Z}[x]$ e gli ideali di $\mathbb{Z}[x^2, x^3]$ $I_1 = (x^3) \Rightarrow I_1^e = (x^3)$, $I_2 = (x^2) \Rightarrow I_2^e = (x^2)$; allora $(I_1 : I_2)^e = (x^3, x^4)^e = (x^3) \not\supseteq I_1^e : I_2^e = (x^3) : (x^2) = (x)$.

8. $(J_1 : J_2)^c \subseteq J_1^c : J_2^c$;
   Controesempio altra inclusione: prendiamo $\mathbb{Z}[xy] \hookrightarrow \mathbb{Z}[x,y]$ e gli ideali di $\mathbb{Z}[x,y]$ $J_1 = (x) \Rightarrow J_1^c = (xy)$, $J_2 = (y) \Rightarrow J_2^c = (xy)$; allora $(J_1 : J_2)^c = (x)^c = (xy) \not\supseteq J_1^c : J_2^c = (xy) : (xy) = (1)$.

9. $I \subseteq I^{ec}$;
   Controesempio altra inclusione: prendiamo $\mathbb{Z} \hookrightarrow \mathbb{Q}$ e l'ideale $I = (2)$; $I^{ec} = (2)^{ec} = \mathbb{Q}^c = (1) \not\subseteq (2) = I$.

10. $J \supseteq J^{ce}$;
    Controesempio altra inclusione: prendiamo $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ e l'ideale $J = (x)$; $J^{ce} = (x)^{ce} = (0)^e = (0) \not\supseteq (x) = J$.

11. $J^c = J^{cec}$;

12. $I^e = I^{ece}$;

Altre proprietà per Operazioni tra ideali:

13. $\sqrt{I} = \sqrt{\sqrt{I}}$;

14. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} \supseteq \sqrt{I}\sqrt{J}$;

15. $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I + J}$;

16. $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$;

17. $\sqrt{I} = \left(\bigcap_{P \supseteq I} P \right)$ con P ideale primo;

18. $\sqrt{(0)} = (\bigcap P)$ con P ideale primo;

19. $I \subseteq I : J$;

20. $(I : J)J \subseteq I$;

21. $(I : J) : K = I : JK = (I : K) : J$;

22. $(\bigcap_i I_i) : J = \bigcap_i (I_i : J)$;

23. $I : (\sum_i J_i) = \bigcap_i (I : J_i)$;

6.6 ED, PID e UFD

DEFINIZIONE: Un dominio di integrità A si dice *dominio euclideo* (spesso abbreviato in ED) se esiste una funzione "grado" $d : A \setminus \{0\} \to \mathbb{N}$ con le seguenti proprietà:

1. $d(x) \leq d(xy)\ \forall x, y \in A \setminus \{0\}$;

2. $\forall x, y \in A, y \neq 0, \exists\ q, r$ tali che $x = qy + r$ con $d(r) < d(y)$ oppure $r = 0$.

Osservazione. In un dominio euclideo esiste l'MCD tra 2 elementi non entrambi nulli che può essere determinato da un algoritmo di Euclide.

PROPOSIZIONE: In un ED A^* consiste in tutti e soli gli elementi di grado minimo.

Dimostrazione. $d(1) \leq d(1 \cdot x) = d(x)\ \forall x \in A \setminus \{0\}$. Dunque 1 ha grado minimo.
Se $a \in A^*$ allora esiste b tale che $ab = 1$, quindi $d(a) \leq d(ab) = d(1) \Rightarrow d(a) = d(1)$, cioè gli invertibili hanno grado minimo.
Viceversa, se x ha grado minimo: $1 = qx + r \Rightarrow r = 0$ poiché non può essere $d(r) < d(x)$.
Dunque $1 = qx \Rightarrow x \in A^*$. □

DEFINIZIONE: Un dominio di integrità si dice *dominio ad ideali principali* (abbreviato in PID) se tutti i suoi ideali sono principali.

PROPOSIZIONE: In un ED tutti gli ideali sono principali (cioè ED $\Rightarrow$ PID).

Dimostrazione. Sia I un ideale di A.
Se $I = (0)$ allora è principale.
Se $I \neq (0)$ allora esiste almeno un elemento in I diverso da 0. Scegliamo un elemento di grado minimo $x \in I$ e dimostriamo che $I = (x)$.
Banalmente $I \supseteq (x)$. Invece, se $y \in I$, allora $y = qx + r \Rightarrow I \ni y - qx = r \Rightarrow r \in I \Rightarrow r = 0$ dato che non può essere $d(r) < d(x)$. Quindi $y = qx$ e cioè $y \in (x)$. □

Osservazione. In un ED esiste un algoritmo di Euclide per determinare l'MCD tra 2 elementi non entrambi nulli. In un PID esiste l'MCD poiché esiste Bézout ma non c'è un algoritmo esplicito per calcolarlo.

PROPOSIZIONE: In un PID ogni catena ascendente di ideali (principali) è stazionaria. Ovvero

$$\forall\ I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots\ \exists n_0 \text{ tale che } I_n = I_{n_0} \forall n \geq n_0$$

Dimostrazione. Siano $I_i = (a_i)\,\forall i$ e sia $I = \bigcup_{n \in \mathbb{N}} I_n = (x)$. Allora $\exists n_0$ tale che $x \in I_{n_0}$, cioè $I_{n_0} \supseteq (x)$. Ma $I_{n_0} \subseteq \bigcup_{n \in \mathbb{N}} I_n = I$, e dunque $(x) \subseteq I_{n_0} \subseteq I_{n_0+1} \subseteq \ldots \subseteq I = (x)$. Quindi sono tutte uguaglianze. □

Proposizione: In un PID ogni elemento irriducibile è primo.

Dimostrazione. x è irriducibile $\Leftrightarrow$ (x) è massimale all'interno degli ideali principali $\Rightarrow$ (x) è massimale $\Rightarrow$ (x) è primo $\Rightarrow$ x è primo. $\square$

Corollario: In un PID gli ideali primi sono (0) (deriva dall'essere dominio di integrità) e gli ideali massimali.

Definizione: Un dominio di integrità A si dice *dominio a fattorizzazione unica* (abbreviato in UFD) se ogni elemento $\neq 0$ si può scrivere in modo unico (a meno di riordinamento e di elementi invertibili) nella forma $x = \lambda p_1 p_2 \cdot \ldots \cdot p_r$ con $\lambda \in A^*$ e p_i irriducibili.

Osservazione. In un UFD ogni ideale principale si scrive in modo unico (a meno dell'ordine) come prodotto di ideali principali primi.

Teorema: Se A è un dominio di integrità tale che:

1. Ogni catena ascendente di ideali principali è stazionaria;

2. Ogni elemento irriducibile è primo.

Allora A è un UFD.

Dimostrazione. Esistenza di una fattorizzazione.
Sia $x \neq 0$; se x è invertibile o è irriducibile non c'è niente da dimostrare.
Supponiamo quindi x non irriducibile. Allora $x = a_1 b_1$ con $a_1, b_1 \notin A^*$. Se sia a_1 che b_1 sono irriducibili abbiamo concluso. Altrimenti supponiamo a_1 non irriducibile. Supponiamo inoltre per assurdo che a_1 non sia prodotto di irriducibili. Allora $a_1 = a_2 b_2$ con $a_2, b_2 \notin A^*$. Dunque almeno uno tra a_2 e b_2 non è prodotto di irriducibili (supponiamo senza perdita di generalità a_2). $a_2 = a_3 b_3$ con $a_3, b_3 \notin A^*$.

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots \subseteq \ldots$$

Iterando il procedimento si ottiene una catena ascendente infinita non stazionaria di ideali principali. Assurdo per la proprietà 1. $\square$

Dimostrazione. Unicità della fattorizzazione.
Sia $x = \lambda p_1 p_2 \cdot \ldots \cdot p_r = \mu q_1 q_2 \cdot \ldots \cdot q_s$ con $\lambda, \mu \in A^*$ e p_i, q_i irriducibili.
Ma irriducibile $\Rightarrow$ primo per la seconda proprietà. Quindi $p_1 \mid \mu q_1 q_2 \cdot \ldots \cdot q_s \Rightarrow p_1 \mid q_1$ (senza perdita di generalità). Allora $q_1 = p_1 \cdot s$, ma q_1 è irriducibile, quindi $s \in A^*$.
Dunque $x = \lambda s p_2 \cdot \ldots \cdot p_r = \mu q_2 \cdot \ldots \cdot q_s$ e da qui si conclude per induzione. $\square$

Teorema: Se A è un UFD allora A possiede le 2 proprietà del teorema precedente.

Dimostrazione. 1.
Sia $x \in A \setminus \{0\}$, $x = \lambda p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$.
$d \mid x \Rightarrow d = \mu p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r}$ con $0 \leq \delta_i \leq a_i$. $\Rightarrow$ i divisori sono un numero finito (a meno di invertibili), e ogni catena ascendente di ideali principali

$$(x) \subseteq (d_1) \subseteq \ldots \subseteq \ldots$$

ha $d_i \mid x$ $\forall i$. Ma allora è stazionaria. $\square$

Dimostrazione. 2.
Sia x irriducibile. $x \mid ab \Rightarrow xy = ab = (\lambda p_1 \cdot \ldots \cdot p_r)(\mu q_1 \cdot \ldots \cdot q_s)$.
Per la fattorizzazione unica, x irriducibile $\Rightarrow x = p_k \vee x = q_k$ per un certo k.
Dunque $x \mid a \vee x \mid b$. $\square$

Osservazione. $x = \lambda p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$, $y = \mu p_1^{b_1} \cdot \ldots \cdot p_r^{b_r} \Rightarrow$ MCD$= p_1^{\min\{a_1,b_1\}} \cdot \ldots \cdot p_r^{\min\{a_r,b_r\}}$.

