Dispense del corso di Algebra 1, a.a. 2016-2017

Giovanni Gaiffi

queste dispense contengono parti riadattate da dispense di un corso precedente, curate da Alessio Del Vigna

20 dicembre 2016

Indice

Capitolo 1

Azioni di gruppi (lezione del 27 settembre)

1.1 Azione di un gruppo su un insieme

Definizione 1.1.1. Sia X un insieme e G un gruppo. Un'*azione* di G su X è una mappa:

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

che soddisfa le seguenti proprietà:

(1) $e \cdot x = x$ per ogni $x \in X$;

(2) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ per ogni $g_1, g_2 \in G$ e per ogni $x \in X$.

Esempio 1.1.1. Un primo esempio lo abbiamo già incontrato: il gruppo $\mathcal{S}_n$ agisce infatti sull'insieme $X = \{1, 2, \ldots, n\}$ permutandone gli elementi. Ossia si costruisce la mappa $(\sigma, x) \mapsto \sigma(x)$, con $\sigma \in \mathcal{S}_n$ e $x \in X$.

Esempio 1.1.2. Consideriamo il gruppo diedrale D_n delle isometrie del piano che mandano un poligono regolare di n lati in sé. Tale gruppo, come sappiamo, è costituito dalle n rotazioni di centro il baricentro dei vertici e di angolo multiplo di $\frac{2\pi}{n}$ e dalle n simmetrie rispetto agli assi di simmetria del poligono stesso.
Numerando i vertici di un poligono con i numeri $1, 2, \ldots, n$ si ha che D_n agisce sull'insieme $X = \{1, 2, \ldots, n\}$. Sostanzialmente questo ci permette di vedere D_n come sottogruppo di $\mathcal{S}_n$ "leggendo" i suoi elementi come permutazioni degli elementi di X.

Esempio 1.1.3. Sia G un gruppo. Affermiamo che

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gxg^{-1} \end{array}$$

è un azione di G su G. La verifica delle proprietà (1) e (2) è immediata.

Esempio 1.1.4. Il gruppo $GL(V)$ degli endomorfismi lineari invertibili di uno spazio vettoriale V agisce sull'insieme V. Se V ha anche una struttura euclidea, il gruppo $O(V)$ delle trasformazioni ortogonali agisce sulla sfera unitaria di V.

Esempio 1.1.5. Sia G un gruppo e $H < G$. Affermiamo che

$$\begin{array}{ccc} G \times G/H & \longrightarrow & G/H \\ (g,\, g_1 H) & \longmapsto & (gg_1)\, H \end{array}$$

è un azione di G su G/H. Anche in questo caso lasciamo la verifica per esercizio.

Definizione 1.1.2. Sia G un gruppo che agisce su un insieme X. Diciamo *orbita* di $x \in X$ l'insieme $\mathrm{orb}(x) = G \cdot x = \{g \cdot x \mid g \in G\}$. Diciamo invece *stabilizzatore* di $x \in X$ l'insieme $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$.

Lemma 1.1.1. *Sia G un gruppo che agisce su un insieme X. Allora* $\mathrm{Stab}(x) < G$.

Dimostrazione. Siano $g_1, g_2 \in \mathrm{Stab}(x)$, vediamo se anche il loro prodotto è nello stabilizzatore. Affermiamo di sì, e infatti si ha

$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x.$$

Sia $g \in \mathrm{Stab}(x)$, allora per definizione $g \cdot x = x$. Applicando g^{-1} ad entrambi i membri si ottiene

$$g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x,$$

ma il membro di sinistra è uguale a x, infatti:

$$g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = e \cdot x = x,$$

Dunque abbiamo ottenuto

$$x = g^{-1} \cdot x,$$

ossia $g^{-1} \in \mathrm{Stab}(x)$. □

Esercizio 1.1.1. Mostrare con un esempio che in generale $\mathrm{Stab}(x)$ non è un sottogruppo normale di G. [Per esempio considerare S_3 che agisce su $\{1, 2, 3\}$, e lo stabilizzatore Stab(1).]

Teorema 1.1.1. *Sia G un gruppo che agisce su un insieme X e sia $x \in X$. Esiste una corrispondenza bigettiva tra $G/\mathrm{Stab}(x)$ e $\mathrm{orb}(x)$.*

Dimostrazione. Costruiamo la mappa seguente:

$$\begin{array}{rccc} f: & G/\mathrm{Stab}(x) & \longrightarrow & \mathrm{orb}(x) \\ & g\,\mathrm{Stab}(x) & \longmapsto & g\cdot x \end{array}.$$

Intanto affermiamo che f è ben definita. Presentiamo $g\,\mathrm{Stab}(x)$ in un'altra forma, ad esempio $k\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x)$: allora dovrà essere $k = gs$ con $s \in \mathrm{Stab}(x)$. Vediamo cosa accade quando si applica la regola per trovare l'immagine: $k \cdot x = gs \cdot x = g \cdot (s \cdot x) = g \cdot x$ e quindi l'applicazione è ben definita.
Per la surgettività è sufficiente osservare che dato $g_1 \cdot x \in \mathrm{orb}(x)$ basta prendere $g_1\mathrm{Stab}(x)$ nel dominio.
Infine per l'iniettività sia $f(g\,\mathrm{Stab}(x)) = f(h\,\mathrm{Stab}(x))$, ossia $g \cdot x = h \cdot x$. Facendo agire da entrambe le parti h^{-1} otteniamo $\left(h^{-1}g\right) \cdot x = x$ e quindi $h^{-1}g \in \mathrm{Stab}(x)$. Da questo immediatamente ricaviamo $g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$. □

Proposizione 1.1.1. *Sia G un gruppo che agisce sull'insieme X. Allora ogni elemento di X appartiene ad una e una sola orbita.*

Dimostrazione. Sia $x \in X$, ovviamente $x \in \mathrm{orb}(x)$. Supponiamo che $x \in \mathrm{orb}(y)$, questo significa che esiste un $g \in G$ tale che $g \cdot y = x$. Questo implica che $\mathrm{orb}(x) \subseteq \mathrm{orb}(y)$; ma potendo scrivere anche che $y = g^{-1} \cdot x$ si ha che $\mathrm{orb}(y) \subseteq \mathrm{orb}(x)$. □

La proposizione appena presentata è molto importante in quanto afferma che le orbite determinano una partizione di X. I risultati sin qui conseguiti portano al seguente:

Teorema 1.1.2. *Siano G un gruppo finito che agisce su un insieme finito X e siano $x_1, \ldots, x_d$ rappresentanti delle orbite dell'azione. Allora*

$$|X| = \sum_{i=1}^{d} \frac{o(G)}{o\left(\mathrm{Stab}(x_i)\right)}.$$

Dimostrazione. Considerando le orbite una partizione di X si ha che $|X| = \sum_{i=1}^{d} |\mathrm{orb}(x_i)|$. Inoltre si ha che $|\mathrm{orb}(x_i)| = \frac{o(G)}{|\mathrm{Stab}(x_i)|}$ per la corrispondenza biunivoca introdotta prima. □

1.2 Formula delle classi e prime conseguenze

Adesso vogliamo applicare tutti i risultati conseguiti fin qui al caso dell'azione di un gruppo finito su se stesso per coniugio. Ossia consideriamo:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & g \cdot x = gxg^{-1} \end{array}.$$

Nel caso di questa azione, che vedremo essere molto importante, le orbite e gli stabilizzatori degli elementi di G assumono dei nomi particolari:

Definizione 1.2.1. Quando G agisce su se stesso per coniugio l'orbita di un elemento prende il nome di *classe di coniugio*, mentre lo stabilizzatore di un elemento $x \in G$ si chiama *centralizzante di* x o anche *centralizzatore di* x, e si indica con $C(x)$.

Osserviamo che il centralizzante è l'insieme

$$C(x) = \mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\},$$

ossia è il più grande sottogruppo di G nel quale x è nel centro.

Esercizio 1.2.1. Consideriamo la permutazione $\sigma = (1, 2, 3) \in S_4$. Come sappiamo, la classe di coniugio a cui appartiene in S_4 è costituita da tutti i 3-cicli, dunque ha 8 elementi. Pensiamo ora a σ come ad un elemento di A_4. Qual è la classe di coniugio a cui appartiene σ in A_4?

Il teorema 1.1.2, nel caso dell'azione di un gruppo finito su se stesso per coniugio, si traduce così:

Teorema 1.2.1 (formula delle classi, detta anche equazione delle classi)**.** *Sia G un gruppo finito. Allora*

$$o(G) = \sum \frac{o(G)}{o(C(g))},$$

dove la somma è estesa ai g rappresentanti delle classi di coniugio, uno per ognuna di esse.

Dimostrazione. È immediata conseguenza del teorema 1.1.2. □

Ecco qualche prima conseguenza della formula delle classi.

Proposizione 1.2.1. *Se $o(G) = p^n$ con p primo, allora $Z(G) \neq \{e\}$.*

Dimostrazione. Se $g \in G$ allora $o(C(g))$, essendo un divisore di p^n (per il Teorema di Lagrange), deve essere uguale a p^{n_g} con $n_g \leq n$. Inoltre affermiamo che $n_g = n$ se e solo se $g \in Z(G)$, perché $g \in Z(G)$ se e solo se l'orbita di g è costituita dal solo g, che equivale a dire $C(g) = G$. Scriviamo l'equazione delle classi per il nostro gruppo; detti $g_1, \ldots, g_k$ rappresentanti di tutte le distinte classi di coniugio si ha:

$$o(G) = p^n = \sum_{i=1}^{k} \frac{o(G)}{o(C(g_i))} = \sum_{i=1}^{k} \frac{p^n}{p^{n_{g_i}}} = o(Z(G)) + \sum_{n_g < n} \frac{p^n}{p^{n_g}},$$

dove abbiamo contato separatamente le orbite costituite da un solo elemento, che sono $o(Z(G))$. A questo punto osserviamo che p divide sia il primo membro sia

$\sum_{n_g<n} \frac{p^n}{p^{n_g}}$; dunque deve dividere anche $o(Z(G))$. Dal momento che $o(Z(G)) \geq 1$ poiché $e \in Z(G)$ si ha $o(Z(G)) > 1$. □

Corollario 1.2.1. *Se $o(G) = p^2$ allora G è abeliano.*

Dimostrazione. Per il teorema precedente il centro di G non è banale e dunque per il suo ordine non ci sono che due possibilità: o è p o è p^2, dovendo dividere $o(G) = p^2$. Supponiamo per assurdo che $o(Z(G)) = p$, allora esisterebbe $a \in G - Z(G)$. Per come sono definiti il centro e il centralizzante si ha che $C(a) \supseteq Z(G)$, ed anzi l'inclusione è stretta perché $a \in C(a)$ ma $a \notin Z(G)$. Ma allora $C(a)$ è un sottogruppo che ha più di p elementi e dunque ne deve avere p^2, ossia $C(a) = G$. Da questo seguirebbe che $a \in Z(G)$ e ciò è assurdo.
Dunque $Z(G)$ ha ordine p^2 e di conseguenza $Z(G) = G$. □

Capitolo 2

Approfondimenti sulle azioni (lezione del 28 settembre)

2.1 Il Teorema di Cauchy

Adesso useremo l'equazione delle classi per dimostrare un teorema cardine della teoria dei gruppi, che è il teorema di Cauchy[1]. In realtà il teorema di Cauchy è conseguenza immediata del teorema di Sylow, un risultato molto più forte che dimostreremo più avanti nel corso. Ma vogliamo lo stesso dare subito questa dimostrazione del teorema di Cauchy, dovuta a McKay, in quanto è molto elegante.

Teorema 2.1.1 (di Cauchy)**.** *Sia G un gruppo finito e sia p un numero primo tale che $p \mid o(G)$. Allora G ha un elemento di ordine p; più precisamente le soluzioni di $x^p = e$ in G sono kp con $k \geq 1$.*

Dimostrazione. Consideriamo l'insieme

$$S = \{(a_1, \ldots, a_p) \mid a_i \in G,\ a_1 a_2 \cdots a_{p-1} a_p = e\},$$

Questo insieme ha cardinalità $|S| = |G|^{p-1}$, in quanto possiamo fissare arbitrariamente in G i primi $p-1$ elementi della p–upla e poi siamo costretti a porre $a_p = (a_1 \cdots a_{p-1})^{-1}$. Ci interesseranno in particolar modo le p–uple in S che hanno tutte le componenti uguali; infatti, se $(a, a, \ldots, a) \in S$ allora $a^p = e$.
Consideriamo l'azione di $\mathbb{Z}_p$ su S definita nel modo seguente: l'elemento $[1]_p \in \mathbb{Z}_p$ applicato alla p–upla $(a_1, \ldots, a_p)$ dà la p-upla $(a_p, a_1, a_2 \ldots, a_{p-1})$, insomma "sposta ciclicamente tutti gli a_i di una posizione". Di conseguenza l'elemento $[i]_p \in \mathbb{Z}_p$ "sposta" gli a_i ciclicamente di i posizioni.

Esercizio 2.1.1. Dimostrare che si tratta effettivamente di un'azione di $\mathbb{Z}_p$ su S.

[1] Augustin-Louis Cauchy (1789 ? 1857), matematico francese.

[Cominciare dalla verifica che, se $(a_1, a_2, \ldots, a_p)$ appartiene ad S, allora anche $(a_p, a_1, a_2 \ldots, a_{p-1})$ appartiene ad S.]

Si osserva che se la p–upla ha tutte le componenti uguali ad a allora la sua orbita ha cardinalità 1. Se invece esistono $i \neq j$ tali che $a_i \neq a_j$ allora la cardinalità dell'orbita di quella p–upla è necessariamente p (del resto, visto che sta agendo il gruppo $\mathbb{Z}_p$, gli stabilizzatori possibili sono solo $\{[0]\}$ e $\mathbb{Z}_p$ e dunque le cardinalità delle orbite possono essere solo p o 1).

Detto U l'insieme delle p–uple con tutte le componenti uguali e detti $s_1, \ldots, s_n \in S$ rappresentanti delle orbite di cardinalità p, usando il teorema 1.1.2 si può scrivere:

$$|S| = |G|^{p-1} = |U| + \sum_{i=1}^{n} |\mathrm{orb}(s_i)| = |U| + pn$$

Da questo segue che $p \mid |U|$. Visto che $|U| \geq 1$ (infatti $(e, e, ..., e) \in U$, si deduce che $|U|$ ha kp elementi per qualche $k \geq 1$. Ma U è l'insieme delle p–uple con tutte le componenti uguali, che possiamo identificare con l'insieme delle soluzioni di $x^p = e$. Ci sono dunque kp soluzioni di questa equazione: a parte l'identità, tutte le altre devono essere elementi di ordine p, visto che p è primo [2]. □

2.2 Il teorema di Cayley

Quando un gruppo agisce su un insieme, l'azione può essere anche descritta in termini di applicazioni dell'insieme in sé indotte da ogni elemento di G.

Teorema 2.2.1. *Sia G un gruppo che agisce su un insieme X e sia $g \in G$. L'applicazione $\phi_g : X \to X$ tale che $\phi_g(x) = g \cdot x$ è bigettiva. Inoltre, se chiamiamo $Big(X)$ il gruppo delle applicazioni bigettive da X in sé, l'applicazione*

$$\phi : G \to Big(X)$$

che associa a g l'applicazione ϕ_g è un omomorfismo di gruppi.

Dimostrazione. L'applicazione ϕ_g è surgettiva perché preso $x \in X$ si ha che $g^{-1} \cdot x \in X$ viene mandato da ϕ_g in x in quanto:

$$\phi_g\left(g^{-1} \cdot x\right) = g \cdot g^{-1} \cdot x = \left(gg^{-1}\right) \cdot x = x.$$

Inoltre ϕ_g è iniettiva perché se $g \cdot x = g \cdot y$ allora $x = y$ in quanto si può applicare g^{-1} da entrambe le parti.
Consideriamo ora l'applicazione:

$$\begin{array}{rccc} \phi : & G & \longrightarrow & Big(X) \\ & g & \longmapsto & \phi_g \end{array},$$

[2] Essendo $a^p = e$ e $a \neq e$ si ha che $o(a) \mid p$, e non potendo essere 1 deve essere p.

e mostriamo che si tratta di un omomorfismo di gruppi. Se $g_1, g_2 \in G$ allora vale $\phi(g_1 g_2) = \phi(g_1) \circ \ \phi(g_2)$. Infatti per ogni $x \in X$ possiamo scrivere:

$$\phi(g_1 g_2)(x) = \phi_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi_{g_1}\left(\phi_{g_2}(x)\right) = \phi_{g_1} \circ \phi_{g_2}(x) = \phi(g_1) \circ \phi(g_2)(x)$$

e abbiamo concluso. □

Corollario 2.2.1. *Consideriamo un gruppo G che agisce su un insieme X di cardinalità n. Se identifichiamo $Big(X)$ con il gruppo S_n, l'omomorfismo ϕ del teorema precedente ci dà un omomorfismo:*

$$\phi \ : \ G \to S_n$$

Applichiamo quanto visto al caso in cui un gruppo G agisce su sé stesso "per moltiplicazione a sinistra".

Teorema 2.2.2 (teorema di Cayley[3])**.** *Sia G un gruppo finito con n elementi. Allora G è isomorfo ad un sottogruppo di S_n.*

Dimostrazione. Consideriamo la seguente azione (il lettore dimostri che in effetti lo è):

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, h) & \longmapsto & gh \end{array} .$$

Sappiamo dal lemma precedente che esiste l'omomorfismo

$$\phi : G \to Big(G) \cong S_n$$

che manda $g \mapsto \phi_g$ dove l'applicazione ϕ_g è quella che porta $h \mapsto gh$ per ogni $h \in G$. Mostriamo adesso che ϕ è iniettivo: supponiamo $\phi_{g_1} = \phi_{g_2}$. Questo significa che per ogni $h \in G$ abbiamo $g_1 h = g_2 h$, e quindi $g_1 = g_2$.
Essendo ϕ un omomorfismo iniettivo abbiamo, per il primo teorema di isomorfismo, che $G \cong \operatorname{Im} \phi < S_n$. □

Osserviamo che nel teorema di Cayley G si immerge nel gruppo simmetrico $S_{|G|}$ che è un gruppo di cardinalità $|G|!$, dunque 'molto grande'. Se prendiamo $G = S_n$ questo significa per esempio che stiamo immergendo S_n in $S_{n!}$: non è certo il gruppo simmetrico più piccolo dove si può immergereS_n (che è S_n stesso...).

[3]Arthur Cayley (1821-1895), matematico inglese.

2.3 Alcuni esercizi sul calcolo di orbite

Cominciamo con alcuni esercizi di ripasso del corso di Aritmetica. Scrivete la dimostrazione con tutti i dettagli:

Esercizio 2.3.1. I coniugati di una permutazione $\sigma \in S_n$ prodotto di r cicli disgiunti di lunghezza $n_1, n_2, \ldots, n_r$ sono tutte e sole le permutazioni prodotto di r cicli disgiunti di lunghezza $n_1, n_2, \ldots, n_r$.

Esercizio 2.3.2. Date $\sigma = (1\ 3\ 2)(4\ 7\ 5\ 6) \in \mathcal{S}_9$ e $\sigma' = (i_1\ i_2\ i_3)(i_4\ i_5\ i_6\ i_7) \in \mathcal{S}_9$ descrivere una permutazione τ tale che $\tau\sigma\tau^{-1} = \sigma'$.

Soluzione. Come sappiamo,

$$\tau\sigma\tau^{-1} = (\tau(1)\ \tau(3)\ \tau(2))(\tau(4)\ \tau(7)\ \tau(5)\ \tau(6)),$$

Allora basta prendere

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ i_1 & i_3 & i_2 & i_4 & i_6 & i_7 & i_5 & x & y \end{pmatrix}$$

con $x, y \neq i_j$ per $1 \leq j \leq 7$ e $y \neq x$. Osserviamo che avremmo anche potuto porre $\tau(1) = i_2$, oppure $\tau(1) = i_3$; una volta scelto $\tau(1)$, allora $\tau(2)$ e $\tau(3)$ sono obbligati. Similmente avremmo potuto porre anche $\tau(4) = i_5$ oppure $\tau(4) = i_6$ oppure $\tau(4) = i_7$, dopodiché $\tau(5),\ \tau(6),\ \tau(7)$ sono obbligati.

Cerchiamo di determinare il centralizzante di una data permutazione, intanto in alcuni casi semplici.

Esempio 2.3.1. Considerare $\sigma = (1\ 2\ 3)$ in $\mathcal{S}_n$ con $n \geq 3$; vogliamo determinarne il centralizzante. Sicuramente commutano con σ tutte le permutazioni che lasciano fissi 1, 2 e 3, che sono $(n-3)!$; inoltre commutano con σ anche σ stessa e σ^2. Quindi tutte le permutazioni del tipo $\tau\sigma^i$, dove τ lascia fissi 1, 2 e 3, e $i = 1, 2, 3$, sono nel centralizzante. Abbiamo esibito $3(n-3)!$ elementi del centralizzante.

Vediamo che non ce ne sono altri. Sappiamo che

$$\frac{o(\mathcal{S}_n)}{o(C(\sigma))} = |\mathrm{orb}(\sigma)|;$$

ora, l'orbita di σ è fatta da tutti e soli i 3-cicli, che sono $\frac{1}{3}\frac{n!}{(n-3)!}$. Dall'equazione precedente ricaviamo che il numero di permutazioni che commutano con σ è $3(n-3)!$, e quindi quelle che abbiamo trovato sono tutte.

Il prossimo esercizio ci chiede di estendere l'esempio quando σ è un ciclo generico di lunghezza k dentro $\mathcal{S}_n$. Ricordiamo che il numero di k–cicli distinti in $\mathcal{S}_n$ (con $k \leq n$) è

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

Esercizio 2.3.3. Sia $\sigma = (1\ 2\ \ldots\ k)$. Dimostrare che il centralizzante di σ è costituito da tutti e soli gli elementi della forma $\sigma^i\tau$, dove $1 \leq i \leq k$ e τ è una permutazione che lascia fissi 1, 2, ..., k.

Esercizio 2.3.4. Descrivere il centralizzante di $(1\ 2\ 3\ 4)(5\ 6)$ in S_9 [svolto a lezione].

Esercizio 2.3.5. Descrivere il centralizzante di $(1\ 2)(3\ 4)$ in S_5. [Contare prima la cardinalità: ha otto elementi. Quali sono?]

Esercizio 2.3.6. Dimostrare che la classe di coniugio di $(1\ 2\ 3)$ in A_4 (attenzione, non in S_4 !) è composta da quattro elementi.

Soluzione. Si calcola, come negli esercizi precedenti, il centralizzante di $(1\ 2\ 3)$ in S_4 e si scopre che è costituito da solo tre elementi: e, $(1\ 2\ 3)$, $(1\ 3\ 2)$. Sono tutte permutazioni pari, dunque coincide con il centralizzante di $(1\ 2\ 3)$ in A_4. Allora l'orbita di $(1\ 2\ 3)$ in A_4 ha $|A_4|/3 = 12/3 = 4$ elementi. [Si consiglia a questo punto di trovarli: sono $(1\ 2\ 3)$, $(2\ 1\ 4)$, $(3\ 4\ 1)$, $(4\ 3\ 2)$.]

Generalizziamo il risultato di questo esercizio.

Esercizio 2.3.7. Sia $\sigma \in A_n$ una permutazione che si scrive come prodotto di $r \geq 1$ cicli disgiunti $c_1, c_2, \ldots, c_r$ di lunghezza rispettivamente $l_1, l_2, \ldots, l_r$ (osserviamo che stiamo considerando anche i cicli di lunghezza 1; per esempio $(1\ 2\ 3)$ in A_4 la consideriamo composta da due cicli, di lunghezza rispettivamente 3 e 1). Dimostrare che la classe di coniugio di σ in A_n coincide con la classe di coniugio di σ in S_n tranne nel caso in cui i numeri l_i siano dispari e, se $r \geq 2$, a due a due distinti. In tal caso la classe di coniugio di σ in A_n contiene la metà degli elementi della classe di coniugio di σ in S_n (che si "spezza" in due classi di coniugio di A_n).

Suggerimento per la soluzione. Supponiamo che ci sia un ciclo c_i di lunghezza pari, e prendiamo σ' appartenente alla classe di coniugio di σ in S_n. Dunque vale $\tau\sigma\tau^{-1} = \sigma'$ per un certo $\tau \in S_n$. Se τ è una permutazione pari, allora si conclude immediatamente che σ' appartiene anche alla classe di coniugio di σ in A_n. Se è dispari, osserviamo che τc_i è pari e che $\tau c_i \sigma c_i^{-1}\tau^{-1} = \sigma'$. In questo modo vediamo che per avere speranza che la classe di coniugio si spezzi gli l_i devono essere tutti dispari... in maniera simile si prosegue e si trova che per avere speranza che la classe di coniugio si spezzi gli l_i devono essere tutti dispari e a due a due disgiunti. D'altra parte, se gli l_i sono tutti dispari e a due a due disgiunti si calcola il centralizzante di σ in S_n e si scopre che i suoi elementi sono tutti permutazioni pari. La relazione $|orb(x)| = |G|/|Stab(x)|$ ci dice in questo caso che la classe di coniugio di σ in A_n contiene la metà degli elementi della classe di coniugio di σ in S_n...

A proposito del gruppo A_n, è importante osservare (ci sarà utile nei prossimi paragrafi) che:

Esercizio 2.3.8. Sia H un sottogruppo di S_n. Allora o tutte le permutazioni in H sono pari ($H < A_n$) oppure in H metà delle permutazioni sono pari e metà sono dispari ($|H \cap A_n| = |H \cap (S_n - A_n)|$).

Soluzione. Se $H < A_n$ abbiamo finito. Se invece $H \cap A_n \subsetneq H$ esiste in H una permutazione σ dispari. La funzione $f : H \cap A_n \to H \cap (S_n - A_n)$ data da $f(h) = \sigma h$ è ben definita.

Ricordiamo che anche la σ^{-1} è una permutazione dispari, visto che ha la stessa struttura ciclica della σ. Questa osservazione ci permette di concludere che f è bigettiva: infatti ha un'inversa $g : H \cap (S_n - A_n) \to H \cap A_n$ data da $g(\tau) = \sigma^{-1}\tau$.

2.4 Un importante criterio per decidere se un sottogruppo è normale

Teorema 2.4.1. *Sia G un gruppo finito e H un sottogruppo il cui indice è un numero primo p. Se p è il più piccolo primo che divide $o(G)$ allora H è normale in G.*

Dimostrazione. Consideriamo G che agisce su G/H con l'azione descritta in uno dei primi esempi:

$$\begin{array}{ccc} G \times G/H & \longrightarrow & G/H \\ (g, xH) & \longmapsto & (gx)H \end{array}.$$

Sappiamo che l'applicazione $\phi : G \to Big(G/H)$ è un omomorfismo di gruppi, con $Big(G/H) \cong \mathcal{S}_p$. Vale che $\ker\phi \subseteq H$: se prendiamo $k \in \ker\phi$ allora $k \cdot (gH) = gH$ per ogni classe gH, e in particolare $kH = H$, ossia $k \in H$.
Vorremmo riuscire a dimostrare l'inclusione opposta, in quanto a quel punto segue immediatamente che H è normale in G, essendolo $\ker\phi$. In particolare mostreremo che $\ker\phi$ ha la stessa cardinalità di H. Dal primo teorema di omomorfismo segue che $G/\ker\phi \cong \operatorname{Im}\phi < \mathcal{S}_p$.

Allora, essendo $\operatorname{Im}\phi < \mathcal{S}_p$, si ha che $o(G/\ker\phi) \mid o(\mathcal{S}_p) = p!$. Se consideriamo la fattorizzazione in primi di $o(G/\ker\phi)$, questo ci dice che il primo più grande che può comparire è p, e con esponente massimo 1. Del resto vale anche che $o(G/\ker\phi) = \frac{o(G)}{o(\ker\phi)} \mid o(G)$. Tornando a considerare la fattorizzazione in primi di $o(G/\ker\phi)$, questo ci dice che il più piccolo primo che può comparire è p, visto che p è il più piccolo primo che divide $o(G)$. Allora $o(G/\ker\phi) = p$ oppure $= 1$, ma quest'ultimo caso si esclude subito[4]. In conclusione

$$\frac{o(G)}{o(\ker\phi)} = p \Longrightarrow o(\ker\phi) = \frac{o(G)}{p} = o(H),$$

[4]Il caso $o(G/\ker\phi) = 1$ si esclude perchè significherebbe che $G = \ker\phi$ ossia che ogni elemento di G agisce su G/H come l'identità. Si osserva subito che questo non è vero: se $g \notin H$ allora $g \cdot H = gH \neq H$.

e quindi $\ker \phi = H$. $\square$

Come corollario riotteniamo un risultato che probabilmente avete già dimostrato per esercizio l'anno scorso con un metodo più diretto.

Corollario 2.4.1. *Sia G un gruppo di ordine pari. Ogni sottogruppo di indice 2 è normale.*

Esempio 2.4.1. Sia G un gruppo di ordine 15. Per il teorema di Cauchy esistono due elementi $x, y \in G$ che hanno ordine uno 5 e l'altro 3; indichiamo con A e B i sottogruppi generati da x e y rispettivamente. Per il Teorema 2.4.1 abbiamo che, essendo $i_G(A) = 3$, il sottogruppo $A = (x)$ è normale in G.

2.5 Esercizi

Esercizio 2.5.1. Sia $n \geq 3$. Considerare le seguenti affermazioni:

- per ogni $n \geq 3$, in A_n tutti i 3-cicli sono coniugati;
- in A_n tutti i 3-cicli sono coniugati se e solo se $n \geq 5$

Una fra le due è vera. Quale, e perché?

Esercizio 2.5.2. Sia $n \geq 3$. Dimostrare che il gruppo A_n è $n-2$ *volte transitivo* su $\{1, 2, ..., n\}$ ossia che, se si prendono da $\{1, 2, ..., n\}$ $n-2$ numeri $a_1, ..., a_{n-2}$ a due a due distinti e poi si prendono da $\{1, 2, ..., n\}$ altri $n-2$ numeri $b_1, ..., b_{n-2}$ a due a due distinti, esiste $\tau \in A_n$ tale che $\tau(a_i) = b_i$ per ogni $i = 1, 2, ..., n-2$.

Esercizio 2.5.3. Sia G un gruppo infinito e sia H un sottogruppo di G, diverso da G e con indice finito[5]. Dimostrare che esiste in G un sottogruppo normale diverso da $\{e\}$ e da G. [Far agire G su G/H.]

Esercizio 2.5.4. Sia G un gruppo finito, sia p il più piccolo numero primo che divide $|G|$, e sia H un sottogruppo normale di G di cardinalità p. Dimostrare che $H < Z(G)$. [Far agire G su H per coniugio.]

Esercizio 2.5.5. Come sapete, due elementi coniugati in un gruppo G hanno lo stesso ordine.
Il viceversa di questa affermazione è: se due elementi di G hanno lo stesso ordine allora sono coniugati.
a) Mostrare con un esempio che in generale non è vero il viceversa.
b) Trovare tutti i gruppi abeliani in cui è vero il viceversa.
c) Trovare un gruppo non abeliano in cui è vero il viceversa.

[5]Ricordiamo che questo vuol dire che l'insieme dei laterali G/H è finito.

Capitolo 3

I teoremi di Sylow e applicazioni (lezioni del 4 e 5 ottobre)

3.1 I teoremi di Sylow

Sappiamo dal teorema di Cauchy che se p è un primo che divide l'ordine di un gruppo finito G allora esiste in G un elemento x di ordine p, e dunque anche almeno un sottogruppo (il sottogruppo (x)) di ordine p.

I teoremi di Sylow offrono un risultato più profondo.

Teorema 3.1.1 (primo teorema di Sylow[1])**.** *Sia G un gruppo finito e p un primo tale che $p^b \mid o(G)$ e $p^{b+1} \nmid o(G)$ con $b \geq 1$ [2]. Allora per ogni $0 \leq a \leq b$ esiste un sottogruppo di G di ordine p^a.*

Dimostrazione. Per $a = 0$ il sottogruppo esiste ed è $\{e\}$. Sia dunque $1 \leq a \leq b$ e sia $o(G) = p^b \cdot m$ con $(m, p^b) = 1$. Consideriamo l'insieme

$$X = \{L \subseteq G \mid |L| = p^a\}.$$

La sua cardinalità è data da

$$|X| = \binom{p^b m}{p^a} = \frac{\prod_{i=0}^{p^a-1} (p^b m - i)}{\prod_{i=0}^{p^a-1} (p^a - i)}.$$

Ci chiediamo qual è la massima potenza di p che divide $|X|$. Iniziamo osservando il seguente fatto: se i è tale che $p^a - 1 \geq i \geq 1$, la massima potenza di p che divide $p^b m - i$ e $p^a - i$ è la stessa. Infatti se $p^k \mid (p^a - i)$ deve essere $k \leq a$, e dunque $p^k \mid i$; di conseguenza $p^k \mid (p^b m - i)$. Viceversa, supponiamo che $p^k \mid (p^b m - i)$; intanto,

[1] Peter Ludwig Mejdell Sylow, 1832-1918, matematico norvegese.

[2] ossia p^b è la massima potenza di p che divide $o(G)$.

poiché $i \leq p^a - 1$, deve essere $k \leq a-1$ e a questo punto si ricava che $p^k \mid (p^a - i)$. Forti di questa osservazione possiamo affermare che la massima potenza di p che divide $|X|$ è p^{b-a} poiché tutte le massime potenze di p che dividono i fattori in cui $i \geq 1$ si elidono tra numeratore e denominatore. Ricordiamoci dunque che $p^{b-a} \mid |X|$ mentre $p^{b-a+1} \nmid |X|$.
Consideriamo ora l'azione di G su X descritta qui sotto:

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, L) & \longmapsto & gL \end{array}.$$

La strategia consisterà nello studiare gli stabilizzatori degli elementi di X rispetto a questa azione: uno di loro risulterà avere cardinalità p^a e sarà dunque il gruppo che stiamo cercando. Chiamiamo $\mathcal{L}_1 = orb(L_1), \ldots, \mathcal{L}_k = orb(L_k)$ le orbite di questa azione, che, come sappiamo, danno una partizione di X, quindi $|X| = \sum_{i=1}^{k} |\mathrm{orb}(L_i)|$. Osserviamo che non può essere che $p^{b-a+1} \mid |\mathrm{orb}(L_i)|$ per ogni i, altrimenti dividerebbe anche $|X|$. Concludiamo allora che deve esistere un'orbita $\mathrm{orb}(L_j)$ tale che $p^{b-a+1} \nmid |\mathrm{orb}(L_j)|$. Sappiamo inoltre che

$$|\mathrm{orb}(L_j)| = \frac{o(G)}{o(\mathrm{Stab}(L_j))} = \frac{p^b m}{o(\mathrm{Stab}(L_j))} \Longrightarrow o(\mathrm{Stab}(L_j)) = \frac{p^b m}{|\mathrm{orb}(L_j)|}.$$

Visto che al massimo $p^{b-a} \mid |\mathrm{orb}(L_j)|$ si ha che la potenza di p che divide $o(\mathrm{Stab}(L_j))$ è divisa da $\frac{p^b}{p^{b-a}} = p^a$. Dunque $p^a \mid o(\mathrm{Stab}(L_j))$; in realtà possiamo dimostrare che $p^a = o(\mathrm{Stab}(L_j))$. Infatti, fissato $\ell \in L_j$, la mappa

$$\begin{array}{ccc} \mathrm{Stab}(L_j) & \longmapsto & L_j \\ \gamma & \longmapsto & \gamma\ell \end{array}$$

è ben definita e iniettiva (se $\gamma_1 \ell = \gamma_2 \ell$ allora $\gamma_1 = \gamma_2$). Quindi $o(\mathrm{Stab}(L_j)) \leq p^a$ e allora $o(\mathrm{Stab}(L_j)) = p^a$, ed è il sottogruppo cercato. □

Definizione 3.1.1. Sia G come nelle ipotesi del teorema di Sylow precedente. Un p-sottogruppo di G di ordine massimo, ossia di ordine p^b, si dice p-Sylow.

Adesso vogliamo mostrare che i vari p-Sylow di un gruppo G sono tutti coniugati fra loro.

Teorema 3.1.2 (secondo teorema di Sylow)**.** *Sia G come nelle ipotesi del teorema di Sylow precedente. Sia H un p-Sylow e $K < G$ di ordine p^a. Allora:*
(i) *esiste un $g \in G$ tale che $K < gHg^{-1}$;*
(ii) *se K è p–Sylow allora esiste $g \in G$ tale che $K = gHg^{-1}$.*

Dimostrazione. Si ha che $o(G/H) = m$ con m primo con p perché p^b è la massima potenza di p che divide $o(G)$. Consideriamo la seguente azione di K su G/H:

$$\begin{array}{ccc} K \times G/H & \longrightarrow & G/H \\ (k, gH) & \longmapsto & (kg)H \end{array}.$$

Siano $g_1H, \ldots, g_rH$ rappresentanti delle orbite; l'equazione delle classi ci dice che

$$o(G/H) = \sum_{i=1}^{r} |\mathrm{orb}(g_iH)| = \sum_{i=1}^{r} \frac{o(K)}{o(\mathrm{Stab}(g_iH))} = \sum_{i=1}^{r} p^{a_i},$$

poiché $o(\mathrm{Stab}(g_iH))$ è potenza di p. Se $a_i \geq 1$ per ogni $i = 1, \ldots, r$ allora $p \mid o(G/H) = m$, ma poiché sappiamo che non lo divide deve esistere un $1 \leq i \leq r$ tale che $a_i = 0$. Questo significa che esiste un'orbita costituita da un solo elemento, ossia deve esistere un i tale che $\mathrm{orb}(g_iH) = \{g_iH\}$. Questo a sua volta significa, ricordando l'azione, che per ogni $k \in K$ e per ogni $h \in H$ esiste un certo $h' \in H$ tale che $kg_ih = g_ih'$, da cui $k = g_ih'h^{-1}g_i^{-1} \in g_iHg_i^{-1}$. Dunque $K < g_iHg_i^{-1}$.
Il secondo punto è diretta conseguenza del primo, in quanto se K ha proprio p^b elementi ed è incluso gHg^{-1} in allora deve coincidere con gHg^{-1} per motivi di cardinalità. □

Introduciamo ora la definizione di normalizzatore:

Definizione 3.1.2. Dato $H < G$ diciamo *normalizzatore* di H in G l'insieme

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

È facile verificare che $N(H)$ è un sottogruppo di G (vedi Esercizio 3.3.3). Osserviamo poi altri due fatti:

- se H è normale in G allora $N(H) = G$;
- H è un sottogruppo normale di $N(H)$, ed anzi $N(H)$ è il più grande sottogruppo di G dentro il quale H è normale.