PROPOSIZIONE: Negli interi di Gauss, se $I = (a+ib)$ allora $|\mathbb{Z}[i]/I| = a^2 + b^2$.

Dimostrazione. Sia $J = (a - ib)$.
È facile osservare che $\mathbb{Z}[i]/I \cong \mathbb{Z}[i]/J$ tramite l'isomorfismo di coniugio.
Inoltre $[\mathbb{Z}[i] : IJ] = [\mathbb{Z}[i] : I][I : IJ]$.
Prendiamo adesso $f : \mathbb{Z}[i] \to I/IJ$ tale che $f(x) = (a+ib)x$. Si nota che $\operatorname{Ker} f = J$, e quindi $\mathbb{Z}[i]/J \cong I/IJ$.
Dunque possiamo riscrivere $[\mathbb{Z}[i] : IJ] = [\mathbb{Z}[i] : I][I : IJ] = [\mathbb{Z}[i] : I][\mathbb{Z}[i] : J] = [\mathbb{Z}[i] : I]^2$.
Ma, poiché $IJ = \left(a^2+b^2\right)$ e $\mathbb{Z}[i]/\left(a^2+b^2\right) \cong (\mathbb{Z}/(a^2+b^2)\mathbb{Z})[i]$, allora $[\mathbb{Z}[i] : IJ] = (a^2+b^2)^2$, da cui $[\mathbb{Z}[i] : I] = a^2 + b^2$. $\square$

Osservazione. ED $\subsetneq$ PID $\subsetneq$ UFD $\subsetneq$ Domini di Integrità. Infatti:

- Abbiamo già visto che $\mathbb{Z}[\sqrt{-5}]$ non è un UFD;
- $\mathbb{K}[x,y]$ è un UFD ma non è un PID.
  Infatti $\mathbb{K}$ campo $\Rightarrow \mathbb{K}[x,y]$ un UFD.
  Sia $I = (x,y)$. Vediamo che non è un ideale principale.
  Se lo fosse, allora $I = (f)$ e $f \mid x \wedge f \mid y \Rightarrow f = 1$. Ma $I = \{f_1 \cdot x + f_2 \cdot y\}$, quindi valutati in $(0,0)$ si annullano tutti. Poichè $f = 1$ non si annulla in $(0,0)$ allora $f \notin I$. Assurdo.
- $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ è un PID ma non è un ED.
  La dimostrazione che sia un PID viene tralasciata (difficile).
  Osserviamo preliminarmente che in un dominio euclideo, preso y di grado minimo tra tutti gli elementi non invertibili (escludendo lo 0) allora $A/(y)$ ha al massimo $|A^*| + 1$ elementi, dato che $\forall x \in A$ si può scrivere $x = qy + r$ con $r \in A^* \vee r = 0$.

$$A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{ a + b\frac{1+\sqrt{-19}}{2} \;\middle|\; a,b \in \mathbb{Z} \right\} = \\ = \left\{ \frac{r + s\sqrt{-19}}{2} \;\middle|\; r,s \in \mathbb{Z} \wedge r \equiv s \pmod 2 \right\}$$

  $A^* = \{\pm 1\}$: infatti $1 = \frac{r+s\sqrt{-19}}{2} \cdot 2\frac{r-s\sqrt{-19}}{r^2+19s^2}$, ma in A un denominatore può essere solamente 1 o 2. Dunque $s = 0$ e $r = \pm 2$ (deve essere pari) $\Rightarrow \frac{r+s\sqrt{-19}}{2} = \pm 1$.
  Supponiamo che A sia euclideo e sia $I = \left(\frac{r+s\sqrt{-19}}{2}\right)$ l'ideale generato da un elemento di grado minimo in $A \setminus \{\pm 1, 0\}$. Allora $|A/I| \leq |A^*| + 1 = 3$.
  Per la proposizione sopra se A fosse euclideo allora $|A/I| = \frac{r^2+19s^2}{4}$ e risolvendo la disuguaglianza si otterrebbe $s = 0$, $r^2 \leq 12$ con r pari $\Rightarrow r = \pm 2 \Rightarrow \frac{r+s\sqrt{-19}}{2} = \pm 1$.
  Assurdo dato che era stato scelto in $A \setminus \{\pm 1, 0\}$. Quindi A non è un ED.

DEFINIZIONE: Sia A un dominio di integrità e sia $\mathbb{K}$ il campo delle frazioni di A. A si dice *integralmente chiuso* in $\mathbb{K}$ se vale la seguente implicazione: $\alpha \in \mathbb{K}$ radice di $p(x) \in A[x]$

monico $\Rightarrow \alpha \in A$.

Proposizione: Sia A un UFD. Allora A è integralmente chiuso nel campo delle frazioni di A.

Dimostrazione. $\alpha = \frac{a}{b}$ è radice di $p(x) \in A[x]$ monico.
Dunque a divide il termine noto di $p(x)$ e b divide il coefficiente del monomio di grado massimo (che è 1) $\Rightarrow \alpha \in A$. □

Proposizione: $\mathbb{Z}[\sqrt{4n+1}]$ non è un UFD con $4n+1 \neq a^2$ e $a \in \mathbb{Z}$.

Dimostrazione. Sia $\alpha = \frac{1+\sqrt{4n+1}}{2}$.
α è radice di $x^2 - x - n$. Sia $\mathbb{K}$ il campo delle frazioni di $\mathbb{Z}[\sqrt{4n+1}]$.
$\{1, \sqrt{4n+1}\}$ è una base di $\mathbb{K}$ visto come spazio vettoriale su $\mathbb{Q}$, dunque $\alpha \in \mathbb{K}$ si scrive in modo unico come sopra.
Poiché invece $\mathbb{Z}[\sqrt{4n+1}] = \{a + b\sqrt{4n+1} \mid a, b \in \mathbb{Z}\}$, $\alpha \notin \mathbb{Z}[\sqrt{4n+1}] \Rightarrow \mathbb{Z}[\sqrt{4n+1}]$ non è integralmente chiuso $\Rightarrow \mathbb{Z}[\sqrt{4n+1}]$ non è un UFD. □

Proposizione: $\mathbb{Z}[\sqrt{-a}]$ non è un UFD $\forall a \in \mathbb{Z}, a \geq 3, a$ square-free.

Dimostrazione. Sia $\omega = \sqrt{-a}$.
$N(x + \omega y) = x^2 + ay^2$. N è moltiplicativa, $N(2) = 4$. Dimostriamo che 2 è irriducibile.
$N(x + \omega y) = x^2 + ay^2 \geq x^2 + 3y^2$. Se 2 non fosse irriducibile, si scriverebbe come prodotto di 2 elementi di norma al quadrato uguale a 2. Ma non esistono elementi con tale caratteristica, quindi 2 è irriducibile.
Vediamo però che 2 non è primo: sia $I = (2)$. $\omega \notin I$.
Se a è pari, allora $\omega^2 = -a \in I \Rightarrow I$ non è primo.
Se a è dispari, allora $(1+\omega)(1-\omega) = 1 + a \in I$, ma $(1 \pm \omega) \notin I \Rightarrow I$ non è primo.

Dunque se I non è primo allora 2 non è primo. Quindi $\mathbb{Z}[\sqrt{-a}]$ non è un UFD. □

6.7 Anelli di Polinomi

Lemma di Gauss:

Lemma 1: Sia $c(f)$:=contenuto di f =MCD dei suoi coefficienti. Se $c(f) = c(g) = 1$ allora $c(fg) = 1$.

Dimostrazione. Supponiamo per assurdo $c(fg) \neq 1$. Allora $\exists p$ primo tale che $p \mid c(fg)$.
$A[x]/(p) \cong A/(p)[x]$ e l'anello dei polinomi a coefficienti in un dominio di integrità è un dominio di integrità, quindi (p) è primo in $A[x]$. Prendiamo quindi $\pi : A[x] \to A[x]/(p)$ la proiezione canonica. Per ipotesi abbiamo $c(f) = 1$ e $c(g) = 1$, quindi $\pi(f) \neq 0$ e $\pi(g) \neq 0$. Ma $\pi(fg) = 0$. Assurdo perché il quoziente è un dominio di integrità. □

Lemma 2: $c(fg) = c(f)c(g)$.

Dimostrazione. Siano $f = c(f)f_1$ e $g = c(g)g_1$ con f_1 e g_1 primitivi.
$c(fg) = c(f)c(g)c(f_1g_1) = c(f)c(g)$ per il lemma precedente. □

Lemma 3: Siano $f, g \in A[x]$ con f primitivo. Se $f \mid g$ in $K[x]$, con K = campo dei quozienti di A, allora $f \mid g$ in $A[x]$.