Corollario 3.1.1. *Sia G come nelle ipotesi dei teoremi di Sylow precedenti. Il numero dei p–Sylow è $n_p = \frac{o(G)}{o(N(H))}$, dove H è un p–Sylow qualunque. In particolare n_p divide l'ordine di G.*

Dimostrazione. Se H è un p–Sylow, allora gli altri sono tutti e soli i coniugati di H. Considerando l'azione di G per coniugio sull'insieme dei p-Sylow, possiamo scrivere

$$|\mathrm{orb}(H)| = n_p = \frac{o(G)}{o(\mathrm{Stab}(H))} = \frac{o(G)}{o(N(H))},$$

e abbiamo così concluso. □

Adesso siamo pronti per l'ultimo teorema di Sylow che riguarda il numero dei p–Sylow in un gruppo.

Teorema 3.1.3 (terzo teorema di Sylow)**.** *Sia G come nelle ipotesi dei teoremi di Sylow precedenti. Il numero n_p dei p-Sylow soddisfa la congruenza*

$$n_p \equiv 1 \pmod{p}.$$

Dimostrazione. Sia H un p–Sylow, facciamolo agire su G/H secondo l'azione seguente:

$$\begin{array}{ccc} H \times G/H & \longrightarrow & G/H \\ (h, gH) & \longmapsto & (hg)H \end{array}.$$

Sia $Y = \{gH \mid h \cdot (gH) = gH \quad \forall\, h \in H\}$, ossia l'insieme dei laterali che costituiscono un'orbita di un solo elemento. Siano $g_1H, \ldots, g_rH$ rappresentanti delle orbite con più di un elemento:

$$|G/H| = |Y| + \sum_{i=1}^{r} |\mathrm{orb}(g_iH)| = |Y| + \sum_{i=1}^{r} \frac{o(H)}{o(\mathrm{Stab}(g_iH))}.$$

Osserviamo che p divide ogni addendo della sommatoria in quanto ciascuno di essi è $\frac{p^b}{p^{b_i}}$ con $b_i < b$ perché i termini in cui $b = b_i$ li abbiamo isolati in $|Y|$. Quindi $|G/H| \equiv |Y| \pmod{p}$.
Ricordiamo che n_p è il numero dei coniugati di H, e, come abbiamo visto nel Corollario 3.1.1,

$$n_p = \frac{o(G)}{o(\mathrm{Stab}(H))} = \frac{o(G)}{o(N(H))}.$$

Ora affermiamo che $|Y| = \frac{o(N(H))}{o(H)}$. Infatti

$$gH \in Y \iff HgH = gH$$

per definizione di Y, dove HgH è, come la notazione fa prevedere, l'insieme i cui elementi sono tutti i prodotti hgh' al variare di h e h' in H. L'uguaglianza insiemistica $HgH = gH$ equivale, moltiplicando a sinistra per g^{-1}, alla uguaglianza $g^{-1}HgH = H$ che a sua volta, usando la proprietà associativa, può essere riscritta $\left(g^{-1}Hg\right) H = H$. Quest'ultima uguaglianza è vera se e solo se $g^{-1}Hg \subseteq H$ che equivale a dire $g^{-1} \in N(H)$. Poiché $N(H)$ è un sottogruppo, questo equivale a $g \in N(H)$. In conclusione il laterale gH appartiene a Y se e solo se $g \in N(H)$, dunque Y contiene esattamente $\frac{o(N(H))}{o(H)}$ classi laterali.

Esercizio 3.1.1. Spiegare in dettaglio perché è vera la frase "dunque Y contiene esattamente $\frac{o(N(H))}{o(H)}$ classi laterali".

Per quanto abbiamo dimostrato nella prima parte possiamo scrivere che

$$|G/H| \equiv \frac{o(N(H))}{o(H)} \pmod{p}. \qquad (*)$$

Allora, ricordando che

$$n_p = \frac{o(G)}{o(N(H))} = \frac{\frac{o(G)}{o(H)}}{\frac{o(N(H))}{o(H)}} \tag{3.1}$$

possiamo scrivere

$$n_p \frac{o(N(H))}{o(H)} = \frac{o(G)}{o(H)}$$

da cui, passando modulo p ed usando l'equazione $(*)$ si ottiene

$$n_p \frac{o(G)}{o(H)} \equiv \frac{o(G)}{o(H)} \pmod{p}$$

Visto che $\frac{o(G)}{o(H)}$ non è congruo a 0 modulo p (dato che H è un p-Sylow), la congruenza precedente equivale a

$$n_p \equiv 1 \pmod{p},$$

e ciò conclude. □

Esempio 3.1.1. Studiamo quali sono i 2-Sylow in S_4. Sono sottogruppi di cardinalità 8 e, per il secondo teorema di Sylow, la loro unione deve coincidere con l'insieme di tutti gli elementi di S_4 il cui ordine divide 8. Come sappiamo si tratta degli elementi del sottogruppo di Klein (che sono 4), degli elementi di ordine 4 (i 4-cicli, che sono 6) e le trasposizioni (che sono 6).

Per il Corollario 3.1.1 e per il terzo teorema di Sylow sappiamo che n_2, il numero dei 2-Sylow, soddisfa le seguenti condizioni:

$$n_2 \equiv 1 \pmod{2} \qquad \text{e} \qquad n_2 \mid 24$$

che lasciano queste due sole possibilità: $n_2 = 1$ oppure $n_2 = 3$.

Se ci fosse un solo 2-Sylow, visto che contiene 8 elementi, non riuscirebbe a contenere tutti i 16 elementi citati sopra (quelli il cui ordine divide 8).

Si deduce quindi che $n_2 = 3$ e i tre 2-Sylow sono esattamente i gruppi H_1, H_2, H_3 descritti nel Capitolo 8, pagina 85 e seguenti, delle dispense del Corso di Aritmetica.

L'azione di S_4 per coniugio sull'insieme dei 2-Sylow fornisce dunque, per il Teorema 2.2.1, un omomorfismo surgettivo

$$\Phi : S_4 \to S_3$$

che coincide con l'omomorfismo descritto nelle dispense di Aritmetica (il nostro nuovo punto di vista ci permettere di sapere subito che c'è un omomorfismo, la surgettività va verificata esattamente come nelle dispense di Aritmetica).

3.2 Studio delle rotazioni di un icosaedro

Ricordiamo una definizione che ci sarà utile:

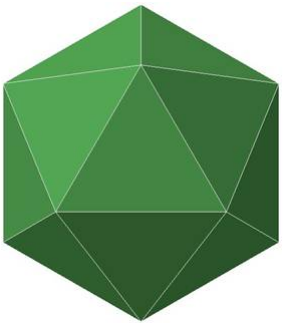
Definizione 3.2.1. Un gruppo $G \neq \{e\}$ si dice *semplice* se non ha sottogruppi normali non banali.

Dunque un gruppo è semplice se è diverso da $\{e\}$ e gli unici suoi sottogruppi normali sono $\{e\}$ e G stesso.

Esempio 3.2.1. I gruppi $\mathbb{Z}_p$, con p primo, sono semplici. Vederemo fra poco un esempio di gruppo non abeliano semplice.

Osserviamo che se abbiamo un omomorfismo $\phi : G \to K$ e G è semplice allora o ϕ immerge G in K o ϕ è l'omomorfismo nullo: i due casi si hanno rispettivamente quando $\ker \phi = \{e\}$ o $\ker \phi = G$.

Vogliamo studiare il gruppo $G(P_{20})$ delle rotazioni che mandano un icosaedro in sè. Proponiamo questo esempio perché descrive una interessante di azione di gruppo; inoltre ci darà l'opportunità di illustrare il secondo teorema di Sylow e di cominciare a scoprire una importante famiglia di gruppi semplici.



Una rotazione di un icosaedro è completamente determinata se sappiamo qual è l'immagine di un vertice e di uno dei lati adiacenti al vertice considerato. Al massimo abbiamo dunque $12 \cdot 5 = 60$ rotazioni dell'icosaedro: infatti ci sono 12 modi per scegliere l'immagine del vertice e 5 modi per determinare l'immagine del lato adiacente. Si esibiscono facilmente (vedi sotto, quando elenchiamo alcuni sottogruppi) 60 distinti elementi di $G(P_{20})$. Dunque $|G(P_{20})| = 60$.

(1) Alcuni sottogruppi. Ci sono sicuramente 15 sottogruppi di ordine 2, derivati della rotazioni di 180 gradi attorno ad assi passanti per spigoli opposti; ci sono poi 10 sottogruppi di ordine 3, dati dalle rotazioni rispetto ad assi passanti per i centri di facce opposte; infine abbiamo anche 6 sottogruppi di ordine 5, dati dalle rotazioni rispetto ad assi passanti per coppie di vertici opposti. Si vede facilmente che gli elementi di ordine 2 sono tutti coniugati tra loro (sia $w \in G(P_{20})$ una

rotazione che manda uno spigolo L_1 nello spigolo L_2, e sia r_1 (risp. r_2) la rotazione di 180 gradi rispetto all'asse passante dallo spigolo L_1 e dal suo opposto: allora vale $wr_1w^{-1} = r_2$). Analogamente, si mostra che in $G(P_{20})$ tutti gli elementi di ordine 3 sono coniugati fra loro. Invece gli elementi di ordine 5 si dividono in due classi di coniugio di 12 elementi ciascuna.[3] Osserviamo che questo nostro elenco di sottogruppi ci ha "fatto conoscere" 15 elementi di ordine 2, $10 \cdot 2 = 20$ elementi di ordine 3, $6 \cdot 4 = 24$ elementi di ordine 5. Considerando anche l'identità abbiamo dunque esibito 60 elementi, dunque tutti gli elementi del gruppo.

(2) Semplicità. Sia N un sottogruppo normale di $G(P_{20})$. Visto che N è chiuso per coniugio, se contiene un elemento x allora deve contenere tutti gli elementi della classe di coniugio a cui appartiene x. Le classi di coniugio le abbiamo descritte nel punto precedente. Quindi

$$o(N) = 1 + 15a + 20b + 12c + 12d,$$

con $a, b, c, d \in \{0, 1\}$. Dal momento che $o(N) \mid 60$ si ha che $a = b = c = d = 0$ oppure $a = b = c = d = 1$ e quindi o $N = \{e\}$ o $N = G(P_{20})$.

(3) Numero dei 2–Sylow. I 2-Sylow hanno 4 elementi, dunque ciascun 2-Sylow contiene l'identità e tre degli elementi di ordine 2. In particolare si osserva che un sottogruppo di ordine 4 si può individuare così: si prende la rotazione di 180 gradi attorno ad un asse l passante per due spigoli opposti e si osserva che ci sono altre due coppie di spigoli opposti i cui due assi sono ortogonali fra loro e giacciono su un piano ortogonale a l. Si verifica subito che le tre rotazioni individuate commutano fra loro e formano un sottogruppo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Sappiamo, dal secondo teorema di Sylow, che i 2-Sylow sono tutti coniugati fra loro, quindi sono tutti isomorfi a $\mathbb{Z}_2 \times \mathbb{Z}_2$: coniugare per delle rotazioni mantiene l'ortogonalità dunque ognuno di questi 2-Sylow contiene tre rotazioni di ordine 2 individuate da assi passanti per spigoli opposti e ortogonali fra loro. Le 15 rotazioni di ordine 2 vengono così suddivise a tre a tre e i 2-Sylow sono cinque.

(4) $G(P_{20})$ è isomorfo a $\mathcal{A}_5$. Consideriamo $G(P_{20})$ che agisce per coniugio sui 2–Sylow; come sappiamo, questa azione induce un omomorfismo

$$\phi : G(P_{20}) \longrightarrow \mathcal{S}_5,$$

ma $G(P_{20})$ è semplice e dunque $\ker \phi = \{id\}$ oppure $\ker \phi = G(P_{20})$. La seconda di queste due possibilità non può darsi perché vorrebbe dire che $G(P_{20})$ agisce in maniera banale sui 2–Sylow, lasciandoli tutti fissi. Invece sappiamo, sempre per il secondo teorema di Sylow, che sotto l'azione di $G(P_{20})$ i 2-Sylow formano un'unica

[3] In una classe di coniugio troviamo tutte le rotazioni di 72 gradi e di 288 gradi attorno ad un asse passante per una coppia di vertici opposti. Nell'altra classe troviamo tutte le rotazioni di 144 gradi e di 216 gradi.

orbita. Quindi ϕ è iniettivo e la sua immagine è un sottogruppo di S_5 isomorfo a $G(P_{20})$.

Importante: d'ora in poi identificheremo $G(P_{20})$ con la sua immagine tramite ϕ, ossia "leggeremo" direttamente $G(P_{20})$ come sottogruppo di S_5. Capiterà spesso in questo corso di identificare, per semplicità di notazione, un gruppo con una sua immagine isomorfa dentro un altro gruppo.

Ora, $G(P_{20})$ ha 60 elementi e dunque ha indice 2 in S_5: questo implica, come sappiamo, che $G(P_{20})$ è normale in S_5. Anche A_5 è normale in S_5, dunque $A_5 \cap G(P_{20})$ è normale in S_5. A maggior ragione $A_5 \cap G(P_{20})$ è normale in $G(P_{20})$. Ma $G(P_{20})$ è semplice, dunque ci sono solo due possibilità: $A_5 \cap G(P_{20}) = G(P_{20})$ e $A_5 \cap G(P_{20}) = \{e\}$.

La prima implica che $A_5 = G(P_{20})$ come volevamo dimostrare. Resta da escludere che possa verificarsi la seconda: se fosse $A_5 \cap G(P_{20}) = \{e\}$ allora $G(P_{20})$ sarebbe composto da una permutazione pari (l'identità) e da 59 permutazioni dispari. Ma per l'Esercizio 2.3.8 sappiamo che un sottogruppo di S_n o è tutto composto da permutazioni pari o ha metà permutazioni pari e metà dispari. Dunque il caso $A_5 \cap G(P_{20}) = \{e\}$ va scartato.

3.3 Esercizi

Nell'esempio che abbiamo appena studiato sono comparse alcune proprietà interessanti dei gruppi simmetrici e alterni e alcuni proprietà generali dei sottogruppi normali. Per sottolinearne l'importanza le riproponiamo sotto forma di esercizio (e aggiungiamo anche qualche altro esercizio):

Esercizio 3.3.1. Dimostrare che, se $H \triangleleft G$ e $h \in H$, allora tutta la classe di coniugio di h in G è inclusa in H.

Esercizio 3.3.2. Dimostrare che, se $H \triangleleft G$ e $K \triangleleft G$, allora $H \cap K \triangleleft G$.

Esercizio 3.3.3. Dimostrare che, dato un gruppo G e un sottogruppo H di G, il normalizzatore $N(H)$ è un sottogruppo di G.

Esercizio 3.3.4. Mostrare un sottogruppo H in S_3 tale che $N(H)$ non è un sottogruppo normale di S_3.

Esercizio 3.3.5. Mostrare un sottogruppo H in S_4 tale che $N(H)$ non è un sottogruppo normale di S_4.

Esercizio 3.3.6. Dimostrare che gli unici gruppi abeliani semplici sono i gruppi $\mathbb{Z}_p$ con p primo.

Esercizio 3.3.7. Quanti sono i 2-Sylow di A_4?

Esercizio 3.3.8. Descrivere esplicitamente i i 2-Sylow di A_5.

Esercizio 3.3.9. Dimostrare che A_5 è semplice in maniera indipendente dalla costruzione geometrica appena proposta. [Contare le cardinalità delle classi di coniugio e concludere che è impossibile, per ragioni "aritmetiche", che l'unione di alcune di esse formi un sottogruppo proprio.]

Osservazione 3.3.1. L'aver scoperto che il gruppo A_5 è semplice è il primo passo verso un teorema più generale di cui per ora diamo solo notizia: per ogni $n \geq 5$ il gruppo A_n è semplice.

Esercizio 3.3.10. Dimostrare che l'unico sottogruppo normale di S_5 diverso da $\{e\}$ e da S_5 è A_5.

Esercizio 3.3.11. Dimostrare che un gruppo di ordine 42 non è semplice.

Esercizio 3.3.12. Dimostrare che un gruppo di ordine 84 non è semplice.

Esercizio 3.3.13. Dimostrare che un gruppo di ordine 56 non è semplice.

Per chi è interessato alle rotazioni dei solidi platonici proponiamo i seguenti esercizi. Visto che, per ragioni di "dualità" il gruppo $G(P_{12})$ delle rotazioni del dodecaedro è isomorfo a $G(P_{20})$ e il gruppo $G(P_8)$ delle rotazioni dell'ottaedro è isomorfo al gruppo $G(P_6)$ delle rotazioni del cubo, basta studiare i due casi seguenti:

Esercizio 3.3.14. Dimostrare che il gruppo $G(P_6)$ delle rotazioni del cubo è isomorfo a S_4. [Per avere una immersione di $G(P_6)$ in S_4 si potrebbe per esempio studiare come $G(P_6)$ agisce sull'insieme delle quattro "grandi diagonali" del cubo.]

Esercizio 3.3.15. Dimostrare che il gruppo $G(P_4)$ delle rotazioni del tetraedro regolare è isomorfo a A_4.