Dimostrazione. Supponiamo $g = fh$ con $h(x) = \frac{a_n}{b_n}x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \ldots + \frac{a_0}{b_0}$.
$h(x) = \frac{a'_n x^n + a'_{n-1}x^{n-1} + \ldots + a'_0}{b} = \frac{a}{b}(c_n x^n + \ldots + c_0)$ con $c_n x^n + \ldots + c_0$ primitivo.
Dunque $g = f \cdot \frac{a}{b} \cdot h_1$, ovvero $bg = afh_1$. Passando ai contenuti $b \cdot c(g) = a$. Poiché $c(g) \in A$ allora $b \mid a \Rightarrow \frac{a}{b} \in A$.
Allora $g = fh$ con $h \in K[x] \Rightarrow g = fh$ con $h \in A[x]$. □

Lemma 4: $f \in A[x]$, $f = gh$ con $g, h \in K[x]$. Allora esistono $g', h' \in A[x]$ tali che $\deg(g) = \deg(g')$, $\deg(h) = \deg(h')$ e $f = g'h'$.

Dimostrazione. $h = \frac{a}{b}h'$ con $h' \in A[x]$.
Dunque $f = g \cdot \frac{a}{b} \cdot h' \ \Rightarrow h' \mid f$ in $K[x] \ \Rightarrow h' \mid f$ in $A[x]$.
Ma allora $g' = \frac{a}{b}g \in A[x]$. □

Teorema (Caratterizzazione Elementi Irriducibili in $A[x]$): $f \in A[x]$ è irriducibile se e solo se:

1. $\deg(f) = 0$, $f = a$ (costante) e a è un elemento irriducibile di A;

2. $\deg(f) > 0$, f è primitivo e f è irriducibile in $K[x]$ (con K il campo dei quozienti di A).

Dimostrazione. 1.
Se $\deg(f) = 0$ e $f = gh$ tutti costanti. Dunque $a = bc$. Poiché $A^* = (A[x])^*$ allora a irriducibile $\Leftrightarrow f$ irriducibile. □

Dimostrazione. 2.
Se $\deg(f) > 0$, e f irriducibile allora $c(f) = 1$ perché $f = c(f)f_1$ a meno di invertibili.
Inoltre, se fosse riducibile in $K[x]$ allora lo sarebbe anche (non banalmente) in $A[x]$.

Viceversa, sia $f = gh$. f irriducibile in $K[x] \Rightarrow$ i gradi di g e h non sono entrambi minori stretti, cioè g è costante.
Ma $c(f) = 1 \Rightarrow c(g) = 1 \Rightarrow g = 1 \Rightarrow f$ irriducibile in $A[x]$. □

Teorema: Se A è un UFD allora $A[x]$ è un UFD.

Dimostrazione. Per la caratterizzazione degli UFD occorre dimostrare le 2 proprietà:

1. Ogni catena ascendente di ideali principali è stazionaria;

2. Ogni elemento irriducibile è primo.

Dimostriamo la prima proprietà.

$$(f_1) \subseteq (f_2) \subseteq \ldots \subseteq \ldots$$

$\forall i \ f_i = c(f_i)f'_i$ con f'_i primitivo.
Dunque ho due catene ascendenti:

$$(c(f_1)) \subseteq (c(f_2)) \subseteq \ldots \subseteq \ldots$$

che è una catena di ideali di A (che è un UFD) e quindi è stazionaria;

$$(f'_1) \subseteq (f'_2) \subseteq \ldots \subseteq \ldots$$

che è una catena di polinomi primitivi tali che $0 \leq \deg(f_i') < \deg(f_{i-1}')$ e dunque è stazionaria.
Allora anche la catena $(f_1) \subseteq (f_2) \subseteq \ldots \subseteq \ldots$ è stazionaria.

Dimostriamo adesso la seconda proprietà.
f irriducibile. Dunque per la caratterizzazione precedente ci sono 2 possibilità:

- $\deg(f) = 0$ e $f = a$ costante con a irriducibile in $A \Rightarrow a$ primo in A. Quindi $a = c(f) \mid c(g)c(h) \Rightarrow a \mid c(g) \vee a \mid c(h)$, ovvero $f \mid g \vee f \mid h$;
- $\deg(f) > 0$, f è primitivo e irriducibile in $K[x]$. $f \mid gh$ in $A[x]$. Dunque $f \mid gh$ in $K[x]$, ma essendo f irriducibile in $K[x]$ ed essendo $K[x]$ un UFD (poiché è un anello di polinomi a coefficienti in un campo) allora f è primo in $K[x]$ e dunque $f \mid g \vee f \mid h$ in $K[x]$. Per il Lemma di Gauss allora $f \mid g \vee f \mid h$ in $A[x]$.

$\square$

PROPOSIZIONE: Se $I \subseteq \mathbb{Z}[x]$ è un ideale principale, allora I non è massimale.

Dimostrazione. Sia $I = (f)$.
Se $f = 0$ allora $I = (0)$ non è massimale.
Se $\deg f = 0$ allora $I = (n) \Rightarrow \mathbb{Z}[x]/(n) \cong \mathbb{Z}/n\mathbb{Z}[x]$ che non è un campo, dunque I non è massimale.
Se $\deg f > 0$ allora $\mathbb{Z} \cap I = \{0\}$, quindi $\mathbb{Z} \subseteq \mathbb{Z}[x]/I$.
Se $\mathbb{Z}[x]/I$ fosse un campo allora anche $\mathbb{Q} \subseteq \mathbb{Z}[x]/I$ (poiché ogni elemento di $\mathbb{Z}$ avrebbe un inverso).
Ma allora $\frac{1}{2} \in \mathbb{Z}[x]/I$, cioè $\mathbb{Z}[x] \not\ni \frac{1}{2} = g(x) + f(x)h(x) \in \mathbb{Z}[x]$, che è assurdo. Allora $\mathbb{Z}[x]/I$ non è un campo, ovvero I non è massimale. $\square$

PROPOSIZIONE: Sia A un UFD e sia $\mathbb{K}$ =Frac(A) il campo delle frazioni di A. Sia $p(x) \in A[x]$. Allora le radici in $\mathbb{K}$ di $p(x) = a_n x^n + \ldots + a_0$ sono del tipo $\frac{a}{b}$ (ridotta ai minimi termini) con $a \mid a_0$ e $b \mid a_n$.

Dimostrazione. Sia $\frac{a}{b} = z \in \mathbb{K}$ una radice di $p(x)$ tale che MCD(a, b)=1.
$0 = p(z) = \left(\frac{a}{b}\right)^n a_n + \ldots + a_0 \Rightarrow b^n p(z) = a^n a_n + b a^{n-1} a_{n-1} + \ldots + b^n a_0 = 0 \Rightarrow b(a^{n-1}a_{n-1} + \ldots + b^{n-1}a_0) = -a^n a_n$.
Ma $b \nmid a \Rightarrow b \mid a_n$. Analogamente portando al membro destro il termine $b^n a_0$ si ha che $a \nmid b \Rightarrow a \mid a_0$. $\square$

PROPOSIZIONE: $z \in \mathbb{Z}[i]$ ha norma al quadrato pari $\Leftrightarrow z$ è divisibile per $(1+i)$.

Dimostrazione. $\Leftarrow$.
Ovvia, dato che la norma è una funzione moltiplicativa. $\square$

Dimostrazione. $\Rightarrow$.
Sia $z = m + in$, $m^2 + n^2 \equiv 0 \pmod 2 \Rightarrow m + in = (1+i)(u+iv) = (u-v) + i(u+v) \Rightarrow u = \frac{m+n}{2} \wedge v = \frac{n-m}{2}$. $\square$

PROPOSIZIONE: $z \in \mathbb{Z}[i]$ è un elemento primo $\Leftrightarrow |z|^2 = p$ con p un primo di $\mathbb{Z}$ tale che $p \equiv 1 \pmod 4$ o $p = 2$, oppure a meno di invertibili $z = p$ con p un primo di $\mathbb{Z}$ tale che $p \equiv 3 \pmod 4$.

Dimostrazione. $\Leftarrow$.
LEMMA: Sono fatti equivalenti:

1. $p \equiv 1 \pmod 4$ o $p = 2$;

2. $x^2 + 1 = 0$ è risolubile in $\mathbb{F}_p$;

3. $\exists a, b \in \mathbb{Z}$ tali che $a^2 + b^2 = p$.

Dimostrazione. $3 \Rightarrow 1$.
$2 = 1^2 + 1^2$ e $\forall x \in \mathbb{Z}$ $x^2 \equiv 0, 1 \pmod 4$. Dunque poiché ogni primo diverso da 2 è congruo a 1 o 3 modulo 4, si ha che $p = a^2 + b^2 \equiv 1 \pmod 4$. □

Dimostrazione. $1 \Rightarrow 2$.
$x^2 + 1 \equiv 0 \pmod 2$ è risolubile. Vediamo che $x^2 - 1 \equiv 0 \pmod p$ è risolubile:
Prendiamo $x^{p-1} - 1 \equiv 0 \pmod p$; il polinomio ha $p - 1$ radici distinte. $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$ e dunque anche $x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$ è risolubile e ha $\frac{p-1}{2}$ radici distinte.
Poiché $p \equiv 1 \pmod 4$, esiste $x \in \mathbb{F}_p$ tale che $\left(x^{\frac{p-1}{4}}\right)^2 \equiv -1 \pmod p$. □

Dimostrazione. $2 \Rightarrow 3$.
Se $a^2 \equiv -1 \pmod p$ allora $p \mid a^2 + 1 = (a + i)(a - i)$. Se p fosse primo in $\mathbb{Z}[i]$ allora dovrebbe dividere uno dei due, ma $p \mid m + in \Rightarrow p \mid m \wedge p \mid n$. Dato che ciò non è possibile, p non è primo in $\mathbb{Z}[i]$.
Dunque $p = (a + ib)(c + id) \Rightarrow$ passando alle norme $p^2 = p \cdot p = (a^2 + b^2)(c^2 + d^2)$, cioè $p = a^2 + b^2 = c^2 + d^2$. □

Se $|z|^2 = p$ allora z è primo grazie al fatto che l'anello $\mathbb{Z}$ sia un UFD. Vediamo che non esistono $z \in \mathbb{Z}[i]$ tali che $|z|^2 = p \equiv 3 \pmod 4$ (p primo di $\mathbb{Z}$). Infatti se $z = a + ib$, allora $|z|^2 = a^2 + b^2 = p$ e la tesi segue dal lemma.