Capitolo 4

Prodotti semidiretti di gruppi (lezione del 12 ottobre)

4.1 Sul prodotto di due sottogruppi di un gruppo

In questo paragrafo presentiamo alcuni semplici risultati sui prodotti di sottogruppi, che saranno di importanza cruciale anche nelle prossime lezioni. Dati due sottogruppi M e N di un gruppo G in generale l'insieme

$$MN = \{mn \mid m \in M, n \in N\}$$

non è un sottogruppo. Se uno dei due sottogruppi è normale, possiamo invece affermare che:

Lemma 4.1.1. *Sia G un gruppo, $M \lhd G$ e $N < G$. Vale $MN < G$.*

Dimostrazione. Siano $m, m_1 \in M$ e $n, n_1 \in N$: dobbiamo dimostrare che $(mn)(m_1n_1) \in MN$ e $(mn)^{-1} \in MN$.
Possiamo scrivere $(mn)(m_1n_1) = m\left(nm_1n^{-1}\right)nn_1$ e osservare che $m \in M$ e anche $nm_1n^{-1} \in M$ per la normalità di M. Inoltre $nn_1 \in N$ visto che N è un sottogruppo. Quindi il prodotto indicato appartiene a MN. Per l'inverso il ragionamento è analogo in quanto si scrive:

$$(mn)^{-1} = n^{-1}m^{-1} = n^{-1}m^{-1}nn^{-1}$$

e si osserva che $n^{-1}m^{-1}n \in M$ per la normalità di M e $n^{-1} \in N$ dato che N è un sottogruppo. □

Il seguente lemma si occupa di un caso particolare:

Lemma 4.1.2. *Sia G un gruppo, siano M e N sottogruppi entrambi normali e tali che $M \cap N = \{e\}$. Allora $mn = nm$ per ogni $n \in N$ e $m \in M$.*

Dimostrazione. Dati $m \in M$ e $n \in N$, dal momento che $mNm^{-1} = N$ si ha $mn = n_1 m$ per un certo $n_1 \in N$, e dal momento che $n_1 M n_1^{-1} = M$ si ha che $n_1 m = m_1 n_1$ per un certo $m_1 \in M$. Ma allora $mn = m_1 n_1$, da cui possiamo scrivere $m_1^{-1} m = n_1 n^{-1}$. Dal membro di destra si capisce che questo elemento sta in M e dal membro di sinistra si capisce che sta in N; ma l'intersezione $M \cap N$ è $\{e\}$ e quindi $m = m_1$ e $n = n_1$. □

In altre parole, il lemma precedente dimostra che se M e N sono entrambi sottogruppi normali e tali che $M \cap N = \{e\}$, il sottogruppo MN di G è isomorfo al gruppo $M \times N$, dove come sapete la struttura di gruppo sul prodotto cartesiano è data dal prodotto $(m_1, n_1)(m_2, n_2) = (m_1 m_2, n_1 n_2)$.

In alcuni libri si trova la seguente terminologia: MN è un *prodotto interno* dei gruppi M e N, perché stiamo moltiplicando M ed N vedendoli all'interno di G, mentre $M \times N$ è il *prodotto esterno* di M e N.

Nel caso delle ipotesi del Lemma 4.1.2, risulta dunque che il prodotto interno MN e quello esterno $M \times N$ sono isomorfi. In generale però non è vero che il prodotto interno di due sottogruppi è isomorfo al loro prodotto esterno. Approfondiremo la questione nei prossimi paragrafi.

Il seguente esempio ci mostra una applicazione dei teoremi di Sylow e dei lemmi precedenti.

Esempio 4.1.1. Vogliamo mostrare che sostanzialmente (ossia a meno di isomorfismo) esistono solo quattro gruppi di ordine $17^2 \cdot 19^2$. Sia G un gruppo tale che $|G| = 17^2 \cdot 19^2$.
Chiediamoci quanti sono i 17–Sylow. Sappiamo che $n_{17} \equiv 1 \pmod{17}$ e che deve dividere l'ordine del gruppo, ossia $n_{17} \mid 19^2$: da queste due informazioni ricaviamo immediatamente che $n_{17} = 1$. Quindi c'è un solo 17–Sylow, che chiameremo N_{17}: deve essere normale in quanto unico elemento della sua orbita per coniugio. Un ragionamento del tutto analogo porta a concludere che esiste anche un solo 19–Sylow, che chiameremo N_{19}, e che pertanto è normale.
Osserviamo che $N_{17} \cap N_{19} = \{e\}$ in quanto se un elemento stesse nell'intersezione dovrebbe avere ordine che divide contemporaneamente 17^2 e 19^2, il che è possibile se e solo se l'ordine dell'elemento in questione è 1. Per il Lemma 4.1.2, N_{17} e N_{19} commutano, ossia $mn = nm$ per ogni $m \in N_{17}$ e $n \in N_{19}$, e sappiamo anche, per il Lemma 4.1.1, che $N_{17}N_{19}$ è un sottogruppo di G. Dal momento che $N_{17}N_{19}$ ha tanti elementi quanti G (riguardate l'Esercizio 8.14 delle dispense di Aritmetica!) possiamo concludere $G = N_{17}N_{19}$. Per il Corollario 4.1.1 sappiamo che i gruppi di ordine p^2 con p primo sono abeliani, dunque N_{17} e N_{19} sono abeliani e si conclude facilmente che il gruppo G è abeliano. Inoltre, $N_{17} \cong \mathbb{Z}_{17^2}$ o $N_{17} \cong \mathbb{Z}_{17} \times \mathbb{Z}_{17}$, e $N_{19} \cong \mathbb{Z}_{19^2}$ o $N_{19} \cong \mathbb{Z}_{19} \times \mathbb{Z}_{19}$. In definitiva per G abbiamo le seguenti possibilità: $\mathbb{Z}_{17^2} \times \mathbb{Z}_{19^2}$ (che è isomorfo a $\mathbb{Z}_{17^2 19^2}$), $\mathbb{Z}_{17} \times \mathbb{Z}_{17} \times \mathbb{Z}_{19^2}$, $\mathbb{Z}_{17^2} \times \mathbb{Z}_{19} \times \mathbb{Z}_{19}$ oppure $\mathbb{Z}_{17} \times \mathbb{Z}_{17} \times \mathbb{Z}_{19} \times \mathbb{Z}_{19}$.

4.2 Prodotto semidiretto

La nozione di prodotto semidiretto generalizza quella di prodotto diretto.

Ripartiamo dal Lemma 4.1.1: se $M \lhd G$ e $N < G$ allora $MN < G$. In particolare, per quel che riguarda il prodotto fra due elementi m_1n_1 e m_2n_2 abbiamo osservato nella dimostrazione del lemma che

$$(m_1n_1)(m_2n_2) = m_1n_1m_2\left(n_1^{-1}n_1\right)n_2 = m_1\left(n_1m_2n_1^{-1}\right)n_1n_2 \tag{4.1}$$

Supponiamo ora $M \cap N = \{e\}$ e $G = MN$: dal punto di vista insiemistico c'è una corrispondenza bigettiva naturale fra MN e $M \times N$, quella che manda mn in (m, n), ma in generale non è vero che come gruppi $MN \cong M \times N$. Come vedremo, però, è possibile definire una particolare moltiplicazione sull'insieme $M \times N$ e ottenere un gruppo isomorfo a MN.

Definizione 4.2.1. Siano H e K gruppi e sia $\tau : K \to \mathrm{Aut}(H)$ un omomorfismo. Si definisce *prodotto semidiretto* di H e K secondo τ, e si indica con $H \rtimes_\tau K$, il prodotto cartesiano $H \times K$ dotato dell'operazione seguente:

$$(h, k)\left(\overline{h}, \overline{k}\right) = \left(h\ \tau(k)\left(\overline{h}\right), k\overline{k}\right).$$

Osserviamo che $\tau(k)\left(\overline{h}\right)$ è un elemento di H, infatti $\tau(k)$ è un automorfismo di H e viene applicato ad $\overline{h} \in H$.

Osservazione 4.2.1. Lasciamo come semplice verifica i seguenti fatti.
(1) $H \rtimes_\tau K$ è un gruppo con l'operazione della definizione, e l'elemento neutro è (e_H, e_K), mentre l'inverso di (h, k) è $\left(\tau(k^{-1})\left(h^{-1}\right), k^{-1}\right)$;
(2) $H' = \{(h, e_K) \mid h \in H\} \lhd H \rtimes_\tau K$ e $H' \cong H$;
(3) $K' = \{(e_H, k) \mid k \in K\} < H \rtimes_\tau K$ ed inoltre $(H \rtimes_\tau K)/H' \cong K' \cong K$.

Osservazione 4.2.2. Se τ è l'omomorfismo banale, ossia se $\tau(k) = id$ per ogni $k \in K$, allora l'operazione di prodotto semidiretto coincide col prodotto componente per componente. In tal caso $H \rtimes_\tau K = H \times K$.

Teorema 4.2.1. *Sia G un gruppo, e siano $H \lhd G$ e $K < G$ due suoi sottogruppi tali che $H \cap K = \{e\}$ e $G = HK$. Allora*

$$G \cong H \rtimes_{c_G} K,$$

dove $c_G : K \to \mathrm{Aut}(H)$ è l'omomorfismo che associa ad ogni $k \in K$ l'automorfismo dato dal coniugio (in G) per k, ossia l'automorfismo $H \to H$ definito da $h \to khk^{-1}$.

Dimostrazione. La mappa

$$\begin{array}{rccc} \phi: & H \rtimes_{c_G} K & \longrightarrow & G \\ & (h,k) & \longmapsto & hk \end{array}$$

è un isomorfismo. Infatti è un omomorfismo per la regola (4.1) ricordata all'inizio della lezione; la condizione $H \cap K = \{e\}$ garantisce l'iniettività, la verifica della surgettività è immediata. □

Esempio 4.2.1. Consideriamo $\mathcal{S}_n$, e i sottogruppi $\mathcal{A}_n \lhd \mathcal{S}_n$ e $\langle (1\,2) \rangle < \mathcal{S}_n$.[1] I due sottogruppi si intersecano solo nella permutazione identica, in quanto il secondo è generato da una permutazione dispari; inoltre, per questioni di cardinalità, deve essere $\mathcal{S}_n = \mathcal{A}_n \langle (1\,2) \rangle$. Ma allora, per il teorema precedente

$$\mathcal{S}_n \cong \mathcal{A}_n \rtimes_{c_{S_n}} \langle (1\,2) \rangle .$$

Esempio 4.2.2. Sia $L = \{ f_{a,b} : \mathbb{R} \to \mathbb{R} \mid f_{a,b}(x) = ax + b,\ a \neq 0,\ b \in \mathbb{R} \}$, con l'operazione data dalla composizione, il gruppo delle affinità su $\mathbb{R}$, e siano N ed M i gruppi delle omotetie e delle traslazioni su $\mathbb{R}$, ossia

$$N = \{ f_{a,b} \in L \mid b = 0 \} \cong \mathbb{R}^* \qquad \text{e} \qquad M = \{ f_{a,b} \in L \mid a = 1 \} \cong \mathbb{R}.$$

Non è difficile vedere che $M \lhd L$, in quanto $f_{a,b}^{-1} = f_{1/a,-b/a}$ e si verifica che $f_{a,b} f_{1,b'} f_{a,b}^{-1} = f_{1,ab'} \in M$. L'intersezione $M \cap N$ contiene un solo elemento, l'affinità $f_{1,0}$, elemento neutro di L; $L = MN$ dato che $f_{a,b} f_{1,b'} = f_{a,ab'+b}$ e ogni affinità può essere espressa nella forma $f_{a,ab'+b}$ scegliendo opportunamente a, b', b. Ma allora

$$L \cong M \rtimes_{c_L} N.$$

Esempio 4.2.3. Consideriamo l'omomorfismo $\tau : \mathbb{Z}_2 \to Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$ dove $\tau([1]$ è l'automorfismo che scambia le coordinate di ogni elemento di $\mathbb{Z}_3 \times \mathbb{Z}_3$. Costruiamo il prodotto semidiretto

$$G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\tau \mathbb{Z}_2.$$

Osserviamo che il sottogruppo $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\tau \{[0]\}$ è normale in G, e che $(\mathbb{Z}_3 \times \{[0]\}) \rtimes_\tau \{[0]\}$ è normale in $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\tau \{[0]\}$, ma $(\mathbb{Z}_3 \times \{[0]\}) \rtimes_\tau \{[0]\}$ non è normale in G (basta calcolare il coniugio $(([0],[0]),[1])$ $(([1],[0]),[0])$ $(([0],[0]),[1])$...). [2]

[1] Talvolta, quando sarà conveniente, indicheremo con $\langle a, b, .. \rangle$ il sottogruppo di un gruppo G generato dagli elementi $a, b, ...$, invece che con $(a, b, ..)$. Nel caso del gruppo simmetrico, dove già gli elementi sono indicati con parentesi tonde, sembra più opportuna la notazione $\langle\ \rangle$.

[2] Questo esempio illustra una tecnica generale di "costruzione" di gruppi. Dato un gruppo K, consideriamo il prodotto diretto $K \times K \times \cdots \times K$ di n copie di K e facciamo agire S_n su $K \times K \times \cdots \times K$ in modo ovvio permutando le coordinate (sia $\tau : S_n \to Aut(K \times K \times \cdots \times K)$ il corrispondente omomorfismo). Allora si può costruire il seguente gruppo, che si chiama *wreath product*, "prodotto intrecciato" di K e S_n:

$$G = (K \times K \times \cdots \times K) \rtimes_\tau S_n.$$

Adesso un punto molto importante. Supponiamo di avere H e K gruppi. Considerato un omomorfismo $\tau : K \to \mathrm{Aut}(H)$ possiamo costruire il prodotto semidiretto $H \rtimes_\tau K$ come detto prima. In generale esistono un certo numero di omomorfismi $K \to \mathrm{Aut}(H)$ e quindi possiamo chiederci come variano le strutture di prodotto semidiretto al variare di τ. Per esempio vorremmo chiederci: se $\tau_1 \neq \tau_2$ allora è vero che $H \rtimes_{\tau_1} K \ncong H \rtimes_{\tau_2} K$? La risposta a questa domanda è no; è possibile che omomorfismi diversi $K \to \mathrm{Aut}(H)$ diano luogo a prodotti semidiretti isomorfi. Il seguente criterio è molto utile:

Proposizione 4.2.1. *Dati due gruppi H e K, siano $\phi, \psi : K \to \mathrm{Aut}(H)$ due omomorfismi. Se esistono $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$ tali che*

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

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

Dimostrazione. Consideriamo la seguente mappa:

$$\begin{array}{rccc} \Xi : & H \rtimes_\phi K & \longrightarrow & H \rtimes_\psi K \\ & (h,k) & \longmapsto & (\alpha(h), \beta(k)) \end{array},$$

e mostriamo che si tratta di un isomorfismo. Intanto mostriamo che Ξ è un omomorfismo:

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

L'iniettività segue da:

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

dove l'ultima equivalenza vale per l'iniettività di α e β. Analogamente, la surgettività è data dal fatto che α e β sono automorfismi, e quindi anch'essi surgettivi. □

Esempio 4.2.4. Classificare i gruppi di ordine 6.
Sia G un gruppo di ordine 6. Ci sono un sottogruppo di ordine 2 e uno di ordine 3, chiamiamoli $N_2 (\cong \mathbb{Z}_2)$ e $N_3 (\cong \mathbb{Z}_3)$ (non occorre invocare il teorema di Sylow per affermare ciò, basta per esempio il teorema di Cauchy) . Inoltre N_3 ha indice 2 in G e quindi è normale: $N_3 \lhd G$. Per questioni di ordine degli elementi i due sottogruppi N_2 e N_3 hanno intersezione uguale a $\{e\}$ e quindi per motivi di cardinalità $G = N_3 N_2$. Ma allora possiamo affermare

$$G \cong N_3 \rtimes_{c_G} N_2.$$

Per capire quanti prodotti semidiretti del tipo $\mathbb{Z}_3 \rtimes_\tau \mathbb{Z}_2$ esistono a meno di isomorfismo dobbiamo per prima cosa studiare gli omomorfismi $\tau : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$. Ricordiamo che $\mathrm{Aut}(Z_3) \cong \mathbb{Z}_2$: in definitiva stiamo cercando gli omomorfismi $\tau : \mathbb{Z}_2 \to \mathbb{Z}_2$, che sono solo due.
Si osserva che quindi al massimo esistono due distinti prodotti semidiretti $\mathbb{Z}_3 \rtimes_\tau \mathbb{Z}_2$ e siccome conosciamo due gruppi, $\mathbb{Z}_6$ e $\mathcal{S}_3$, di ordine 6 e non isomorfi fra loro, possiamo concludere che in effetti le distinte strutture di prodotto semidiretto sono proprio due ($\mathbb{Z}_6$ corrisponde al caso in cui τ è l'omomorfismo banale e dunque il prodotto è diretto).

L'esempio precedente si generalizza nel seguente modo:

Proposizione 4.2.2. *Consideriamo due numeri primi p e q, con $p > q$. Se q non divide $p-1$ esiste, a meno di isomorfismo, un solo gruppo di ordine pq, ossia $\mathbb{Z}_{pq}$. Se invece $q|p-1$ allora esistono a meno di isomorfismo due gruppi di ordine pq: uno è $\mathbb{Z}_{pq}$, l'altro non è abeliano.*

Dimostrazione. Sia G di ordine pq. Dal teorema di Cauchy (non occorre in questo caso invocare i teoremi di Sylow) sappiamo che esistono due sottogruppi di ordine p e q, chiamiamoli N_p e N_q, isomorfi rispettivamente a $\mathbb{Z}_p$ e a $\mathbb{Z}_q$. L'indice di N_p è q, il più piccolo primo che divide $o(G)$, e quindi, per il Teorema 2.4.1, N_p è normale in G. Essendo p e q due numeri primi distinti, l'intersezione fra N_p e N_q contiene, per ragioni di ordine degli elementi, solo l'elemento neutro del gruppo. Inoltre vale $N_pN_q = G$ per questioni di cardinalità. Possiamo quindi concludere che

$$G \cong N_p \rtimes_{c_G} N_q.$$

Adesso dobbiamo studiare gli omomorfismi $\tau : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ e a quali strutture di prodotto semidiretto danno luogo.

- Se $q \nmid (p-1)$ allora l'unico omomorfismo τ che possiamo costruire è quello che manda ogni elemento di $\mathbb{Z}_q$ in $[0]$ in $\mathbb{Z}_{p-1}$: infatti l'immagine di un generatore di $\mathbb{Z}_q$ deve avere ordine che divide q, dunque uguale a 1 o a q, ma in $\mathbb{Z}_{p-1}$, se $q \nmid (p-1)$, non ci sono elementi di ordine q. Allora si conclude che siamo nel caso del prodotto diretto

  $$G = \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$$

  (ricordiamo che $([1]_q, [1]_p)$ ha ordine pq).