Sia addesso $z = p \equiv 3 \pmod 4$ (con p primo di $\mathbb{Z}$). Se z non fosse primo in $\mathbb{Z}[i]$ allora esisterebbero $x, y \in \mathbb{Z}[i]$ non invertibili tali che $z = xy$. Ma quindi passando alle norme al quadrato si avrebbe che $p^2 = p \cdot p = |x|^2 \cdot |y|^2 \Rightarrow |x|^2 = p \equiv 3 \pmod 4$ che risulta impossibile. □

Dimostrazione. $\Rightarrow$.
Sia $z = a + ib$. Se $a = 0 \vee b = 0$ allora a meno di invertibili $z \in \mathbb{Z}$. Dunque z primo $\Rightarrow z = p$ con p primo congruo a 3 modulo 4.
Se $a \neq 0 \wedge b \neq 0$ allora sia p un primo di $\mathbb{Z}$ che divide $|z|^2$.
$p \not\equiv 3 \pmod 4$ perché essendo primo in $\mathbb{Z}[i]$ si avrebbe $p \mid a^2 + b^2 = (a + ib)(a - ib) \Rightarrow p \mid a \pm ib \Rightarrow p \mid a \wedge p \mid b \Rightarrow z = p(a' + ib')$ non sarebbe primo. Assurdo.
Dunque $p \equiv 1 \pmod 4$ o $p = 2$, $p = (c + id)(c - id) \mid a^2 + b^2 = (a + ib)(a - ib)$ con $(c \pm id)$ primi in $\mathbb{Z}[i]$. Ma allora, essendo z primo, si deve avere (a meno di invertibili) $z = c \pm id$, e quindi $|z|^2 = p$. □

Capitolo 7

Teoria dei Campi

In questa sezione tratteremo solamente campi con caratteristica nulla o campi finiti. Ciò perché sotto tali ipotesi vale che un polinomio irriducibile ha radici distinte.

Definizione: Siano $\mathbb{K} \subseteq \mathbb{F}$ campi. Un elemento $\alpha \in \mathbb{F}$ si dice *algebrico* su $\mathbb{K}$ se $\exists f \in \mathbb{K}[x] \setminus \{0\}$ tale che $f(\alpha) = 0$.

Definizione: Siano $\mathbb{K} \subseteq \mathbb{F}$ campi. Un elemento $\alpha \in \mathbb{F}$ si dice *trascendente* su $\mathbb{K}$ se $\nexists f \in \mathbb{K}[x] \setminus \{0\}$ tale che $f(\alpha) = 0$.

Osservazione. Equivalentemente, possiamo definire $\alpha \in \mathbb{F}$ trascendente (algebrico) se l'omomorfismo di sostituzione $\varphi_\alpha : \mathbb{K}[x] \to \mathbb{F}$ ha nucleo (non) banale.

Osservazione. Se $\alpha \in \mathbb{F}$ è algebrico, allora $\operatorname{Im} \varphi_\alpha$ è un sottocampo di $\mathbb{F}$.

Definizione: Un'estensione di campi $\mathbb{F} \supseteq \mathbb{K}$ si dice *finita* se $[\mathbb{F} : \mathbb{K}] = \dim_{\mathbb{K}} \mathbb{F} < \infty$.

Definizione: Un'estensione $\mathbb{F} \supseteq \mathbb{K}$ si dice *algebrica* se $\forall \alpha \in \mathbb{F}$ α è algebrico su $\mathbb{K}$.

Teorema (Estensione Finita $\Rightarrow$ Estensione Algebrica): Siano $\mathbb{K} \subseteq \mathbb{F}$ campi. $[\mathbb{F} : \mathbb{K}] < \infty \Rightarrow \forall \alpha \in \mathbb{F}$ α è algebrico su $\mathbb{K}$.

Dimostrazione. Sia $[\mathbb{F} : \mathbb{K}] = n$.
Essendo $\mathbb{F}$ in modo naturale uno spazio vettoriale di dimensione n su $\mathbb{K}$, allora $\forall \alpha \in \mathbb{F}$ gli elementi $1, \alpha, \alpha^2, \ldots, \alpha^n$ sono linearmente dipendenti. Ovvero esiste una combinazione lineare non nulla su $\mathbb{K}$. Abbiamo dunque trovato un polinomio in $\mathbb{K}[x]$ non nullo che si annulla su α. $\square$

Definizione: Un campo $\mathbb{K}$ si dice *algebricamente chiuso* se per ogni $f \in \mathbb{K}[x]$ non costante esiste $\alpha \in \mathbb{K}$ tale che $f(\alpha) = 0$.

Teorema (Teorema Fondamentale dell'Algebra): $\mathbb{C}$ è algebricamente chiuso.

Dimostrazione. Sia $f(x) \in \mathbb{C}[x]$, $\deg f \geq 1$ e sia inoltre $\varphi : \mathbb{C} \to \mathbb{R}^+$ tale che $\varphi(z) = |f(z)|$. Poiché

$$\begin{array}{ccccc} \mathbb{C} & \to & \mathbb{C} & \to & \mathbb{R}^+ \\ z & \mapsto & f(z) & \mapsto & |f(z)| \end{array}$$

φ è continua perchè composizione di funzioni continue (la funzione polinomiale e il modulo). Inoltre $\lim_{|z|\to+\infty} |f(z)| = +\infty$. Dunque esiste un compatto in cui la funzione ha minimo. Supponiamo per assurdo tale minimo sia diverso da zero. Possiamo allora normalizzare la funzione per poter considerare $\min_{|f(z)|} = 1$ e traslarla per avere senza perdita di generalità $f(0) = 1$.
Dunque $f(z) = 1 + a_k z^k + \ldots$ e per Taylor, in un intorno di zero vale $f(z) \sim 1 + a_k z^k$. Essendo su $\mathbb{C}$, sappiamo risolvere $a_k z^k = -1$: sia z_0 una radice, allora per $t \in \mathbb{R}^+$ si ha che $a_k(tz_0)^k = -t^k$.
Quindi $|f(z)| \sim 1 - t^k < 1$. Assurdo. $\square$

TEOREMA: Sia p un primo. $\mathbb{F} = \bigcup_{n\in\mathbb{N}\setminus\{0\}} \mathbb{F}_{p^n}$ è algebricamente chiuso.

Dimostrazione. $\mathbb{F}$ è un campo perché le operazioni sono sempre effettuate tra un numero finito di elementi di $\mathbb{F}_{p^{k_i}}$ per certi $k_i \Rightarrow$ tutti gli elementi stanno in $\mathbb{F}_{p^{\mathrm{mcm}\{k_i\}}}$.
Sia adesso $f(x) \in \mathbb{F}[x]$, $\deg f = d \geq 1$; esiste $n \in \mathbb{N}$ tale che $f(x) \in \mathbb{F}_{p^n}[x]$. Poiché f si scompone in un numero finito di fattori irriducibili di grado $\delta_i \leq d$, allora $f(x)$ si spezza in fattori lineari in $\mathbb{F}_{p^{\mathrm{mcm}\{\delta_i\}}} \subseteq \mathbb{F}$. $\square$

Osservazione. Se $\mathrm{char}(\mathbb{K}) = 0$ oppure $\mathbb{K}$ è finito allora i polinomi irriducibili in $\mathbb{K}[x]$ hanno radici distinte (in una chiusura algebrica).

Dimostrazione. $\mathrm{char}(\mathbb{K}) = 0$.
Sia $f(x) \in \mathbb{K}[x]$ irriducibile. Se avesse radici multiple allora $\mathrm{MCD}(f(x), f'(x)) \neq 1$, e dunque $f(x)$ non sarebbe irriducibile. $\square$

Dimostrazione. $\mathbb{K} = \mathbb{F}_{p^n}$.
Sia $f(x) \in \mathbb{F}_{p^n}[x]$ irriducibile. Se avesse radici multiple e $f' \neq 0$ allora si conclude come sopra. Se invece $f' = 0 \Rightarrow f(x) = a_{ps}x^{ps} + \ldots + a_p x^p + a_0$.
Notiamo adesso che poiché $\mathbb{F}_{p^n}$ ha caratteristica p l'applicazione $\begin{array}{ccc} \mathbb{F}_{p^n} & \to & \mathbb{F}_{p^n} \\ x & \mapsto & x^p \end{array}$ è un automorfismo (detto automorfismo di Frobenius), dunque $a_i = b_i^p$ per certi $b_i \in \mathbb{F}_{p^n}$. Allora $f(x) = b_{ps}^p x^{ps} + \ldots + b_p^p x^p + b_0^p = (b_{ps}x^s + \ldots + b_p x + b_0)^p$ e dunque $f(x)$ non era irriducibile. $\square$

Osservazione. Detto $\mu_\alpha(x)$ il polinomio minimo di α in $\mathbb{K}[x]$, si ha che $\mathbb{K}(\alpha) \cong \mathbb{K}[x]/(\mu_\alpha)$ è un campo (la più piccola estensione di $\mathbb{K}$ che contiene α).

PROPOSIZIONE: Sia Ω un campo algebricamente chiuso ($\mathbb{C}$ o $\mathbb{F} = \bigcup_n F_{p^n}$), sia $\mathbb{K} \subseteq \Omega$ e sia $\alpha \in \Omega$ algebrico su $\mathbb{K}$. Se $\deg \mu_\alpha(x) = n$ allora esistono n omomorfismi (iniettivi) distinti $\varphi_1, \ldots, \varphi_n$ con $\varphi_i : \mathbb{K}(\alpha) \to \Omega$ tali che $\varphi_i|_{\mathbb{K}} =$inclusione.

Dimostrazione. Consideriamo il seguente diagramma:

$$\begin{tikzcd} \mathbb{K}[x] \arrow[rr, "\psi_i"] \arrow[dr, "\pi"'] & & \Omega \\ & \mathbb{K}[x]/(\mu_\alpha) \cong \mathbb{K}(\alpha) \arrow[ur, hook, dashed, "\varphi_i"'] & \end{tikzcd}$$

Esistono tante applicazioni φ_i quante sono le possibili $\psi_i : \mathbb{K}[x] \to \Omega$ tali che $\mathrm{Ker}\,\psi_i = (\mu_\alpha(x))$. Dunque $\psi_i : \left\{ \begin{array}{ccc} 1 & \mapsto & 1 \\ x & \mapsto & \beta_i \end{array} \right.$ con β_i tutte e sole le radici di $\mu_\alpha(x)$, che sono esattamente n. $\square$

Proposizione: Siano $\mathbb{K} \subseteq \mathbb{E} \subseteq \Omega$ campi (Ω algebricamente chiuso) e sia $[\mathbb{E} : \mathbb{K}] = d$. Allora esistono esattamente d omomorfismi (iniettivi) distinti $\varphi_1, \dots, \varphi_d$ con $\varphi_i : \mathbb{E} \to \Omega$ tali che $\varphi_i|_{\mathbb{K}}$ =inclusione.

Dimostrazione. Poiché $\mathbb{E}$ è un'estensione finita, allora è anche algebrica e dunque $\mathbb{E} = \mathbb{K}(\alpha_1, \dots, \alpha_m)$.
Sia $\mathbb{K} = \mathbb{K}_0$ e poniamo $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_{i+1})$, $d_i = [\mathbb{K}_i : \mathbb{K}_{i-1}]$.
Dunque $d = d_1 \cdot d_2 \cdot \ldots \cdot d_m$.
Per la proposizione precedente, data $\varphi : \mathbb{K}_0 = \mathbb{K} \to \Omega$, possiamo estenderla a $\overline{\varphi} : \mathbb{K}_1 = \mathbb{K}(\alpha_1)$ in d_1 modi diversi.

Lemma: Ogni omomorfismo $\psi : \mathbb{K}_i \to \Omega$ tale che $\psi|_{\mathbb{K}_0}$ =inclusione si può estendere a $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_{i+1})$ in esattamente d_{i+1} modi.

Dimostrazione. Poiché l'omomorfismo è iniettivo, si ha che $\psi(\mathbb{K}_i) = \mathbb{K}'_i \cong \mathbb{K}_i$.
Allora $\mathbb{K}_i[x] \cong \mathbb{K}'_i[x]$, e considerando tale isomorfismo $\mu_{\alpha_{i+1}}(x) \mapsto \mu'_{\alpha_{i+1}}(x)$ con $\mu'_{\alpha_{i+1}}(x)$ irriducibile, dello stesso grado, monico e con le stesse radici. Su questo polinomio ψ può lavorare in d_{i+1} modi differenti (tanti quante le radici di $\mu'_{\alpha_{i+1}}$), e quindi ψ si estende naturalmente in d_{i+1} diversi modi. □

Utilizzando il lemma si conclude la dimostrazione per induzione. □

7.1 Teoria di Galois

Definizione: Sia $\mathbb{E}/\mathbb{K}$ un'estensione finita. $\mathbb{E}/\mathbb{K}$ si dice *estensione normale* se per ogni omomorfismo $\varphi : \mathbb{E} \to \Omega$ con $\varphi|_{\mathbb{K}} = id$ si ha $\varphi(\mathbb{E}) = \mathbb{E}$.

Definizione: Sia $\mathbb{E}/\mathbb{K}$ è un'estensione finita e normale. Allora l'insieme $G = \mathrm{Gal}(\mathbb{E}/\mathbb{K}) = \{\sigma : \mathbb{E} \to \mathbb{E} \mid \sigma \text{ omomorfismo}, \ \sigma|_{\mathbb{K}} = id\}$ è un gruppo e si dice *gruppo di Galois* dell'estensione.

Proposizione: Sia $f(x) \in \mathbb{K}[x]$ e sia $\mathbb{E} \subseteq \Omega$ il campo di spezzamento di $f(x)$. Allora $\mathbb{E}/\mathbb{K}$ è un'estensione normale.

Dimostrazione. Siano $\alpha_1, \dots, \alpha_n$ le radici di $f(x) \Rightarrow \mathbb{E} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$.
per mostrare che $\varphi(\mathbb{E}) \subseteq \mathbb{E}$ basta vedere che $\varphi(\alpha_i) \in \mathbb{E}\ \forall i$, poiché generano $\mathbb{E}$.
α_i radice di $f_i(x)$ fattore irriducibile di $f(x)$; dunque $\alpha_i \mapsto \beta_i$ radice dello stesso fattore irriducibile $\Rightarrow \beta_i \in \mathbb{E}$. □

Proposizione: Sia $\mathbb{E}/\mathbb{K}$ il campo di spezzamento di un polinomio $f(x) \in \mathbb{K}[x]$ di grado n. Allora $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ è isomorfo ad un sottogruppo di S_n.

Dimostrazione. Costruiamo un omomorfismo $\psi : G = \mathrm{Gal}(\mathbb{E}/\mathbb{K}) \to S_n$.
Sia $\mathbb{E} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ con α_i le radici di $f(x)$.
Allora $\mathbb{E} = \mathbb{K}(\beta_1, \dots, \beta_m)$ con β_i radici distinte di $f(x)$ $(m \leq n)$.
$\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \ni \varphi \overset{\psi}{\to} \varphi|_{\{\beta_1, \dots, \beta_m\}} \in S_m \subseteq S_n$ (la funzione restrizione) è iniettiva: infatti sia $\varphi \in \operatorname{Ker} \psi$. Allora $\varphi(\beta_i) = \beta_i\ \forall i$. Ma poiché $\varphi|_{\mathbb{K}} = id$ e $\{\beta_1, \dots, \beta_m\}$ è un insieme di generatori $\Rightarrow \varphi = id_{\mathbb{E}}$. □

Osservazione. $[\mathbb{E}:\mathbb{K}]=2 \Rightarrow \mathbb{E}/\mathbb{K}$ è normale.

Teorema (Teorema dell'Elemento Primitivo): Ogni estensione finita di un campo $\mathbb{K}$ è semplice, ovvero se $\mathbb{E}\supseteq\mathbb{K}$ è un'estensione finita allora $\exists\alpha\in\mathbb{E}$ tale che $\mathbb{E}=\mathbb{K}(\alpha)$.

Dimostrazione. Suddividiamo la dimostrazione in 2 casi:

- $\mathbb{K}$ finito.
  $\mathbb{K}=\mathbb{F}_{p^a}$, $\mathbb{E}=\mathbb{F}_{p^b}$ per certi a,b tali che $a\mid b$. Ma $\mathbb{E}^*$ è ciclico, generato da un elemento α. Allora $\mathbb{E}=\mathbb{K}(\alpha)$.

- $\mathbb{K}$ infinito e char$\mathbb{K}=0$.
  Supponiamo $[\mathbb{E}:\mathbb{K}]=n$. Allora sappiamo che $\mathbb{E}=\mathbb{K}(\alpha_1,\alpha_2,\dots,\alpha_m)$ con $m\leq n$.

  Lemma: Siano $\mathbb{E}'\supseteq\mathbb{K}$ campi tali che $\mathbb{E}'=\mathbb{K}(\alpha,\beta)$. Allora $\exists\gamma\in\mathbb{E}'$ tale che $\mathbb{E}'=\mathbb{K}(\gamma)$.

  Dimostrazione. Sia $[\mathbb{E}':\mathbb{K}]=d$.
  Allora esistono esattamente d omomorfismi distinti $\sigma_1,\dots,\sigma_d$ tali che $\sigma_i:\mathbb{E}'\to\Omega$ che fissano $\mathbb{K}$.
  Le coppie $(\sigma_1(\alpha),\sigma_1(\beta)),\dots,(\sigma_d(\alpha),\sigma_d(\beta))$ sono distinte; infatti α e β (insieme a 1) generano $\mathbb{E}'$ e se σ_i,σ_j coincidessero su questi allora si avrebbe $\sigma_i=\sigma_j$.
  Prendiamo adesso

  $$f(x)=\prod_{i\neq j}\left[(\sigma_i(\alpha)+x\sigma_i(\beta))-(\sigma_j(\alpha)+x\sigma_j(\beta))\right]\neq 0$$

  Essendo non nullo ed essendo $\mathbb{K}$ infinito, $\exists c\in\mathbb{K}$ tale che $f(c)\neq 0$.
  Dato che σ_i è un omomorfismo che fissa $\mathbb{K}$ per ogni i, dunque

  $$\sigma_i(\alpha)+c\sigma_i(\beta)=\sigma_i(\alpha)+\sigma_i(c)\sigma_i(\beta)=\sigma_i(\alpha+c\beta)$$

  Ne segue che per $i\neq j$ allora $\sigma_i(\alpha+c\beta)\neq\sigma_j(\alpha+c\beta)$.
  Quindi, se $\gamma=\alpha+c\beta$, $[\mathbb{K}(\gamma):\mathbb{K}]\geq d$ poiché $\sigma_1(\gamma),\dots,\sigma_d(\gamma)$ sono tutti distinti.
  Inoltre $\mathbb{K}(\gamma)\subseteq\mathbb{K}(\alpha,\beta)\Rightarrow[\mathbb{K}(\gamma):\mathbb{K}]\leq d\Rightarrow\mathbb{K}(\gamma)=\mathbb{K}(\alpha,\beta)$. □

  Grazie al lemma si chiude per induzione la dimostrazione.