- Se $q \mid (p-1)$ allora abbiamo diverse possibilità. Consideriamo un omomorfismo $\mathbb{Z}_q \to \mathbb{Z}_{p-1}$ (ricordiamo che $\mathbb{Z}_{p-1} \cong \mathrm{Aut}(\mathbb{Z}_p)$); questo è completamente determinato dall'immagine di $[1]_q$, che può avere ordine 1 o q: se ha ordine

1 siamo nuovamente nel caso dell'omomorfismo banale, e dunque del prodotto diretto, già trattato; se ha ordine q abbiamo la possibilità di scegliere l'immagine come

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

che sono tutti e soli gli elementi di ordine q in $\mathbb{Z}_{p-1}$. In definitiva abbiamo $q-1$ omomorfismi non banali, che chiameremo $\phi_1, \ldots, \phi_{q-1}$. Vogliamo mostrare che tutti questi omomorfismi inducono la stessa struttura sul prodotto semidiretto.
Consideriamo ϕ_1 e ϕ_j con $1 \neq j$: useremo la Proposizione 4.2.1 per mostrare che inducono prodotti semidiretti isomorfi. Questo dimostra in particolare che tutte le ϕ_i inducono prodotti semidiretti isomorfi. Consideriamo $\alpha = id \in \mathrm{Aut}(\mathbb{Z}_p)$ e, per ogni $j = 1, ..., q-1$, $\beta_j \in \mathrm{Aut}(\mathbb{Z}_q)$ tale che $\beta_j([1]_q) = [j]_q$. Visto che α è l'identità, dobbiamo verificare che $\phi_j([1]_q)$ e $\phi_1(\beta_j([1]_q))$ (che in base alla identificazione $\mathbb{Z}_{p-1} \cong \mathrm{Aut}(\mathbb{Z}_p)$ sono elementi di $\mathbb{Z}_{p-1}$) coincidono[3]. Infatti

$$\phi_j([1]_q) = j\left[\frac{p-1}{q}\right]_{p-1} = \phi_1\left([j]_q\right) = \phi_1(\beta_j([1]_q))$$

Esistono dunque, a meno di isomorfismo, al più due gruppi di ordine pq: $\mathbb{Z}_p \times \mathbb{Z}_q$ e $\mathbb{Z}_p \rtimes_\tau \mathbb{Z}_q$ con $\tau = \phi_i$ scelto un qualsiasi $i = 1, \ldots, q-1$. Mostriamo adesso che sono diversi facendo vedere che il secondo non è abeliano. Prendiamo $a \in \mathbb{Z}_p$ e $b \in \mathbb{Z}_q$, allora (usando come di consueto la notazione additiva per i gruppi $\mathbb{Z}_p$ e $\mathbb{Z}_q$ e scrivendo per brevità i loro elementi senza parentesi quadre [ ]) vale:

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

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

Siccome τ non è banale allora esisterà un $b \in \mathbb{Z}_q$ tale che $\tau(b) \neq id$ e quindi esiste un a tale che $\tau(b)(a) \neq a$ [4]. Scelti questi a e b possiamo concludere che$(a,b)(0,b) \neq (0,b)(a,b)$ e dunque $\mathbb{Z}_p \rtimes_\tau \mathbb{Z}_q$ non è abeliano.

□

[3] Andrebbe verificato che $\phi_j([r]_q) = \phi_1(\beta_j([r]_q))\ \forall\ [r]_q$ ma basta la verifica su un generatore, visto che ϕ_j e $\phi_1 \circ \beta_j$ sono omomorfismi da $\mathbb{Z}_q$ a $\mathbb{Z}_{p-1}$.

[4] Gli omomorfismi ϕ_i andavano da $\mathbb{Z}_q$ a $\mathbb{Z}_{p-1} \cong \mathrm{Aut}(\mathbb{Z}_p)$. Abbiamo detto che $\tau = \phi_i$ quindi, per essere rigorosi, $\tau(b)$ è un elemento di $\mathbb{Z}_{p-1}$. Quando abbiamo scritto $\tau(b) \neq id$ e $\tau(b)(a)$ abbiamo invece interpretato $\tau(b)$ come automorfismo di $\mathbb{Z}_p$.

Esempio 4.2.5. Le considerazioni dell'esempio precedente mostrano che, preso un primo dispari p, ci sono solo due gruppi di ordine $2p$. Uno è $\mathbb{Z}_{2p}$ e l'altro? Sappiamo che il gruppo diedrale D_p è un gruppo di ordine $2p$ non abeliano. Si tratta dunque proprio del gruppo che stiamo cercando.

4.3 Esercizi

Esercizio 4.3.1. Trovare due sottogruppi M e N di un gruppo G tali che l'insieme

$$MN = \{mn \mid m \in M, n \in N\}$$

non sia un sottogruppo di G.

Esercizio 4.3.2. Dimostrare che un gruppo G di ordine 108 ha un sottogruppo normale di ordine 9 o 27.

Esercizio 4.3.3. Sia $\tau : \mathbb{Z}_2 \to Aut(S_3)$ un omomorfismo non banale. Dimostrare che $S_3 \times \mathbb{Z}_2$ è isomorfo a $S_3 \rtimes_\tau \mathbb{Z}_2$. [Avete già osservato questo a esercitazioni quando avete classificato i gruppi di ordine 12; l'esercizio ha lo scopo di farvi tenere ben presente questo esempio.]

Esercizio 4.3.4. Descrivere tutti i sottogruppi di ordine 6 di S_4. Ci sono sottogruppi di ordine 6 in A_4?

Esercizio 4.3.5. Descrivere (se esistono) tutti i sottogruppi di ordine 8 di S_5.

Esercizio 4.3.6. Descrivere (se esistono) tutti i sottogruppi di ordine 10 di S_5.

Esercizio 4.3.7. Descrivere (se esistono) tutti i sottogruppi di ordine 12 di S_5.

Esercizio 4.3.8. Descrivere (se esistono) tutti i sottogruppi di ordine 15 di S_5.

Esercizio 4.3.9. Descrivere (se esistono) tutti i sottogruppi di ordine 20 di S_5.

Esercizio 4.3.10. Descrivere (se esistono) tutti i sottogruppi di ordine 24 di S_5.

Esercizio 4.3.11. Dimostrare che, se $n \geq 5$, allora S_n non ha nessun sottogruppo di indice k con $2 < k < n$. [In particolare S_5 non ha sottogruppi di ordine 30 o 40.]

Esercizio 4.3.12. Dato un primo di Mersenne[5] $q = 2^p - 1$, dimostrare che in un gruppo G di ordine $2^p q$ o c'è un solo 2-Sylow o c'è un solo q-Sylow (con 'o' si intende che potrebbero anche valere entrambe le cose contemporaneamente).

Esercizio 4.3.13. Dimostrare che esiste, a meno di isomorfismo, un solo prodotto semidiretto non abeliano di $\mathbb{Z}_4$ per $\mathbb{Z}_4$. Calcolare il centro di tale gruppo.

[5] Vedi dispense di Aritmetica, Esercizio 15.3, pagina 129.

Capitolo 5

Esercizi di classificazione (lezione del 18 ottobre)

5.1 Classificazione dei gruppi di ordine 18

Nota: le note di questo paragrafo sono state scritte da alcuni studenti, che ringrazio a nome di tutti. Le trovate come file separato nella pagina web del corso.

5.2 I gruppi di ordine 225

La classificazione dei gruppi di ordine 225 non è stata svolta in classe, ma leggetela come utile esercizio.

Sia G un gruppo di ordine 225. Osserviamo che $225 = 3^2 \cdot 5^2$. Sia n_3 il numero dei 3-Sylow di G. Poiché $n_3 \equiv 1 \mod 3$ e $n_3 | 3^2 \cdot 5^2$ le possibilità sono $n_3 = 1$ e $n_3 = 25$.

Quanto a n_5, il numero dei 5-Sylow, visto che $n_5 \equiv 1 \mod 5$ e $n_5 | 3^2 \cdot 5^2$ si conclude che $n_5 = 1$. Dunque c'è un solo 5-Sylow N_5, che è normale.

Se $n_3 = 1$ allora anche l'unico 3-Sylow N_3 è normale. Sappiamo per motivi di ordine degli elementi che $N_3 \cap N_5 = \{e\}$ e che dunque per motivi di cardinalità $N_5 N_3 = G$. Inoltre sappiamo, per il Lemma 4.1.2, che gli elementi di due gruppi normali con intersezione banale commutano fra loro, Osserviamo anche che N_3 e N_5 sono abeliani, avendo ordine uguale al quadrato di un numero primo. Il gruppo N_3 può essere isomorfo a $\mathbb{Z}_9$ o a $\mathbb{Z}_3 \times \mathbb{Z}_3$, il gruppo N_5 può essere isomorfo a $\mathbb{Z}_{25}$ o a $\mathbb{Z}_5 \times \mathbb{Z}_5$. Dunque il gruppo G è abeliano. Le quattro possibilità per G sono:

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$$

$$\mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$\mathbb{Z}_9 \times \mathbb{Z}_{25}$$

Può accadere che invece sia $n_3 = 25$? Questo equivale a dire: può accadere che esista un gruppo G di ordine 225 non abeliano?

Nel caso $n_3 = 25$, la normalità di N_5, unita alle osservazioni $N_3 \cap N_5 = \{e\}$ e $N_5 N_3 = G$ ci permette di concludere che il gruppo G è un prodotto semidiretto $N_5 \rtimes_\tau N_3$.

Studiamo le possibilità:

- $$\tau \, : \, \mathbb{Z}_9 \to Aut(\mathbb{Z}_{25})$$

  c'è solo l'omomorfismo banale perché $\mathbb{Z}_{25}^*$ ha ordine 20 e dunque non contiene elementi di ordine 3 o 9. Si ritrova dunque un gruppo abeliano.

- $$\tau \, : \, (\mathbb{Z}_3 \times \mathbb{Z}_3) \to Aut(\mathbb{Z}_{25})$$

  come sopra c'è solo l'omomorfismo banale. Si ritrova dunque un gruppo abeliano.

- $$\tau \, : \, \mathbb{Z}_9 \to Aut(\mathbb{Z}_5 \times \mathbb{Z}_5) \cong GL(2, \mathbb{Z}_5)$$

  Si osserva che $GL(2, \mathbb{Z}_5)$ ha $24 \cdot 20$ elementi (24 scelte per la prima colonna della matrice, che deve essere non nulla, e 20 scelte per la seconda colonna, che non deve essere multipla della prima). L'immagine di τ può avere ordine 1,3 o 9, essendo isomorfa al quoziente di un gruppo di ordine 9. Però in un gruppo di $24 \cdot 20$ elementi non c'è un sottogruppo di ordine 9. Dunque l'immagine di τ ha ordine 1 o 3. Nel caso in cui abbia ordine 1 allora τ è l'omomorfismo banale e si ritrova un gruppo abeliano. Il caso in cui l'immagine di τ ha ordine 3 è quello in cui τ manda $\mathbb{Z}_9$ su un $3-$Sylow di $GL(2, \mathbb{Z}_5)$. Ci sono dunque molte scelte per τ. Però i 3-Sylow di $GL(2, \mathbb{Z}_5)$ sono tutti coniugati fra loro. Applicando la Proposizione 4.2.1, si conclude immediatamente che tutti i τ possibili danno origine a prodotti semidiretti isomorfi (compare appunto appunto la possibilità di coniugare per α e in alcuni casi dovremo utilizzare l'automorfismo β di $\mathbb{Z}_9$ che manda ogni elemento nel suo opposto).

- $$\tau \, : \, (\mathbb{Z}_3 \times \mathbb{Z}_3) \to Aut(\mathbb{Z}_5 \times \mathbb{Z}_5) \cong GL(2, \mathbb{Z}_5)$$

  simile al precedente. L'immagine di τ può avere ordine 1 o 3. Nel primo caso si ritrova un gruppo abeliano, nel secondo si nota che tutte le τ possibili

danno origine a prodotti semidiretti isomorfi utilizzando la proposizione. Dati due omomorfismi $\phi, \psi : (\mathbb{Z}_3 \times \mathbb{Z}_3) \to Aut(\mathbb{Z}_5 \times \mathbb{Z}_5) \cong GL(2, \mathbb{Z}_5)$, si utilizza sempre infatti che i 3-Sylow di $GL(2, \mathbb{Z}_5)$ sono tutti coniugati fra loro e dunque, usando α, possiamo supporre da ora in poi che abbiano la stessa immagine. Quanto a β, potrà essere necessario sceglierlo opportunamente: si osserva che ϕ, ψ sono determinati una volta che si conoscono $Ker\ \phi$, $Ker\ \psi$ (hanno ordine 3) e si sa il valore di ϕ , ψ su un vettore v che non è in nessuno dei due Ker. Il β che ci serve deve mandare per esempio $Ker\ \phi$ in $Ker\ \psi$ (deve dunque mandare un generatore dell'uno in un generatore dell'altro) e soddisfare $\psi(\beta(v)) = \phi(v)$, che si traduce a seconda dei casi nel porre $\beta(v) = v$ oppure $\beta(v) = -v$. Si tratta di due condizioni su due vettori linearmente indipendenti dunque un tale β si trova.

In conclusione i gruppi di ordine 225 sono 6, quattro abeliani e due non abeliani. I due non abeliani sono non isomorfi fra loro perché hanno 3-Sylow non isomorfi.

Capitolo 6

Gli automorfismi di S_n, prima parte (lezione del 19 ottobre)

6.1 Gli automorfismi di S_n per $n \neq 6$

Nota: le note di questo paragrafo sono state scritte da alcuni studenti, che ringrazio a nome di tutti. Le trovate come file separato nella pagina web del corso.

Capitolo 7

La classificazione dei gruppi abeliani finitamente generati (lezione del 26 ottobre)

7.1 L'enunciato del teorema

Definizione 7.1.1. Un gruppo abeliano M si dice *finitamente generato* se esistono degli elementi $m_1, m_2, \ldots, m_n \in M$ tali che ogni $m \in M$ si può scrivere come combinazione lineare degli $m_1, m_2, \ldots, m_n$ a coefficienti interi:

$$m = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n \qquad \text{con } a_1, a_2, \ldots, a_n \in \mathbb{Z}.$$

Si dice che l'insieme $\{m_1, m_2, \ldots, m_n\}$ è un *insieme di generatori* per M.

Osservazione 7.1.1. L'idea richiama dunque quella di insieme di generatori per uno spazio vettoriale. Nel contesto dei gruppi abeliani non è detto che da un insieme di generatori si possa estrarre un sottoinsieme di elementi linearmente indipendenti.

Osservazione 7.1.2. Un gruppo finito è finitamente generato (si potrebbe prendere come insieme di generatori addirittura l'insieme di tutti gli elementi del gruppo!).

Esempio 7.1.1. Il gruppo abeliano $(\mathbb{Q}, +)$ non è finitamente generato: se per assurdo $\frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_n}{s_n}$ fosse un insieme di generatori, basta prendere un primo p che non divide nessuno degli s_i e osservare che non è possibile scrivere:

$$\frac{1}{p} = a_1 \frac{r_1}{s_1} + a_2 \frac{r_2}{s_2} + \cdots + a_n \frac{r_n}{s_n}$$

con gli a_i interi.

Definizione 7.1.2. Se un gruppo abeliano A è isomorfo a $\mathbb{Z}^k$ ($k \geq 1$), A si dice *gruppo abeliano libero* di rango k.

Teorema 7.1.1. *Sia M un gruppo abeliano finitamente generato.*
a) Vale che

$$M \cong \mathbb{Z}^k$$

con $k \geq 0$ oppure

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

dove $k \geq 0$, d_i numeri interi ≥ 2 e, se $i < j$, d_i divide d_j.
b) I numeri k, $d_1, d_2, \ldots, d_r$ sono univocamente determinati da M.

Osservazione 7.1.3. È importante notare che i numeri $k, d_1, d_2, \ldots, d_r$ sono univocamente determinati, ma la formula del teorema non individua in maniera univoca in M un sottogruppo isomorfo a $\mathbb{Z}_{d_1}$, uno isomorfo a $\mathbb{Z}_{d_2}$ etc..: basti pensare a $M = \mathbb{Z}_2 \times \mathbb{Z}_2$. In M ci sono tre distinti sottogruppi isomorfi a $\mathbb{Z}_2$ e il prodotto interno di due qualunque di questi è isomorfo a M.

Dimostreremo questo teorema nei paragrafi 7.3 e 8.2.

7.2 Successioni esatte e sottogruppi di gruppi abeliani liberi

Definizione 7.2.1. Una successione di n ($n \geq 2$) omomorfismi di gruppi abeliani

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \to \ldots \to A_{n-1} \xrightarrow{f_n} A_n$$

si dice *esatta in A_i* se $Imm\ f_i = Ker\ f_{i+1}$. Si dice *esatta* se è esatta in A_i per ogni $i = 1, 2, \ldots, n$.

Una successione esatta di omomorfismi di gruppi abeliani della forma

$$\{0\} \to A \xrightarrow{f} B \xrightarrow{g} C \to \{0\}$$

si dice *esatta corta*. Dalla definizione segue che in questo caso l'omomorfismo f è iniettivo e g è surgettivo.

Proposizione 7.2.1. *Data una successione esatta corta*

$$\{0\} \to A \xrightarrow{f} B \xrightarrow{g} \mathbb{Z} \to \{0\}$$

vale che $B \cong A \oplus \mathbb{Z}$.

Dimostrazione. Visto che g è surgettiva, esiste $b \in B$ tale che $g(b) = 1$. Costruisco allora l'omomorfismo $\psi : \mathbb{Z} \to B$ ponendo $\psi(1) = b$. Vale allora che $g \circ \psi : \mathbb{Z} \to \mathbb{Z}$ è l'identità. La mappa

$$\Gamma : A \oplus \mathbb{Z} \to B$$

data da $\Gamma((a, n)) = f(a) + \psi(n)$ fornisce l'isomorfismo cercato.

Osservazione 7.2.1. Attenzione, in generale non è vero che, data la successione esatta corta

$$\{0\} \to A \to B \to C \to \{0\}$$

allora $B \cong A \oplus C$. Per esempio, la successione

$$\{0\} \to \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_{p^2} \xrightarrow{g} \mathbb{Z}_p \to \{0\}$$

dove f è l'immersione nell'unico sottogruppo isomorfo a $\mathbb{Z}_p$ e g è la proiezione sul quoziente rispetto a questo sottogruppo. Una dimostrazione molto simile a quella vista sopra ci garantisce che lo "spezzamento" $B \cong A \oplus C$ è vero quando C è un gruppo abeliano libero.

Proposizione 7.2.2. *Sia M un sottogruppo di un gruppo libero di rango n. Allora $M \cong \mathbb{Z}^r$ per un certo $0 \leq r \leq n$ (con la convenzione $\mathbb{Z}^0 = \{0\}$).*

Dimostrazione. A meno di isomorfismo, possiamo pensare M come sottogruppo di $\mathbb{Z}^n$. Si procede per induzione su n.

Se $n = 1$, sappiamo che il sottogruppo M è della forma $d\mathbb{Z}$ per $d \in \mathbb{N}$, dunque è isomorfo a $\{0\} = \mathbb{Z}^0$ se $d = 0$ e a $\mathbb{Z}$ se $d \neq 0$.

Consideriamo ora $n > 1$ e sia $\pi : \mathbb{Z}^n \to \mathbb{Z}$ l'omomorfismo dato dalla proiezione sull'ultima coordinata. Allora $\pi_{|M} : M \to \mathbb{Z}$ ha come immagine un sottogruppo del tipo $d\mathbb{Z}$ per $d \in \mathbb{N}$. Se $d = 0$ allora

$$M \subseteq \{(a_1, a_2, \ldots, a_{n-1}, 0) \mid a_i \in \mathbb{Z}\} \cong \mathbb{Z}^{n-1}$$

e si conclude subito per ipotesi induttiva che M è isomorfo a $\mathbb{Z}^r$ con $0 \leq r \leq n-1$. Se $d \neq 0$ allora abbiamo la seguente successione esatta corta:

$$\{0\} \to Ker\ \pi_{|M} \xrightarrow{i} M \xrightarrow{\pi_{|M}} d\mathbb{Z} \cong \mathbb{Z} \to \{0\}$$

dove i è la (ovvia) immersione di $Ker\ \pi_{|M}$ in M. Per la Proposizione 7.2.1 sappiamo che

$$M \cong Ker\ \pi_{|M} \oplus \mathbb{Z}$$

Ma, visto che π è la proiezione sull'ultima coordinata,

$$Ker\ \pi_{|M} \subseteq \{(a_1, a_2, \ldots, a_{n-1}, 0) \mid a_i \in \mathbb{Z}\} \cong \mathbb{Z}^{n-1}$$

e dunque per ipotesi induttiva $Ker\ \pi_{|M} \cong \mathbb{Z}^s$ con $0 \leq s \leq n-1$. Si conclude dunque che

$$M \cong \mathbb{Z}^s \oplus \mathbb{Z} = \mathbb{Z}^{s+1}$$

con $s + 1 \leq n$ come volevamo.