□

Corollario: Sia $\mathbb{E}\supseteq\mathbb{K}$ un'estensione algebrica tale che $\exists n\in\mathbb{N}$ per cui $\forall\alpha\in\mathbb{E}$ $[\mathbb{K}(\alpha):\mathbb{K}]\leq n$. Allora $\mathbb{E}/\mathbb{K}$ è finita di grado minore o uguale a n.

Dimostrazione. Sia $\gamma\in\mathbb{E}$ tale che $[\mathbb{K}(\gamma):\mathbb{K}]=m\leq n$ sia massimale.
Supponiamo per assurdo che $\mathbb{K}(\gamma)\neq\mathbb{E}$: allora esiste $\beta\notin\mathbb{K}(\gamma),\beta\in\mathbb{E}$ tale che $\mathbb{K}(\gamma)\subsetneq\mathbb{K}(\beta,\gamma)=\mathbb{K}(\delta)=\mathbb{E}$. Ma allora $\delta\in\mathbb{E}$ è tale che $[\mathbb{K}(\delta):\mathbb{K}]>m$. Assurdo. □

Teorema (Teorema di Artin): Siano $\mathbb{E}$ un campo e G un gruppo di automorfismi di $\mathbb{E}$ di ordine n. Allora $\mathbb{K}=\mathbb{E}^G=\{x\in\mathbb{E}\mid\sigma(x)=x\ \forall\sigma\in G\}$ è un campo, $\mathbb{E}/\mathbb{K}$ è un'estensione di Galois di grado n e $G=\mathrm{Gal}(\mathbb{E}/\mathbb{K})$.

Dimostrazione. Le verifiche che $\mathbb{K}$ sia un campo sono lasciate.

$\mathbb{E}/\mathbb{K}$ è finita e algebrica: sia $\alpha \in \mathbb{E}$. Da $\{\sigma_{id}(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$ estraiamo un sottoinsieme di immagini distinte di α, $\{\alpha, \sigma_2(\alpha), \dots, \sigma_m(\alpha)\}$ con $m \leq n$.
Sia $f(x) = (x - \alpha)\,(x - \sigma_2(\alpha)) \cdot \ldots \cdot (x - \sigma_m(\alpha))$. Questo polinomio si annulla in α e se $\sigma \in G$ allora $\sigma \circ f(x) = f(x)$.
Dunque $f(x) \in \mathbb{K}[x]$, $[\mathbb{K}(\alpha) : \mathbb{K}] = m \leq n$ e dunque per il corollario precedente $[\mathbb{E} : \mathbb{K}] \leq n$.

$\mathbb{E}/\mathbb{K}$ è normale: per ogni $\alpha \in \mathbb{E}$, data $\tau : \mathbb{E} \to \Omega$ tale che $\tau|_{\mathbb{K}} = id$, si ha che $\tau(\alpha) = \tau|_{\mathbb{K}(\alpha)}(\alpha)$. Inoltre, come visto sopra, esiste $f(x) \in \mathbb{K}[x]$ che ha α come radice. Dunque il polinomio minimo di α su $\mathbb{K}$ divide $f(x)$ e quindi $\tau(\alpha) = \tau|_{\mathbb{K}(\alpha)}(\alpha) = \beta$ con β un'altra radice del polinomio minimo di α su $\mathbb{K}$, e dunque di $f(x)$. Allora $\beta = \sigma_i(\alpha)$ con $\sigma_i \in G \Rightarrow \tau(\alpha) = \beta \in \mathbb{E}$.

Abbiamo già provato che $[\mathbb{E} : \mathbb{K}] \leq n$. Poiché sappiamo per ipotesi che esistono almeno n omomorfismi distinti $\sigma_i : \mathbb{E} \to \Omega$ tali che $\sigma_i|_{\mathbb{K}} = id$ (quelli di G), allora $[\mathbb{E} : \mathbb{K}] = n = |\mathrm{Gal}(\mathbb{E}/\mathbb{K})|$ ed essendo $G < \mathrm{Gal}(\mathbb{E}/\mathbb{K}) \Rightarrow G = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$. □

Teorema (Corrispondenza di Galois): Sia $\mathbb{F}/\mathbb{K}$ un'estensione finita di Galois con $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Allora esiste una corrispondenza biunivoca tra:

- estensioni intermedie $\mathbb{E}$ (cioè campi $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{F}$);
- sottogruppi H di G.

dato da $\alpha : \mathbb{E} \to \mathrm{Gal}(\mathbb{F}/\mathbb{E})$.

Dimostrazione. Dimostriamo che $\mathbb{F}/\mathbb{E}$ è un'estensione normale:
sia $\tau : \mathbb{F} \to \Omega$ tale che $\tau|_{\mathbb{E}} = id \Rightarrow \tau|_{\mathbb{K}} = id \Rightarrow \tau \in \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \Rightarrow \tau(\mathbb{F}) \subseteq \mathbb{F}$.

Sia $\beta : H \to \mathbb{F}^H = \{x \in \mathbb{F} \mid \sigma(x) = x\ \forall \sigma \in H\}$. Dimostriamo che $\alpha \circ \beta = \beta \circ \alpha = id$.

$H \xmapsto{\beta} \mathbb{E} = \mathbb{F}^H \xmapsto{\alpha} \mathrm{Gal}(\mathbb{F}/\mathbb{E})$. Banalmente $H \subseteq \mathrm{Gal}(\mathbb{F}/\mathbb{E})$. Per il teorema di Artin, $|H| = d \Rightarrow [\mathbb{F} : \mathbb{E}] = d \Rightarrow |H| = d = |\,\mathrm{Gal}(\mathbb{F}/\mathbb{E})| \Rightarrow H = \mathrm{Gal}(\mathbb{F}/\mathbb{E})$. Dunque $\alpha \circ \beta = id$.

$\mathbb{E} \xmapsto{\alpha} \mathrm{Gal}(\mathbb{F}/\mathbb{E}) = H \xmapsto{\beta} \mathbb{F}^H$. Banalmente $\mathbb{E} \subseteq \mathbb{F}^H$. Analogamente a sopra, per il teorema di Artin e per cardinalità si ottiene l'uguaglianza e dunque $\beta \circ \alpha = id$. □

Esempio:

$$\begin{tikzcd}
\mathbb{F} \arrow[r, leftrightarrow] \arrow[d, dash, "d_1"] \arrow[ddd, dash, bend right, "n"'] & H = \mathrm{Gal}(\mathbb{F}/\mathbb{F}) & |H| = 1 & H = \{e\} \\
\mathbb{E}' \arrow[r, leftrightarrow] \arrow[d, dash, "d_2"] & H = \mathrm{Gal}(\mathbb{F}/\mathbb{E}') & |H| = d_1 & \\
\mathbb{E} \arrow[r, leftrightarrow] \arrow[d, dash, "d_3"] & H = \mathrm{Gal}(\mathbb{F}/\mathbb{E}) & |H| = d_1 d_2 & \\
\mathbb{K} \arrow[r, leftrightarrow] & H = \mathrm{Gal}(\mathbb{F}/\mathbb{K}) & |H| = d_1 d_2 d_3 = n & H = G
\end{tikzcd}$$

Proposizione: Siano $\mathbb{F} \supseteq \mathbb{E} \supseteq \mathbb{K}$ campi tali che $\mathbb{F}/\mathbb{K}$ sia normale e $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Sia inoltre $H < G$, $\mathbb{E} = \mathbb{F}^H$. Allora $H \triangleleft G \Leftrightarrow \mathbb{E}/\mathbb{K}$ è un'estensione normale. In questo caso si ha anche $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \cong G/H$.

Dimostrazione. H è lo stabilizzatore di $\mathbb{E}$.
Sia $\sigma : \mathbb{E} \to \Omega$ tale che $\sigma|_{\mathbb{K}} = id$. Allora $\sigma(\mathbb{E}) = \mathbb{E}' \cong \mathbb{E}$. Sia H' il sottogruppo in corrispondenza di Galois con $\mathbb{E}'$.
Vediamo che $H' = \sigma H \sigma^{-1}$:

- $\subseteq$.
  $h' \in H' \Rightarrow h'(x') = x' \ \forall x' \in \mathbb{E}'$. $\sigma : \mathbb{E} \to \mathbb{E}'$ è un isomorfismo, dunque esiste $x \in \mathbb{E}$ tale che $\sigma(x) = x'$. Allora $\sigma^{-1}(h'(\sigma(x))) = x \Rightarrow h' = \sigma \circ h \circ \sigma^{-1}$ con $h \in H$.