7.3 Prima parte della dimostrazione del teorema di classificazione

Dimostriamo la parte a) del teorema 7.1.1.

Sia $\{m_1, m_2, \ldots, m_n\}$ un insieme di generatori per M. Consideriamo l'omomorfismo $\phi : \mathbb{Z}^n \to M$ definito da

$$\phi(a_1, a_2, \ldots, a_n) = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n.$$

È surgettivo visto che $m_1, m_2, \ldots, m_n$ sono generatori. Abbiamo allora la successione esatta corta

$$\{0\} \to Ker\ \phi \xrightarrow{i} \mathbb{Z}^n \xrightarrow{\phi} M \to \{0\}$$

Per la Proposizione 7.2.2 sappiamo che $Ker\ \phi$ è isomorfo a $\mathbb{Z}^r$ con $0 \leq r \leq n$. Se $r = 0$ allora ϕ è un isomorfismo e $M \cong \mathbb{Z}^n$.

Se $r \geq 1$, identificando $Ker\ \phi$ con $\mathbb{Z}^r$ possiamo riscrivere così la precedente successione esatta:

$$\{0\} \to \mathbb{Z}^r \xrightarrow{i} \mathbb{Z}^n \xrightarrow{\phi} M \to \{0\}$$

L'omomorfismo i (per semplicità abbiamo continuato a chiamarlo così anche dopo l'identificazione) è rappresentato, nelle basi[1] standard di $\mathbb{Z}^r$ e Z^n, da una matrice L di dimensione $n \times r$. Sappiamo, per il primo teorema di omomorfismo, che

$$M \cong \frac{\mathbb{Z}^n}{Ker\ \phi} \cong \frac{\mathbb{Z}^n}{Imm\ i}$$

Per studiare bene questo quoziente, dobbiamo innanzitutto trovare il modo migliore di scrivere $Imm\ i$. Osserviamo che può essere di aiuto cambiare base sia in partenza che in arrivo, in modo da avere la matrice nella forma più leggibile possibile. Utilizzando l'algoritmo di Gauss, possiamo cambiare base facendo le "mosse" elementari di riga e di colonna nella loro versione "intera" ossia:

- possiamo scambiare fra di loro le righe (o le colonne);
- possiamo moltiplicare una riga o una colonna per -1;
- possiamo sommare ad una riga un'altra riga moltiplicata per un intero m (lo stesso per le colonne).

Come sappiamo dall'algebra lineare, queste operazioni corrispondono infatti a moltiplicare a destra o a sinistra per matrici invertibili, dunque si tratta di operazioni reversibili, appunto cambiamenti di base. Ricordiamo (lo dimostreremo alla fine) il seguente:

[1] Anche nel contesto dei gruppi abeliani, in piena analogia con quanto accade per gli spazi vettoriali, chiamiamo base un insieme di generatori che sono linearmente indipendenti.

Teorema 7.3.1. *Data una matrice L non nulla di dimensione $t \times s$ a coefficienti interi di rango h è possibile, attraverso una sequenza di mosse intere elementari di riga e di colonna, trasformarla nella matrice L' tale che $L'_{ij} = 0$ se $i \neq j$ e, per quel che riguarda gli elementi "diagonali" vale che $L'_{ii} > 0$ se $i \leq h$, $L'_{ii} = 0$ se $i > h$ ed inoltre*

$$L'_{11} = MCD\{L_{ij}\}_{\substack{i=1,\dots,t \\ j=1,\dots,s}}$$

e $L'_{11}|L'_{22}|\cdots|L'_{hh}$.

Applicando questo teorema possiamo dunque trasformare la matrice L che è di dimensione $n \times r$ ($r \leq n$) e di rango r (è infatti associata ad una applicazione iniettiva) in una matrice del tipo

$$\begin{pmatrix} k_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & k_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & k_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & ... & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & ... & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & k_r \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

dove i k_i sono interi positivi e $k_1|k_2|\cdots|k_r$.

Riassumendo, sappiamo che il gruppo M è isomorfo a $\mathbb{Z}^n$ modulo il sottogruppo H generato dalle colonne di questa matrice. L'omomorfismo

$$\gamma : \mathbb{Z}^n \to \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_r} \oplus \mathbb{Z}^{n-r}$$

data da $\gamma((a_1, a_2, \dots, a_n)) = ([a_1]_{k_1}, [a_2]_{k_2}, \dots, [a_r]_{k_r}, a_{r+1}, a_{r+2}, \dots, a_n)$ è surgettivo e ha per nucleo proprio H, dunque

$$M \cong \frac{\mathbb{Z}^n}{H} \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_r} \oplus \mathbb{Z}^{n-r}.$$

Questo conclude la dimostrazione della parte a) del teorema 7.1.1. Naturalmente, se alcuni (o tutti) i k_i sono uguali a 1, possiamo trascurare le relative componenti $\mathbb{Z}_1$ nel prodotto; ecco perché nell'enunciato del teorema compaiono solo dei $d_i \geq 2$. Resta da dimostrare il teorema 7.3.1: proponiamo qui una dimostrazione simile nella sostanza a quella vista a lezione (a lezione abbiamo dato più rilievo all'aspetto algoritmico).

Dimostrazione del teorema 7.3.1.
Dimostreremo innanzitutto che la matrice si può ridurre nella forma indicata, con $L'_{11}|L'_{22}|\cdots|L'_{hh}$, tralasciando per il momento la parte dell'enunciato che dice che

$$L'_{11} = MCD\{L_{ij}\}_{\substack{i=1,\ldots,t \\ j=1,\ldots,s}}$$

La dimostrazione è per induzione sulla dimensione della matrice (rappresentata dal prodotto ts del numero delle sue righe per il numero delle sue colonne). I casi $ts = 1, ts = 2$ sono immediati, e in generale sono immediati i casi con $t = 1$ o $s = 1$.

Data una matrice non nulla $A = (A_{ij})$ chiamiamo $min\ A$ il minimo fra i valori assoluti dei coefficienti non nulli di A:

$$min\ A = min\ \{|A_{ij}|\ |\ A_{ij} \neq 0\}$$

Consideriamo ora matrici $t \times s$ con $t > 1$ e $s > 1$. Sulle matrici non nulle B di dimensione $t \times s$ iniziamo una induzione su $min\ B$. Se $min\ B = 1$ agiamo con mosse elementari di riga e colonna in modo da ottenere una nuova matrice B^1 con $B^1_{11} = 1$. A questo punto usiamo la prima colonna di B^1 per porre uguali a 0, attraverso le mosse elementari di colonna, i coefficienti $B^1_{12}, B^1_{13}, \ldots, B^1_{1s}$ della prima riga. Dopodiché, con procedimento simile, attraverso mosse elementari di riga possiamo rendere uguali a zero i coefficienti della prima colonna (a parte ovviamente quello più in alto, che rimane uguale a 1), e otteniamo una matrice B^2 della seguente forma:

$$\begin{pmatrix} 1 & 0 \\ 0 & T \end{pmatrix}$$

dove T è una matrice $(t-1) \times (s-1)$. Se T è nulla abbiamo già finito, altrimenti possiamo concludere usando l'ipotesi induttiva sulla dimensione $(t-1)(s-1)$.

Consideriamo adesso una matrice L di dimensione $t \times s$ con $t > 1$ e $s > 1$ e tale che $min\ L > 1$. Ci sarà un coefficiente L_{ij} tale che $|L_{ij}| = min\ L$. Possiamo, con mosse elementari di riga e di colonna trasformare L in modo da avere una nuova matrice L^1 in cui $L^1_{11} = |L_{ij}|$. A questo punto cerchiamo di usare la prima colonna di L^1 per rendere uguali a 0, attraverso mosse elementari, i coefficienti della prima riga $L^1_{12}, L^1_{13}, \ldots, L^1_{1s}$. Se L^1_{11} non divide L^1_{1i} allora la divisione euclidea ci fa ottenere una nuova matrice L^2 in cui al posto di L^1_{1i} c'è un numero intero positivo $k < L^1_{11}$. In tal caso concludiamo per l'ipotesi induttiva su "min" perché $min\ L^2 < min\ L^1$. Se invece L^1_{11} divide tutti i L^1_{1i} possiamo ottenere una matrice L^3 in cui la prima riga è $(L_{11}, 0, 0, \ldots, 0)$. Agiamo allora con mosse di riga per rendere uguali a 0 tutti i coefficienti $L^3_{21}, L^3_{31}, \ldots, L^3_{t1}$ della prima colonna. Anche qui, come prima, o uno di tali coefficienti non è diviso da L_{11}, e allora si conclude

per l'ipotesi induttiva su "min", oppure si riesce ad ottenere una matrice L^4 della forma:

$$\begin{pmatrix} L_{11} & 0 \\ 0 & C \end{pmatrix}$$

dove C è una matrice $(t-1) \times (s-1)$. Se C è nulla abbiamo finito. Se C non è nulla e L_{11} divide tutti i coefficienti di C possiamo concludere per l'ipotesi induttiva sulla dimensione. Se invece c'è un coefficiente C_{hl} che non è diviso da L_{11} allora possiamo sommare la riga h-esima alla prima riga. A questo punto possiamo sottrarre alla colonna l-esima un multiplo della prima colonna in modo da ottenere (in posizione $(1, l)$) un coefficiente positivo $< L_{11}$. Si conclude allora per induzione su "min".

Per concludere osserviamo che quando si passa da una matrice D ad una matrice F applicando una mossa elementare intera di riga o di colonna vale $MCD\{D_{ij}\} = MCD\{F_{ij}\}$. Dunque il coefficiente L'_{11} della matrice descritta nell'enunciato del teorema, che, come si verifica immediatamente, è uguale a $MCD\{L'_{ij}\}$, è anche uguale a $MCD\{L_{ij}\}$.

7.4 Qualche esercizio

Esercizio 7.4.1. I gruppi $\mathbb{Z}_{12} \times \mathbb{Z}_{72}$ e $\mathbb{Z}_{18} \times \mathbb{Z}_{48}$ sono isomorfi? E i gruppi $\mathbb{Z}_{72} \times \mathbb{Z}_{84}$ e $\mathbb{Z}_{36} \times \mathbb{Z}_{168}$?

Esercizio 7.4.2. Trovare tutte le coppie di numeri interi positivi (a, b) tali che il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ sia isomorfo a $\mathbb{Z}_a \times \mathbb{Z}_b$.

Esercizio 7.4.3. Quanti gruppi abeliani di ordine 100 esistono (a meno di isomorfismo)?

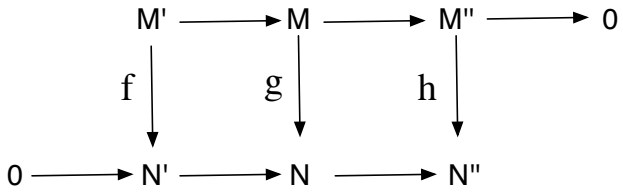
Esercizio 7.4.4. Quanti sono i sottogruppi di cardinalità 50 di $\mathbb{Z}_{20} \times \mathbb{Z}_{100}$?

Esercizio 7.4.5. Consideriamo il gruppo $A = \mathbb{Z}_2 \times \mathbb{Z}_{12}$ e i sottogruppi $H = \mathbb{Z}_2 \times \{[0]\}$ e $K = \{[0]\} \times \{[0], [6]\}$. Vale che $H \cong \mathbb{Z}_2 \cong K$, ma è vero o falso che $A/H \cong A/K$?

Esercizio 7.4.6. Ripensare all'enunciato e alla dimostrazione del Teorema 7.3.1. Si potrebbe estendere al caso di matrici con coefficienti sull'anello dei polinomi $K[x]$ su un campo K?

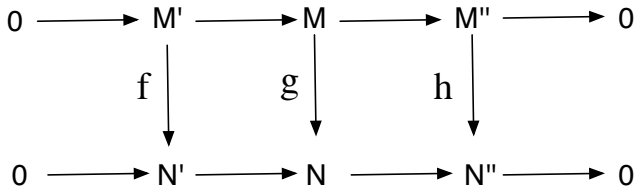
Esercizio 7.4.7. Sia Γ un sottogruppo discreto (rispetto alla topologia standard) non nullo di $\mathbb{R}^n$. Dimostrare che Γ è un gruppo abeliano libero con generatori $g_1, g_2, \ldots, g_r$ linearmente indipendenti su $\mathbb{R}$. [Nota: un sottogruppo discreto di $\mathbb{R}^n$ può essere definito anche così: un sottogruppo Γ tale che per ogni $r \in \mathbb{R}^+$ l'intersezione $\Gamma \cap B(r)$ è finita, dove $B(r)$ è la palla centrata nell'origine e di raggio r.]

Esercizio 7.4.8. Consideriamo il seguente diagramma di gruppi abeliani e omomorfismi in cui tutti i quadrati "commutano" e le successioni orizzontali sono esatte:



Dimostrare che:
a) se f e h sono iniettive allora lo è anche g;
b) se f e h sono surgettive allora lo è anche g.

Esercizio 7.4.9. Consideriamo il seguente diagramma di gruppi abeliani e omomorfismi in cui tutti i quadrati "commutano" e le successioni orizzontali sono esatte:



Dimostrare che se due qualunque fra gli omomorfismi f, h, g sono isomorfismi allora lo è anche il terzo.

Capitolo 8

Ancora sui gruppi abeliani finitamente generati (lezione del 2 novembre)

8.1 Sottogruppi di torsione

Cominciamo con alcune definizioni.

Definizione 8.1.1. Sia A un gruppo abeliano. Chiamiamo $T(A)$ il *sottogruppo di torsione*

$$T(A) = \{x \in A \mid \exists n \in \mathbb{N}, n > 0 \text{ tale che } nx = 0\}.$$

Si tratta dunque del sottogruppo formato da tutti gli elementi che hanno ordine finito.

Esercizio 8.1.1. Verificare che $T(A)$ è un sottogruppo (attenzione, l'ipotesi di abelianità è importante, vedi Esercizio 8.3.2).

Definizione 8.1.2. Sia A un gruppo abeliano. Dato un numero primo p chiamiamo $A(p)$ il *sottogruppo di p-torsione*

$$A(p) = \{x \in T(A) \mid \exists a \in \mathbb{N} \text{ tale che } o(x) = p^a\}$$

Osserviamo che $A(p)$ è un sottogruppo che coincide con il p-Sylow. Infatti per il secondo teorema di Sylow un elemento di ordine p^a è contenuto in un p-Sylow. In questo caso, dato che il gruppo è abeliano, c'è un solo p-Sylow. Dunque $A(p)$ è tutto contenuto nel p-Sylow. L'altra inclusione è ovvia.

Proposizione 8.1.1. *Un gruppo abeliano finito A è il prodotto diretto dei suoi sottogruppi di Sylow (ossia dei suoi sottogruppi di p-torsione).*

Dimostrazione. Dimostriamo l'enunciato per induzione sul numero dei sottogruppi di Sylow (ossia sul numero dei primi p che dividono l'ordine del gruppo). Nel caso con un solo Sylow non c'è nulla da dimostrare. Sia allora A un gruppo abeliano finito e siano N_{p_1}, N_{p_2},..,N_{p_k} i suoi sottogruppi di Sylow. Si osserva facilmente, per esempio applicando ripetutamente il Lemma 4.1.1 che $N_{p_2}N_{p_3}\cdots N_{p_k}$ è un sottogruppo di A. Inoltre (usiamo la notazione moltiplicativa) vale che $N_{p_1} \cap (N_{p_2}N_{p_3}\cdots N_{p_k}) = \{e\}$ per ragioni legate all'ordine degli elementi. Allora per motivi di cardinalità $N_{p_1}(N_{p_2}N_{p_3}\cdots N_{p_k}) = A$. Per il Lemma 4.1.2 sappiamo che i sottogruppi N_{p_1} e $N_{p_2}N_{p_3}\ldots N_{p_k}$ sono in prodotto diretto. Si conclude osservando che per ipotesi induttiva $N_{p_2}N_{p_3}\cdots N_{p_k}$ è prodotto diretto di N_{p_2},..,N_{p_k}.

Alla luce della proposizione precedente possiamo esprimere il Teorema 7.1.1 di classificazione dei gruppi abeliani finitamente generati in un altro modo, mettendo in risalto le componenti di p-torsione:

Teorema 8.1.1. *Sia M un gruppo abeliano finitamente generato.*
a) Vale che

$$M \cong \mathbb{Z}^k$$

con $k \geq 0$ oppure, se $T(M) \neq \{0\}$,

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{t} M(p_i)$$

dove $k \geq 0$ e $p_1, p_2, \ldots, p_t$ sono i primi che dividono $|T(M)|$. Inoltre, per ogni $1 \leq i \leq t$, vale che

$$M(p_i) \cong \mathbb{Z}_{p_i^{a_{i1}}} \oplus \mathbb{Z}_{p_i^{a_{i2}}} \cdots \oplus \mathbb{Z}_{p_i^{a_{ir(i)}}}$$

dove $r(i)$ è un intero ≥ 1 e $1 \leq a_{i1} \leq a_{i2} \leq \ldots \leq a_{ir(i)}$.
b) I numeri k,p_i, $r(i)$ e a_{ij} sono univocamente determinati da M.

Osservazione 8.1.1. Osserviamo che, dato M, gruppo abeliano (non necessariamente finitamente generato), i sottogruppi $T(M)$ e $M(p_i)$ sono univocamente individuati, mentre il solito esempio $\mathbb{Z}_2 \times \mathbb{Z}_2$ ci mostra che i sottogruppi isomorfi a $\mathbb{Z}_{p_i^{a_{ij}}}$ che compaiono nella formula del teorema di classificazione per i gruppi abeliani finitamente generati non sono individuati in maniera univoca dentro $M(p_i)$.

È facile osservare che le parti a) del Teorema 8.1.1 e del Teorema 7.1.1 sono equivalenti. La differenza consiste solo nel modo in cui è presentato il sottogruppo $T(M)$.

Mostriamo con un esempio come si passa da una presentazione all'altra. Sia

$$T(M) \cong \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{24} \times \mathbb{Z}_{72} \times \mathbb{Z}_{360} \times \mathbb{Z}_{1800}$$

espresso come nel Teorema 7.1.1. Possiamo ora scrivere ogni gruppo ciclico che appare come prodotto dei suoi p-Sylow, che sono a loro volta gruppi ciclici:

$$T(M) \cong \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_3 \times \mathbb{Z}_8) \times (\mathbb{Z}_8 \times \mathbb{Z}_9) \times (\mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_9) \times (\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25})$$

Raccogliendo le componenti di p-torsione otteniamo

$$T(M) \cong (\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_8) \times (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_9) \times (\mathbb{Z}_5 \times \mathbb{Z}_{25})$$

e osserviamo che abbiamo espresso il gruppo $T(M)$ come richiesto dal Teorema 8.1.1.

Viceversa, se fossimo partiti da quest'ultima espressione, avremmo potuto ricostruire la presentazione del gruppo richiesta dal Teorema 7.1.1 tramite il seguente algoritmo:

- si fa il prodotto dei gruppi ciclici più grandi che appaiono nelle componenti di p-torsione di $T(M)$. Nel nostro esempio si ottiene

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \cong \mathbb{Z}_{1800}$$

- Si cancellano i gruppi ciclici appena utilizzati e se il gruppo residuo non è banale si ripete il passo precedente. Nel nostro esempio cancellando i gruppi utilizzati abbiamo

$$(\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_8) \times (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9) \times \mathbb{Z}_5$$

Applicando l'algoritmo al nostro esempio otteniamo dunque in sequenza i gruppi ciclici $\mathbb{Z}_{1800}$, $\mathbb{Z}_{360}$, $\mathbb{Z}_{72}$, $\mathbb{Z}_{24}$, $\mathbb{Z}_6$, $\mathbb{Z}_3$, che sono proprio i gruppi che appaiono nella presentazione di $T(M)$ offerta dal Teorema 7.1.1.

In realtà gli algoritmi appena esposti mostrano in particolare che se avessimo due diverse presentazioni di $T(M)$ del tipo richiesto dal Teorema 7.1.1 (in altre parole se non valesse l'unicità) queste darebbero origine a due diverse presentazioni di $T(M)$ del tipo richiesto dal Teorema 8.1.1, e viceversa.

Terremo conto di questa osservazione nel prossimo paragrafo, in cui dimostreremo la parte b) del Teorema 7.1.1 (e anche, come immediato corollario, la parte b) del Teorema 8.1.1, che è ad essa equivalente).

8.2 Dimostrazione dell'unicità nel teorema di classificazione

Cominciamo col dimostrare l'unicità nel caso dei p -gruppi abeliani, ossia dei gruppi abeliani il cui ordine è la potenza di un primo p.

Lemma 8.2.1. *Siano A un gruppo abeliano finito di ordine p^a con p primo e $a \geq 1$. Supponiamo che*

$$A \cong \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_j}}$$

con $1 \leq \alpha_1 \leq \alpha_2 \leq .... \leq \alpha_j$ e anche che

$$A \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \cdots \times \mathbb{Z}_{p^{\beta_h}}$$

con $1 \leq \beta_1 \leq \beta_2 \leq .... \leq \beta_h$. Allora $j = h$ e $\alpha_i = \beta_i$ per ogni $i = 1, ..., h$.

Dimostrazione. Contiamo gli elementi di ordine $\leq p$ in A: dalla prima presentazione risulta che ce ne sono p^j, dalla seconda p^h, dunque deve valere $h = j$. Ora supponiamo per assurdo che le due liste $\alpha_1 \leq \alpha_2 \leq .... \leq \alpha_h$ e $\beta_1 \leq \beta_2 \leq .... \leq \beta_h$ non siano uguali. Sia u il più piccolo numero in $\{1, ..., h\}$ tale che $\alpha_u \neq \beta_u$ e per fissare le idee diciamo che $\alpha_u > \beta_u$. Consideriamo ora il sottogruppo H di A definito (in notazione moltiplicativa) da

$$H = \{x^{p^{\beta_u}} \ : \ x \in A\}$$

Esercizio 8.2.1. Dimostrare che H è un sottogruppo di A.

Dalla prima presentazione di A risulta che

$$H \cong \mathbb{Z}_{p^{\alpha_u - \beta_u}} \times \cdots \times \mathbb{Z}_{p^{\alpha_h - \beta_u}}$$

mentre dalla seconda presentazione risulta che

$$H \cong \mathbb{Z}_{p^{\beta_{u'} - \beta_u}} \times \cdots \times \mathbb{Z}_{p^{\beta_h - \beta_u}}$$

dove $\beta_{u'}$ è il primo numero della lista $\beta_1 \leq \beta_2 \leq .... \leq \beta_h$ maggiore di β_u (se esiste).

Se contiamo adesso gli elementi di ordine $\leq p$ in H, notiamo che dalla prima presentazione risultano p^{h-u+1}, dalla seconda presentazione $p^{h-u'+1}$, che è strettamente minore di p^{h-u+1}. Questo dà un assurdo.

□

Possiamo ora dimostrare la parte di unicità del Teorema 7.1.1.

Dimostrazione. [Dimostrazione della parte b) del Teorema 7.1.1.]

Supponiamo che per un gruppo abeliano finitamente generato M valga

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

ma anche

$$M \cong \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$$

con i $d_i \geq 2$ e tali che se $i < j$ allora $d_i | d_j$ e lo stesso per i b_i.[1] Esiste dunque un isomorfismo

$$\gamma \, : \, \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \to \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$$

Osserviamo innanzitutto che γ, essendo un isomorfismo, preserva gli ordini degli elementi e dunque manda la parte di torsione del dominio bigettivamente sulla parte di torsione del codominio, che sono entrambe isomorfe a $T(M)$. Abbiamo cioè un isomorfismo:

$$\gamma' = \gamma_{| \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}} \, : \, \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \to \bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$$

Possiamo dire di più su γ': per ogni primo p che divide l'ordine di $T(M)$, γ' deve essere un isomorfismo fra i corrispondenti sottogruppi di p-torsione.

Ognuno di tali sottogruppi si decompone come

$$\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_j}}$$

con $1 \leq \alpha_1 \leq \alpha_2 \leq .... \leq \alpha_j$, e per il Lemma 8.2.1 sappiamo allora che la lista $1 \leq \alpha_1 \leq \alpha_2 \leq .... \leq \alpha_j$ è univocamente determinata.

Sappiamo dunque che le decomposizioni

$$\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_j}}$$

dei gruppi di p-torsione di $\bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$ e di $\bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$ coincidono. Allora per le osservazioni del paragrafo precedente possiamo concludere che $r = t$ e $d_i = b_i$ per ogni $i = 1, ..., t$.

Resta da dimostrare che $k = s$. Supponiamo per assurdo che $k > s$.

Consideriamo l'omomorfismo $\gamma'' \, : \, \mathbb{Z}^k \to \mathbb{Z}^s$ ottenuto dalla composizione

$$\mathbb{Z}^k \xrightarrow{i} \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \xrightarrow{\gamma} \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{b_i} \xrightarrow{\pi} \mathbb{Z}^s$$

[1] Questo è uno dei casi da analizzare. Va anche studiato il caso in cui M viene presentato in due modi diversi $M \cong \mathbb{Z}^k$ e $M \cong \mathbb{Z}^s$ che non hanno elementi non banali di torsione. Si tratta però di una situazione più facile e basterà applicare solo una versione ridotta della dimostrazione che stiamo per descrivere. Il caso in cui una presentazione abbia torsione non banale e l'altra no si esclude molto rapidamente....

dove i e π sono rispettivamente l'immersione e la proiezione ovvie. Si osserva che γ'' è iniettivo. Infatti se vale $\gamma''((a_1, a_2, \ldots, a_k)) = \gamma''((b_1, b_2, \ldots, b_k))$, questo vuole dire che $\pi \circ \gamma((a_1 - b_1, a_2 - b_2, \ldots, a_k - b_k, [0], \ldots, [0])) = (0, 0, \ldots, 0)$. Dunque $\gamma((a_1 - b_1, a_2 - b_2, \ldots, a_k - b_k, [0], \ldots, [0]))$ o è $(0, 0, 0 \ldots, 0, [0], \ldots, [0])$ oppure è un elemento non nullo che ha componenti non nulle solo nella parte di torsione. In ogni caso è un elemento di ordine finito. Ma sappiamo che γ, che è un isomorfismo, non può mandare elementi di ordine infinito in elementi di ordine finito. L'unica possibilità rimasta è che $a_1 = b_1, a_2 = b_2, \ldots, a_k = b_k$ e dunque l'iniettività della γ'' è dimostrata.

Possiamo esprimere γ'' con una matrice a coefficienti interi con s righe e k colonne. Possiamo "leggere" le colonne come vettori colonna $v_1, v_2, \ldots, v_k$ a coefficienti in $\mathbb{Q}$. Tali vettori non possono essere linearmente indipendenti su $\mathbb{Q}$, visto che abbiamo supposto che $s < k$. Allora devono esistere coefficienti $q_1, q_2, \ldots, q_k$ razionali non tutti nulli tali che

$$q_1 v_1 + q_2 v_2 + \cdots + q_k v_k = \underline{0}.$$

Moltiplicando per il minimo comune multiplo dei denominatori dei q_i ottengo una relazione a coefficienti interi non tutti nulli

$$n_1 v_1 + n_2 v_2 + \cdots + n_k v_k = \underline{0}.$$

Questo vuol dire che $\gamma''((n_1, n_2, \ldots, n_k)) = (0, 0, \ldots, 0)$ contraddicendo l'iniettività di γ''.

Abbiamo così dimostrato che non può valere $k > s$. Il caso $k < s$ si affronta in maniera del tutto analoga, e possiamo dunque concludere che $k = s$.

□

Osserviamo, che, come immediato corollario segue la parte b) del Teorema 8.1.1 (le due parti sono equivalenti, come si osserva facilmente).

8.3 Esercizi

Esercizio 8.3.1. Mostrare con un esempio che il sottogruppo isomorfo a $\mathbb{Z}^k$ che appare nella formula del teorema di classificazione per i gruppi abeliani finitamente generati non è individuato in maniera univoca in M.

Esercizio 8.3.2. Si dimostri che esiste un prodotto semidiretto $\mathbb{Z} \rtimes \mathbb{Z}_2$ non abeliano. Si mostri che in tale gruppo il sottoinsieme degli elementi di torsione non è un sottogruppo. *Questo gruppo può essere pensato come un gruppo diedrale D_∞: la rotazione r va pensata come una rotazione di un angolo $2\pi\rho$ con ρ irrazionale...*

Esercizio 8.3.3. Si consideri il gruppo $A = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_6$. Per quali numeri interi m esiste in A un sottogruppo ciclico di cardinalità m? È vero o falso che per ogni intero positivo d divisore di 48 esiste in A un sottogruppo di cardinalità d?

Esercizio 8.3.4. Mostrare che gruppo abeliano M di torsione, ossia tale che $M = T(M)$, non è necessariamente finito. In M esiste un limite superiore per l'ordine degli elementi o si trova un esempio in cui ci sono elementi di ordine arbitrariamente grande?

Esercizio 8.3.5. La definizione di gruppo abeliano libero si estende anche al caso di rango "infinito". Un gruppo abeliano A si dice libero se, detto S un insieme di indici,

$$A \cong \bigoplus_{s \in S} \mathbb{Z}.$$

Se un gruppo abeliano A non ha torsione, ossia $T(A) = \{0\}$, si può concludere che è libero? [Più che un esercizio, è una scusa per segnalarvi l'interessante e breve articolo di S. Schröer *Baer's result: the infinite product of the integers has no basis*, su The American Mathematical Monthly Vol. 115, No. 7 (Aug. - Sep., 2008), pp. 660-663, che potete scaricare digitando il titolo su internet.]

Capitolo 9

Prodotti liberi di gruppi e gruppi liberi (lezione del 9 novembre)

Questa lezione comparirà in un file separato sulla pagina web del corso.

Capitolo 10

Campi e automorfismi (lezioni del 15 e del 16 novembre)

10.1 Derivata di un polinomio e molteplicità

Questo paragrafo è di ripasso (l'argomento è stato trattato l'anno scorso a esercitazioni, lo scrivo per fare da 'raccordo' col nuovo programma di quest'anno).

Definizione 10.1.1. Sia F un campo, e $f(x) \in F[x]$, con $f(x) = a_0 + a_1x + \ldots + a_nx^n$. Definiamo la *derivata* di $f(x)$ come il polinomio

$$f'(x) = a_1 + 2a_2x + \ldots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1}.$$

(con questa scrittura si intende che se $f(x) = a_0$ allora $f'(x) = 0$).

La derivata è definita in modo formale (indipendentemente dalla nozione di 'limite') dalla precedente espressione. Non è difficile mostrare che dalla precedente definizione seguono le ben note regole di calcolo delle derivate:

Lemma 10.1.1. *Siano $f(x)$ e $g(x)$ polinomi in $F[x]$, e $\alpha, \beta \in F$. Allora*

(1) $(\alpha f(x) + \beta g(x))' = \alpha f'(x) + \beta g'(x)$;

(2) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Dimostrazione. (1) Verifica immediata (esercizio).
(2) È sufficiente mostrare questo punto nel caso particolare $f(x) = x^i$ e $g(x) = x^j$, in virtù della (1). □

Bisogna prestare attenzione al caso in cui F è un campo a caratteristica finita. Prendiamo ad esempio un campo a caratteristica p e i polinomi in $\mathbb{Z}_p[x]$. La derivata del polinomio x^p è

$$px^{p-1} = 0$$

perché p è la caratteristica del campo.

La derivata viene introdotta a questo punto perché entra in gioco in un criterio utile per stabilire se un polinomio ha radici multiple.

Lemma 10.1.2. *Sia $f(x) \in F[x]$, con F campo. Se $f(x)$ ha fattori (non invertibili) multipli in $F[x]$ allora il grado di $MCD(f(x), f'(x))$ è maggiore o uguale a 1.*

Dimostrazione. Senza perdere di generalità possiamo supporre che $f(x)$ abbia un fattore non banale di molteplicità due, ossia abbiamo $f(x) = g_1^2(x)f_1(x)$. Consideriamo la sua derivata e calcoliamola grazie al lemma 10.1.1:

$$f'(x) = (g_1^2(x))' \cdot f_1(x) + g_1^2(x)f_1'(x) = g_1(x)\left(2f_1(x)g_1'(x) + g_1(x)f_1'(x)\right).$$

Questo calcolo mostra che $g_1(x)$ è un fattore sia di $f(x)$ che di $f'(x)$, e quindi abbiamo che $f(x)$ e $f'(x)$ hanno massimo comun divisore di grado maggiore o uguale a 1.□

Teorema 10.1.1. *Sia $f(x) \in F[x]$, con F campo. Il polinomio $f(x)$ non ha fattori multipli in un campo di spezzamento $E \supseteq F$ di $f(x)$ se e solo se $MCD(f(x), f'(x)) = 1$.* [1]

Dimostrazione. Sia E il campo di spezzamento di $f(x)$ su F; se in E si ha che $f(x)$ non ha fattori multipli avremo

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i),$$

con $\alpha_i \neq \alpha_j$ per ogni $i \neq j$. Calcolando in E la derivata di $f(x)$ abbiamo che

$$f'(x) = \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (x - \alpha_j),$$

da cui $f'(\alpha_k) \neq 0$ per ogni $k = 1, \ldots, n$ [2]. Questo mostra che $f(x)$ e $f'(x)$, in E, non hanno fattori in comune. D'altra parte, un fattore comune in $F[x]$ sarebbe un fattore comune anche in $E[x]$, quindi $f(x)$ e $f'(x)$ non possono avere fattori in comune in $F[x]$.

[1] Questo massimo comun divisore è fatto in $F[x]$, comunque segue subito (per es. usando il Lemma di Bezout) che $MCD(f(x), f'(x)) = 1$ in $K[x]$ con K una qualunque estensione di F.

[2] Infatti $f'(\alpha_k) = \prod_{\substack{j=1 \\ j\neq k}}^{n} (\alpha_k - \alpha_j) \neq 0$ in quanto gli α_i sono tutti distinti.

Per l'altra implicazione si applica il lemma precedente. Infatti, se $f(x)$ ha fattori multipli in $E[x]$ allora per il lemma vale che, in $E[x]$, $MCD(f(x), f'(x))$ ha grado maggiore o uguale a 1. Ma allora anche in $F[x]$ deve valere che $MCD(f(x), f'(x))$ ha grado maggiore o uguale a 1, ossia $MCD(f(x), f'(x)) \neq 1$. Infatti, come abbiamo osservato in una nota all'enunciato, se fosse $MCD(f(x), f'(x)) = 1$ in $F[x]$ allora per Bezout avremmo $MCD(f(x), f'(x)) = 1$ anche in $E[x]$, assurdo.

10.2 Polinomi ed elementi separabili

Definizione 10.2.1. Sia F un campo. Un polinomio irriducibile $g(x) \in F[x]$ si dice *separabile* se la derivata $g'(x)$ è non nulla. Un polinomio $f(x) \in F[x]$ si dice *separabile* se è prodotto di irriducibili separabili.

Osservazione 10.2.1. Osserviamo che se F è a caratteristica 0 allora ogni polinomio di grado maggiore di zero è separabile. Infatti dato $g(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ irriducibile si ha $g'(x) = nx^{n-1} + \sum_{i=0}^{n} i a_i x^{i-1}$ e quindi è non nullo.

Osservazione 10.2.2. Se $g(x) \in F[x]$ è irriducibile separabile allora non ha radici multiple in un campo di spezzamento. Infatti essendo irriducibile si ha che $MCD(g(x),\, g'(x))$ o è $g(x)$ o è 1 (a meno di associati); ma, visto che $g(x)$ è separabile, $g'(x)$ è non nullo e ha grado minore di $g(x)$ e quindi $MCD(g(x),\, g'(x)) = 1$. Si conclude applicando il Teorema 10.1.2.