- $\supseteq$.
  $(\sigma \circ h \circ \sigma^{-1})(x') = \sigma(h(x)) = \sigma(x) = x' \Rightarrow \sigma \circ h \circ \sigma^{-1} \in H'$.

Dunque $H \triangleleft G \Leftrightarrow H = H' \Leftrightarrow \mathbb{E} = \mathbb{E}' \Leftrightarrow \mathbb{E}/\mathbb{K}$ è normale.

Prendiamo adesso l'omomorfismo $\psi : G \to \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ tale che $\psi(\sigma) = \sigma|_{\mathbb{E}}$.
$\mathrm{Ker}\,\psi = \{\sigma \in G \mid \sigma|_{\mathbb{E}} = id\} = \{\sigma : \mathbb{F} \to \mathbb{F} \mid \sigma|_{\mathbb{E}} = id\} \cong \mathrm{Gal}(\mathbb{F}/\mathbb{E}) = H$. Quindi $G/H \cong \mathrm{Gal}(\mathbb{E}/\mathbb{K})$. □

Proposizione: Siano $\mathbb{E}/\mathbb{K}$ e $\mathbb{F}/\mathbb{K}$ due estensioni finite. $\mathbb{E}/\mathbb{K}$ estensione normale $\Rightarrow \mathbb{E}\mathbb{F}/\mathbb{F}$ estensione normale.

Dimostrazione. Riassumiamo le ipotesi della proposizione nel diagramma seguente:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{E}\mathbb{F} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{E} \arrow[dr, dash, "\text{normale}"'] & & \mathbb{F} \arrow[dl, dash] \\
 & \mathbb{K} &
\end{tikzcd}$$

Sia $\varphi : \mathbb{E}\mathbb{F} \to \Omega$ tale che $\varphi|_{\mathbb{F}} = id$.
$\mathbb{F} \supseteq \mathbb{K} \Rightarrow \varphi|_{\mathbb{K}} = id$, $\mathbb{E} \subseteq \mathbb{E}\mathbb{F} \Rightarrow \varphi(\mathbb{E}) \subseteq \mathbb{E}$.
Ma poiché $\varphi(\mathbb{F}) = \mathbb{F}$ allora anche $\varphi(\mathbb{E}\mathbb{F}) \subseteq \mathbb{E}\mathbb{F}$ dato che $\mathbb{E}\mathbb{F}$ è generato dagli elementi di $\mathbb{E}$ e di $\mathbb{F}$. □

Proposizione: Siano $\mathbb{E}/\mathbb{K}$ e $\mathbb{F}/\mathbb{K}$ estensioni finite con $\mathbb{E}/\mathbb{K}$ normale. Siano inoltre $G_1 = \mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{F})$ e $G_2 = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$. Allora la funzione restrizione $r : G_1 \to G_2$ tale che $r(\varphi) = \varphi|_{\mathbb{E}}$ è un isomorfismo tra G_1 e $\mathrm{Gal}(\mathbb{E}/\mathbb{E} \cap \mathbb{F})$.

Dimostrazione. La verifica che r sia un omomorfismo è lasciata.

r è iniettiva: supponiamo $\varphi|_{\mathbb{E}} = id$. Sappiamo per ipotesi che $\varphi|_{\mathbb{F}} = id$, $\Rightarrow \varphi|_{\mathbb{E}\mathbb{F}} = \varphi = id$.

r è surgettiva in $\mathrm{Gal}(\mathbb{E}/\mathbb{E} \cap \mathbb{F})$: usiamo il teorema di Artin, cercando il campo lasciato fisso dall'immagine.
$\varphi \in \mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{F}) \Rightarrow \varphi|_{\mathbb{F}} = id$, dunque il campo degli elementi fissati da $\mathrm{Im}(r)$ è costituito dagli elementi di $\mathbb{E}$ che appartengono a $\mathbb{F}$, ovvero $\mathbb{E} \cap \mathbb{F}$. $\Rightarrow \mathrm{Im}(r) \cong \mathrm{Gal}(\mathbb{E}/\mathbb{E} \cap \mathbb{F})$. □

Proposizione: Siano $\mathbb{E}/\mathbb{K}$ e $\mathbb{F}/\mathbb{K}$ estensioni normali. Allora $\mathbb{E}\mathbb{F}/\mathbb{K}$ è normale e $\mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{K})$ è isomorfo ad un sottogruppo di $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \times \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. Inoltre, se $\mathbb{E} \cap \mathbb{F} = \mathbb{K}$ allora $\mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{K}) \cong \mathrm{Gal}(\mathbb{E}/\mathbb{K}) \times \mathrm{Gal}(\mathbb{F}/\mathbb{K})$.

Dimostrazione. Riassumiamo le ipotesi della proposizione nel diagramma seguente:

$$\begin{tikzcd}
& \mathbb{E}\mathbb{F} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{E} \arrow[dr, dash] \arrow[ddr, dash, bend right, "\text{normale}"'] & & \mathbb{F} \arrow[dl, dash] \arrow[ddl, dash, bend left, "\text{normale}"] \\
& \mathbb{E}\cap\mathbb{F} \arrow[d, dash] & \\
& \mathbb{K} &
\end{tikzcd}$$

$\mathbb{E}\mathbb{F}/\mathbb{K}$ è normale: sia $\sigma : \mathbb{E}\mathbb{F} \to \Omega$ tale che $\sigma|_{\mathbb{K}} = id$; $\sigma|_{\mathbb{E}} \in \mathrm{Gal}(\mathbb{E}/\mathbb{K})$, dunque $\sigma(\mathbb{E}) \subseteq \mathbb{E}$. Analogamente $\sigma(\mathbb{F}) \subseteq \mathbb{F}$ e dato che gli elementi di $\mathbb{E}$ e $\mathbb{F}$ generano $\mathbb{E}\mathbb{F}$ allora $\sigma(\mathbb{E}\mathbb{F}) \subseteq \mathbb{E}\mathbb{F}$.

Consideriamo l'omomorfismo $\psi : \mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{K}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{K}) \times \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ tale che $\psi(\sigma) = (\sigma|_{\mathbb{E}}, \sigma|_{\mathbb{F}})$.
ψ è banalmente un omomorfismo. Verifichiamo che sia iniettivo:
se $\sigma|_{\mathbb{E}} = \sigma|_{\mathbb{F}} = id$ allora, poiché gli elementi di $\mathbb{E}$ e $\mathbb{F}$ formano un insieme di generatori per $\mathbb{E}\mathbb{F}$, $\sigma|_{\mathbb{E}\mathbb{F}} = \sigma = id$.

Quindi $\mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{K}) \hookrightarrow \mathrm{Gal}(\mathbb{E}/\mathbb{K}) \times \mathrm{Gal}(\mathbb{F}/\mathbb{K})$.

Inoltre, se $\mathbb{E}\cap\mathbb{F} = \mathbb{K}$ allora grazie all'isomorfismo $\mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{F}) \cong \mathrm{Gal}(\mathbb{E}/\mathbb{E}\cap\mathbb{F}) = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ si ha $|\,\mathrm{Gal}(\mathbb{E}\mathbb{F}/\mathbb{K})| = [\mathbb{E}\mathbb{F} : \mathbb{K}] = [\mathbb{E}\mathbb{F} : \mathbb{F}][\mathbb{F} : \mathbb{K}] = [\mathbb{E} : \mathbb{K}][\mathbb{F} : \mathbb{K}] = |\,\mathrm{Gal}(\mathbb{E}/\mathbb{K})| \cdot |\,\mathrm{Gal}(\mathbb{F}/\mathbb{K})|$ e dunque l'isomorfismo cercato. □

Teorema: Sia ζ_n una radice n-esima dell'unità in $\mathbb{C}$. Allora $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ e $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Dimostrazione. Sia $f(x) \in \mathbb{Q}[x]$ il polinomio minimo di ζ_n su $\mathbb{Q}[x]$. Poiché $f(\zeta_n) = 0$ allora $f(x) \mid x^n - 1$, ovvero $f(x)h(x) = x^n - 1$.
Per il Lemma di Gauss $f(x), h(x) \in \mathbb{Z}[x]$.
Sia p primo tale che $p \nmid n$. Dimostriamo che anche ζ_n^p (che è ancora una radice primitiva) è radice di $f(x)$.

Supponiamo per assurdo che ζ_n^p non sia radice di $f(x)$; allora $h(\zeta_n^p) = 0 \Rightarrow h(x^p)$ si annulla in $\zeta_n \Rightarrow f(x) \mid h(x^p)$.
Attraverso l'omomorfismo di riduzione modulo p abbiamo che $\overline{h(x^p)} = \overline{h(x)}^p$. Ma allora $\overline{f(x)} \mid \overline{h(x)}^p \Rightarrow \overline{f(x)} \mid \overline{h(x)}$ essendo $f(x)$ irriducibile. Ma allora $\overline{f}, \overline{h}$ non sono coprimi.
$x^n - 1 = \overline{f(x)} \cdot \overline{h(x)}$; ma $x^n - 1$ ha tutte le radici distinte, mentre $\overline{f(x)} \cdot \overline{h(x)}$ ha una radice multipla. Assurdo.

Osserviamo adesso che prendendo un $m < n$ tale che $(m, n) = 1$, allora $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ non necessariamente distinti tali che $(p_i, n) = 1$. Applicando ripetutamente quanto dimostrato sopra si giunge alla conclusione che tutte le radici n-esime primitive sono radici di $f(x)$. Dunque $\deg(f) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \geq \phi(n)$.

Notiamo adesso che $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longhookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ attraverso l'omomorfismo $(\sigma : \zeta_n \mapsto \zeta_n^i) \longmapsto i$.
Infatti sia $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\sigma(\zeta_n) = \zeta_n^i$. Poiché σ è un automorfismo di $\mathbb{Q}(\zeta_n)$ allora

anche $\sigma^{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $\sigma^{-1}(\zeta_n) = \zeta_n^j$. Allora $\zeta_n = \sigma^{-1}\sigma(\zeta_n) = \zeta_n^{ij} \Rightarrow \zeta_n^{ij-1} = 1$, ovvero $ij \equiv 1 \pmod n$ e dunque $i, j \in (\mathbb{Z}/n\mathbb{Z})^*$.
Quindi l'applicazione è ben definita; la verifiche che si tratti di un omomorfismo e che sia iniettivo sono banali.

Allora $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n) \Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ e inoltre

$$f(x) = \prod_{\substack{i<n \\ (i,n)=1}} (x - \zeta_n^i)$$

$\square$

7.2 Gruppo di Galois del c.d.s. di polinomi di grado 2

Sia $p(x) \in \mathbb{Q}[x]$ un polinomio di grado 2. Senza perdita di generalità possiamo considerarlo monico: $p(x) = x^2 + ax + b$ con $a, b \in \mathbb{Q}$.

Se $p(x)$ è riducibile come prodotto di fattori lineari allora il campo di spezzamento di $p(x)$ su $\mathbb{Q}$ è $\mathbb{Q}$ stesso, e il gruppo di Galois è banale.

Se $p(x)$ è irriducibile allora le radici sono $\alpha_{1,2} = \frac{-a \pm \sqrt{a^2-4b}}{2} \notin \mathbb{Q}$. Chiamando $\Delta = a^2 - 4b$, il campo di spezzamento di $p(x)$ su $\mathbb{Q}$ è $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\frac{-a\pm\sqrt{\Delta}}{2}) = \mathbb{Q}(\pm\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\Delta})$ e dunque $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

7.3 Gruppo di Galois del c.d.s. di polinomi di grado 3

Sia $p(x) \in \mathbb{Q}[x]$ un polinomio di grado 3. Senza perdita di generalità possiamo considerarlo monico: $p(x) = x^3 + ax^2 + bx + c$.
Inoltre, vediamo come possiamo considerare $a = 0$: infatti, ponendo $x' = x + \frac{a}{3}$, si ha che $p(x') = x'^3 + \alpha x + \beta$ per certi valori di $\alpha \quad \beta \in \mathbb{Q}$.

Se $p(x) = x^3 + \alpha x + \beta$ è riducibile su $\mathbb{Q}$ allora si ricade nel caso analizzato sopra.
Se $p(x)$ è irriducibile, chiamando $\mathbb{K}$ il suo campo di spezzamento, abbiamo $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \hookrightarrow S_3$ e $3 \mid \#\,\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Dunque $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong S_3 \vee \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong A_3$.

Siano a_1, a_2, a_3 le radici di $p(x)$: allora $p(x) = (x - a_1)(x - a_2)(x - a_3) = x^3 + \alpha x + \beta \Rightarrow$
$\begin{cases} a_1 + a_2 + a_3 = 0 \\ a_1a_2 + a_1a_3 + a_2a_3 = \alpha \\ a_1a_2a_3 = -\beta \end{cases}$.

Sia $\delta = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$. $\delta \in \mathbb{K}$. Se $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ allora $\sigma(\delta) = \pm\delta$: le permutazioni pari fissano δ mentre le permutazioni dispari ne cambiano il segno.

Allora δ^2 è invariante rispetto a $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, cioè $\delta^2 \in \mathbb{Q}$. Infatti $\Delta = \delta^2 = -4\alpha^3 - 27\beta^2$.

- Se $\sqrt{\Delta} = \delta \in \mathbb{Q}$ allora in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ ci sono solo permutazioni pari, e dunque $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong A_3$;
- Se $\sqrt{\Delta} = \delta \notin \mathbb{Q}$ allora $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong S_3$.

7.4 Gruppo di Galois del c.d.s. di polinomi biquadratici

Sia $p(x) \in \mathbb{Q}[x]$ di grado 4 e biquadratico. Sena perdita di generalità possiamo considerarlo monico: $p(x) = x^4 + ax^2 + b$.

Se $p(x)$ è riducibile allora si scrive come prodotto di fattori di secondo grado e il gruppo di Galois risultante si trova analizzando i campi di spezzamento dei fattori di grado 2.

Se $p(x)$ è irriducibile allora considero il polinomio $q(y) = y^2 + ay + b$ ponendo $y = x^2$. Poiché $p(x)$ non si fattorizza, allora le radici di $q(y)$ generano una prima estensione di grado 2 su $\mathbb{Q}$.

Siano ω_1, ω_2 le radici di $q(y)$: $\omega_{1,2} = \frac{-a \pm \sqrt{a^2-4b}}{2} = \frac{-a \pm \sqrt{\Delta}}{2}$. Allora le radici di $p(x)$ sono $\pm\sqrt{\omega_1}, \pm\sqrt{\omega_2}$ e $b = \omega_1\omega_2$.

$$\begin{array}{c}
\mathbb{K} = \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}, \sqrt{\omega_2}) \\
\big| \scriptstyle{1\ o\ 2} \\
\mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1}) \\
\big| \scriptstyle{1\ o\ 2} \\
\mathbb{Q}(\sqrt{\Delta}) \\
\big| \scriptstyle{2} \\
\mathbb{Q}
\end{array}$$

Dunque $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \hookrightarrow D_4$ cioè il 2-Sylow di S_4.

- Se b è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$, cioè $\sqrt{b} = \sqrt{\omega_1}\sqrt{\omega_2} \in \mathbb{Q}(\sqrt{\Delta})$:

  – Se b è un quadrato in $\mathbb{Q}$, cioè $\sqrt{b} = \sqrt{\omega_1}\sqrt{\omega_2} \in \mathbb{Q}$ allora $\sqrt{\omega_2} \in \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1})$ e dunque $[\mathbb{K} : \mathbb{Q}] = 4$.

    Inoltre $\left.\begin{array}{l} (\sqrt{\omega_1} \leftrightarrow -\sqrt{\omega_1}, \sqrt{\omega_2} \leftrightarrow -\sqrt{\omega_2}) \\ (\sqrt{\omega_1} \leftrightarrow \sqrt{\omega_2}, -\sqrt{\omega_1} \leftrightarrow -\sqrt{\omega_2}) \\ (\sqrt{\omega_1} \leftrightarrow -\sqrt{\omega_2}, -\sqrt{\omega_1} \leftrightarrow \sqrt{\omega_2}) \end{array}\right\} \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ e hanno tutte ordine 2.
    $\Rightarrow \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

  – Se b non è un quadrato in $\mathbb{Q}$ ma lo è in $\mathbb{Q}(\sqrt{\Delta})$, allora analogamente a sopra $\sqrt{\omega_1}\sqrt{\omega_2} \in \mathbb{Q}(\sqrt{\Delta}) \Rightarrow \sqrt{\omega_2} \in \mathbb{Q}(\sqrt{\Delta}, \sqrt{\omega_1})$ e dunque $[\mathbb{K} : \mathbb{Q}] = 4$.

    Sia $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q})$ tale che $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$. τ può essere estesa a $\tilde{\tau} \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ tale che $\tilde{\tau} : \left\{\begin{array}{l} \sqrt{\Delta} \longmapsto -\sqrt{\Delta} \\ \sqrt{\omega_1} \longmapsto \pm\sqrt{\omega_2} \\ \sqrt{\omega_2} \longmapsto \mp\sqrt{\omega_1} \end{array}\right.$ (perchè $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$ e dunque $\tau(\omega_1) = \omega_2$).
    Si verifica banalmente che $\tilde{\tau}$ ha ordine 4 $\Rightarrow \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

- Se b non è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$, allora $[\mathbb{Q}(\sqrt{\Delta}, \sqrt{b}) : \mathbb{Q}(\sqrt{\Delta})] = 2$.
  $\Rightarrow \exists \sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta}, \sqrt{b})/\mathbb{Q}(\sqrt{\Delta}))$ tale che $\sigma(\sqrt{b}) = -\sqrt{b}$.

  Vediamo in quali modi è possibile estendere σ a $\tilde{\sigma} \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q}(\sqrt{\Delta}))$:
  poiché σ fissa il campo $\mathbb{Q}(\sqrt{\Delta})$ allora $\tilde{\sigma}(\omega_1) = \tilde{\sigma}(\frac{-a+\sqrt{\Delta}}{2}) = \omega_1$.
  Dunque le uniche $\tilde{\sigma}$ possibili sono $\tilde{\sigma} : \begin{cases} \sqrt{b} \longmapsto -\sqrt{b} \\ \sqrt{\omega_1} \longmapsto \pm\sqrt{\omega_1} \\ \sqrt{\omega_2} \longmapsto \mp\sqrt{\omega_2} \end{cases}$.
  Entrambi questi automorfismi hanno ordine 2 e sono distinti, quindi $|\,\mathrm{Gal}(\mathbb{K}/\mathbb{Q}(\sqrt{\Delta}))| \geq 4$ e dunque $[\mathbb{K} : \mathbb{Q}(\sqrt{\Delta})] = 4$.

  Allora $[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\sqrt{\Delta})][\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 4 \cdot 2 = 8 \Rightarrow \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong D_4$.