Proposizione 10.2.1. *Sia $F \subseteq E$ un'estensione di F. Se $f(x) \in F[x]$ si spezza in E come $f(x) = \prod_{i=1}^{n}(x - a_i)$ con $a_i \in E$ e $a_i \neq a_j$ per $i \neq j$ allora $f(x)$ è un polinomio separabile.*

Dimostrazione. Sia $g(x)$ un fattore irriducibile di $f(x)$: essendo $g(x) \mid f(x)$ si ha che, in $E[x]$, $g(x) = \prod_{j \in I}(x - a_j)$, con $\emptyset \subsetneq I \subseteq \{1, \ldots, n\}$. Osserviamo che $g'(a_k) \neq 0$ per ogni $k \in I$, e quindi $g'(x)$ non può essere il polinomio nullo. Dunque $g(x)$ è irriducibile separabile e quindi $f(x)$ è separabile per definizione. □

Proposizione 10.2.2. *Sia $g(x) \in F[x]$ irriducibile e separabile, e sia E un campo di spezzamento di $g(x)$ su F. Sia $a \in E$ una radice di $g(x)$. Allora*

$$|\{\phi : F(a) \to E \text{ omomorfismo} \mid \phi|_F = id_F\}| = [F(a) : F].$$

Dimostrazione. Il polinomio $g(x)$, essendo separabile, ha tutte le radici distinte, e sono in numero di $\deg g(x)$. Per il Teorema 12.8 delle dispense di Aritmetica sappiamo che, se $a, b \in E$ sono due radici distinte di g allora esiste un unico isomorfismo $F(a) \cong F(b)$ che manda a in b, e quindi ci sono almeno $\deg g$ omomorfismi da $F(a)$ in E. Ma un omomorfismo $\phi : F(a) \to E$ è del tipo descritto:

infatti lascia fisso il polinomio $g(x)$ perché non ne altera i coefficienti e quindi deve mandare a in una radice di $g(x)$. Quindi ci sono esattamente $\deg g = [F(a) : F]$ omomorfismi. □

Corollario 10.2.1. *Sia $g(x) \in F[x]$ irriducibile e separabile, e sia E un campo di spezzamento di $g(x)$ su F. Sia $a \in E$ una radice di $g(x)$ e sia $k \in F(a) - F$. Allora esiste $\tau : F(a) \to E$ con $\tau|_F = id$ e $\tau(k) \neq k$.*

Dimostrazione. Consideriamo la torre $F \subseteq F(k) \subseteq F(a)$. Ora, a è radice di $g(x)$ su F, ma sarà anche radice di un polinomio $q(x) \in F(k)[x]$ irriducibile. Siccome $q(x) \mid g(x)$ in $F(k)[x]$ segue che $q(x)$ si fattorizza come prodotto di fattori lineari in $E[x]$ e non ha radici multiple. Dunque $q(x)$ è separabile. Per la proposizione precedente si ha

$$N = \left|\{\phi : F(a) \to E \text{ omomorfismo} \mid \phi|_{F(k)} = id\}\right| = [F(a) : F(k)].$$

Se per assurdo per ogni $\tau : F(a) \to E$ che lascia fisso F si avesse $\tau(k) = k$ allora gli insiemi $\{\phi : F(a) \to E \text{ omomorfismo} \mid \phi|_{F(k)} = id\}$ e $\{\phi : F(a) \to E \text{ omomorfismo} \mid \phi|_F = id\}$ coinciderebbero, e dunque $N = [F(a) : F]$. Ma allora

$$[F(a) : F(k)] = N = [F(a) : F] = [F(a) : F(k)][F(k) : F],$$

e dunque $[F(k) : F] = 1$, ossia $k \in F$, assurdo. □

Corollario 10.2.2. *Sia $E \supsetneq F$ il campo di spezzamento di un polinomio separabile $g(x) \in F[x]$. Sia $a \in E - F$. Allora esiste $\tau : E \to E$ automorfismo tale che $\tau(a) \neq a$ e $\tau|_F = id$.*

Dimostrazione. Possiamo scrivere $E = F(a_1, \ldots, a_t)$, dove $a_1, a_2, \ldots, a_t$ sono le radici di $g(x)$ in E. Dovrà essere, per qualche $1 \leq i \leq n$, che $a \notin F(a_1, \ldots, a_{i-1})$ ma $a \in F(a_1, \ldots, a_i)$, ossia

$$a \in F(a_1, \ldots, a_{i-1})(a_i) - F(a_1, \ldots, a_{i-1})$$

Sia $g_i(x)$ il polinomio irriducibile di a_i su $F(a_1, \ldots, a_{i-1})$ e sia $L \subseteq E$ il campo di spezzamento di $g_i(x)$ su $F(a_1, \ldots, a_{i-1})$. Essendo $g_i(x)$ separabile (perché $g_i(x) \mid g(x)$, dunque non ha radici multiple in L), esiste $\tau' : F(a_1, \ldots, a_{i-1})(a_i) \to L$ con $\tau'(a) \neq a$ per il Corollario 10.2.1. Osserviamo che in particolare τ' soddisfa $\tau'|_F = id$. Grazie al Teorema 14.10 delle dispense di Aritmetica, di estensione sui campi di spezzamento, a questo punto possiamo costruire un isomorfismo di E su E la cui restrizione a $F(a_1, \ldots, a_{i-1}, a_i)$ coincide con τ'. □

Definizione 10.2.2. Sia $F \subseteq E$ un'estensione di campi. Un elemento $a \in E$ è *separabile* su F se è algebrico su F e se il suo polinomio minimo su F è separabile.

Osservazione 10.2.3. Se il campo F è a caratteristica 0 allora ogni elemento algebrico su F è separabile: infatti ogni polinomio, e quindi il polinomio irriducibile dell'elemento, è separabile.

Teorema 10.2.1 (dell'elemento primitivo)**.** *Sia $F \subseteq E$ un'estensione finita di campi, e sia $E = F(\alpha, \beta_1, \ldots, \beta_n)$ con i β_i separabili su F. Allora esiste $\delta \in E$ tale che $E = F(\delta)$.*

Dimostrazione. Se F è un campo finito allora E è un campo finito. Sappiamo che E^* è ciclico[3], e quindi $E^* = (\gamma)$ per un certo γ. Ma allora $E = F(\gamma)$.
Supponiamo adesso F infinito: osserviamo che basta dimostrare l'enunciato per $n = 1$, poi la tesi generale segue per induzione. Sia dunque $E = F(\alpha, \beta)$, con α algebrico su F e β separabile. Siano $f(x)$ e $g(x)$ in $F[x]$ i polinomi irriducibili di α e β su F, e sia $\tilde{E}$ il campo di spezzamento di $f(x)g(x)$ su F che contiene E (lo possiamo costruire a partire da E aggiungendo le altre radici del polinomio prodotto). In $\tilde{E}[x]$ vale

$$f(x) = \prod_{i=1}^{\deg f} (x - a_i) \quad \text{e} \quad g(x) = \prod_{k=1}^{\deg g} (x - b_k),$$

e diciamo $a_1 = \alpha$ e $b_1 = \beta$. Inoltre, visto che β è separabile allora i b_k sono distinti a due a due. Consideriamo adesso l'equazione

$$a_i + xb_k = \alpha + x\beta.$$

Osserviamo che se $k \neq 1$ allora, per ogni i, l'equazione ha una sola soluzione, che è

$$x = \frac{a_i - \alpha}{\beta - b_k}$$

Essendo F infinito possiamo quindi trovare un $r \in F$ tale che $a_i + rb_k \neq \alpha + r\beta$ per ogni $k \neq 1$ e per ogni i. Affermiamo che, detto $\delta = \alpha + r\beta$, si ha $F(\delta) = F(\alpha, \beta)$. Essendo $\delta \in F(\alpha, \beta)$ si ha dunque $F(\delta) \subseteq F(\alpha, \beta)$; adesso mostriamo che $\alpha, \beta \in F(\delta)$, da cui seguirà l'altra inclusione che ci serve.
Ora, β è radice del polinomio $g(x)$, ed inoltre vale $f(\delta - r\beta) = f(\alpha) = 0$. Dunque $g(x)$ e $f(\delta - rx)$ hanno $x - \beta$ come fattore comune in $\tilde{E}[x]$, ed anzi affermiamo che questo è proprio il loro massimo comun divisore in $\tilde{E}[x]$. Presa infatti un'altra radice $b_k \neq \beta$ di $g(x)$, allora $f(\delta - rb_k) \neq 0$ in quanto, per la scelta di r, tra

[3] Lo avete dimostrato nel corso di Aritmetica, comunque daremo alla fine di questo capitolo, nel Paragrafo 10.3.1, una seconda dimostrazione.

i $\delta - rb_k$ non compare alcun a_i radice di $f(x)$; inoltre $(x-\beta)^2 \nmid g(x)$ e quindi il massimo comun divisore in $\tilde{E}[x]$ è proprio $x-\beta$. Ma allora i due polinomi hanno un massimo comun divisore non costante su $F(\delta)[x]$ (se fossero primi fra loro in $F(\delta)[x]$ lo sarebbero anche in $\tilde{E}[x]$ - si vede per esempio usando Bezout), e questo deve essere un divisore di $x-\beta$: dunque tale massimo comun divisore sarà $c_0 + c_1 x \in F(\delta)[x]$. Inoltre tale massimo comun divisore differisce solo per moltiplicazione per un elemento di $\tilde{E}^*$ da $x-\beta$, dunque valutato in β deve essere nullo, pertanto

$$\beta = -\frac{c_0}{c_1} \in F(\delta).$$

Infine osserviamo che $\alpha = \delta - r\beta \in F(\delta)$. $\square$

Una estensione di un campo F del tipo $F(\gamma)$, ossia ottenuta 'aggiungendo' un solo elemento si chiama *estensione semplice*. Il seguente corollario è di immediata dimostrazione:

Corollario 10.2.3. *Ogni estensione finita di un campo F a caratteristica 0 è una estensione semplice.*

10.3 Prime nozioni della teoria di Galois

Definizione 10.3.1. Sia $F \subseteq E$ un'estensione di campi e denotiamo con $\mathrm{Aut}(E/F)$ l'insieme degli automorfismi ϕ di E che lasciano fisso F punto a punto (ossia $\phi|_F = id$).

È immediato dimostrare che $\mathrm{Aut}(E/F)$ è un gruppo con la composizione di applicazioni. Poniamo

$$E' = \{h \in E \mid \phi(h) = h,\ \forall \phi \in \mathrm{Aut}(E/F)\}.$$

Non è difficile vedere che E' è un campo. Ovviamente vale $F \subseteq E' \subseteq E$.

Definizione 10.3.2. Il campo E' è detto *campo fisso* di $\mathrm{Aut}(E/F)$.

Mostriamo due esempi: nel primo $E' = F$, nel secondo $E' = E$.

Esempio 10.3.1. Consideriamo $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$, sappiamo che $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$. Cerchiamo gli automorfismi di $\mathbb{Q}(\sqrt{2})$ che lasciano fisso $\mathbb{Q}$: tali automorfismi lasceranno fisso x^2-2 e dunque devono mandare $\sqrt{2}$ in un'altra radice di x^2-2. Quindi abbiamo due possibilità: o l'automorfismo è l'identità, oppure l'automorfismo è quello che fissa $\mathbb{Q}$ e che porta $\sqrt{2}$ in $-\sqrt{2}$ (sappiamo che esiste per il Teorema 12.8 delle dispense di Aritmetica). Dunque $\mathbb{Q}(\sqrt{2})' = \mathbb{Q}$.

Esempio 10.3.2. Prendiamo $\mathbb{Q}(\sqrt[3]{2})$. Essendo tale campo isomorfo a $\mathbb{Q}[x]/(x^3-2)$ si ha che un elemento generico del campo è $\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2$ con $\alpha_i \in \mathbb{Q}$ (questo equivale a dire che 1, $\sqrt[3]{2}$,$(\sqrt[3]{2})^2$ è una base di $\mathbb{Q}(\sqrt[3]{2})$ su $\mathbb{Q}$). Sia $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$: argomentando come prima si ha che $\tau(\sqrt[3]{2})$ deve essere una radice di x^3-2 (in quanto questo polinomio è lasciato fisso da τ). Quindi necessariamente $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, essendo le altre due radici in $\mathbb{C}$ dei numeri complessi non reali, e allora $\tau = id$. Dunque $\mathbb{Q}(\sqrt[3]{2})' = \mathbb{Q}(\sqrt[3]{2})$.

Definizione 10.3.3. Un'estensione $F \subseteq E$ si dice *estensione di Galois*[4] se E è finita su F [5] e se il campo fisso è F. In tal caso $\mathrm{Aut}(E/F)$ si chiama *gruppo di Galois* dell'estensione.

L'idea che ci accompagnerà fino agli ultimi risultati che presenteremo qui sulla teoria di Galois sarà quella di far corrispondere sottocampi delle estensioni di Galois con dei sottogruppi del gruppo di Galois dell'estensione.

Proposizione 10.3.1. *Sia $F \subseteq E$ estensione finita. Allora* $\mathrm{Aut}(E/F)$ *è finito.*

Dimostrazione. Siccome E è finita avremo che sarà $F(a_1, \ldots, a_n)$ per certi a_i algebrici su F. Sia $\phi \in \mathrm{Aut}(E/F)$: lasciando fisso F esso è determinato univocamente dalle immagini degli a_i. Sia $p_i(x)$ il polinomio irriducibile di a_i su F: ϕ dovrà mandare a_i in una radice di $p_i(x)$, ma le radici di $p_i(x)$ sono finite. □

Teorema 10.3.1. *Sia $F \subseteq E$ estensione di Galois. Allora ogni elemento $a \in E$ è radice di un polinomio irriducibile e separabile $f(x) \in F[x]$. Inoltre E contiene un campo di spezzamento di $f(x)$.*

Dimostrazione. Sia $\mathscr{O}$ l'orbita di $a \in E$ sotto l'azione di $\mathrm{Aut}(E/F)$. Definiamo il polinomio

$$f(x) = \prod_{\gamma \in \mathscr{O}} (x - \gamma) \in E[x].$$

Osserviamo che $f(x)$ viene lasciato fisso da qualsiasi automorfismo in $\mathrm{Aut}(E/F)$; infatti preso $\sigma \in \mathrm{Aut}(E/F)$ si ha

$$\tilde{\sigma}(f(x)) = \prod_{\gamma \in \mathscr{O}} (x - \sigma(\gamma)) = f(x)$$

in quanto σ compie solo una permutazione degli elementi dell'orbita $\mathscr{O}$.[6] Adesso vogliamo dire di più. Sia $f(x) = \sum_{i=0}^{r} b_i x^i$ con $b_i \in E$: per quanto osservato

[4] Évariste Galois, 1811-1832, matematico francese.

[5] Non è la definizione più generale possibile: adottiamo nel corso questa condizione di finitezza e dunque considereremo solo estensioni di Galois finite.

[6] Anche in queste dispense, come in quelle di Aritmetica, usiamo la seguente notazione: quando abbiamo un isomorfismo $\phi : A \to A'$ fra due anelli, chiameremo $\tilde{\phi}$ l'isomorfismo indotto fra i

$\sigma(b_i) = b_i$ per ogni i e per ogni $\sigma \in \mathrm{Aut}(E/F)$. Dunque $b_i \in F$ per ogni i, in quanto l'estensione è di Galois. Quindi $f(x) \in F[x]$.
Ora dobbiamo mostrare che $f(x)$ ha le proprietà richieste. Intanto $f(x)$ è separabile per costruzione in quanto ha tutte le radici distinte (vedi Proposizione 10.2.1). Adesso dobbiamo mostrare che $f(x)$ è irriducibile in $F[x]$: supponiamo che $f(x) = f_1(x)f_2(x)$ con $f_1(x), f_2(x) \in F[x]$. L'elemento a è radice di $f(x)$ per costruzione, quindi supponiamo senza perdere di generalità che $f_1(a) = 0$. Avendo $f_1(x)$ i coefficienti in F si ha che, per ogni $\sigma \in \mathrm{Aut}(E/F)$,

$$\tilde{\sigma}(f_1(x)) = f_1(x).$$

Ma allora $\sigma(a)$, che è radice di $\tilde{\sigma}(f_1(x))$, è radice di $f_1(x)$. Siccome questo vale per ogni $\sigma \in \mathrm{Aut}(E/F)$, otteniamo che ogni $\gamma \in \mathscr{O}$ è radice di $f_1(x)$. Ma allora $f_1(x)$ ha tutte le radici di $f(x)$, ossia $f_1(x) = kf(x)$ con $k \in F$, e quindi $f_2(x)$ ha grado 0 ed è invertibile. Da questo si conclude che $f(x)$ è irriducibile. □

Siamo in grado adesso di dare una caratterizzazione delle estensioni di Galois:

Teorema 10.3.2. *Sia $F \subseteq E$ un'estensione di campi. L'estensione è di Galois se e solo se E è il campo di spezzamento su F di un polinomio di $F[x]$ separabile.*

Dimostrazione. ($\Longrightarrow$) Sia $F \subseteq E$ un'estensione di Galois. Essendo E un'estensione finita di F avremo che sarà della forma $E = F(a_1, \ldots, a_n)$ per certi a_i algebrici su F. Per il Teorema 10.3.1 sappiamo che tutti gli a_i sono separabili. Dunque possiamo applicare il teorema dell'elemento primitivo, e concludere che $E = F(\gamma)$, per un certo γ che, sempre in virtù del Teorema 10.3.1, è separabile. Costruiamo ora il polinomio irriducibile $g(x)$ di γ su F, creato come nella dimostrazione precedente. Tale polinomio è separabile e, come sappiamo dal Teorema 10.3.1, E contiene un suo campo di spezzamento K. Poichè però $E = F(\gamma) \subseteq K \subseteq E$ si conclude subito che E coincide con K.
($\Longleftarrow$) Sia E campo di spezzamento di un polinomio separabile su $F[x]$. Si osserva subito che $[E : F]$ è finito; studiamo il campo fisso E' di $\mathrm{Aut}(E/F)$ e mostriamo che $E' = F$. Preso $a \in E - F$, per il Corollario 10.2.2, esiste un automorfismo di $\mathrm{Aut}(E/F)$ che non lo lascia fisso: dunque il campo fisso coincide con F, e l'estensione è di Galois. □

Corollario 10.3.1. *Se $F \subseteq E$ è un'estensione di Galois e L è un'estensione di E allora ogni $\sigma \in \mathrm{Aut}(L/F)$ manda E in E.*

---

corrispondenti anelli di polinomi $A[x]$, $A'[x]$:

$$\begin{array}{rccc} \tilde{\phi}: & A[x] & \longrightarrow & A'[x] \\ & \sum_{i=0}^{n} a_i x^i & \longmapsto & \sum_{i=0}^{n} \phi(a_i) x^i \end{array}$$

Dimostrazione. Intanto, come nella dimostrazione precedente, si osserva che $E = F(\gamma)$, con γ radice del polinomio separabile $g(x)$ di cui E è campo di spezzamento su F. Sia ora $\sigma \in \mathrm{Aut}(L/F)$: ovviamente σ lascia fisso F, ma allora $\tilde{\sigma}$ lascia fisso il polinomio $g(x)$. Dunque $\sigma(\gamma)$ deve essere una radice di $g(x)$, in particolare appartiene a E. Si conclude che E viene mandato in se stesso. □

Abbiamo già detto che se E è un estensione finita di F allora il gruppo $\mathrm{Aut}(E/F)$ è finito. Se in particolare l'estensione è di Galois, caso che a noi interessa particolarmente, si può dire esattamente quanti elementi ha $\mathrm{Aut}(E/F)$.

Corollario 10.3.2. *Sia $F \subseteq E$ un'estensione di Galois. Allora*

$$|\mathrm{Aut}(E/F)| = [E : F].$$

Dimostrazione. Come sopra si osserva che $E = F(\gamma)$, con γ radice del polinomio separabile $g(x)$ di cui E è campo di spezzamento su F. Osserviamo che:

$$[E : F] = [F(\gamma) : F] = |\{\phi : F(\gamma) \to E \text{ omomorfismo } | \ \phi|_F = id\}| = |\mathrm{Aut}(E/F)|,$$

con la seconda uguaglianza giustificata dalla Proposizione 10.2.2, in quanto E è il campo di spezzamento di $g(x)$. □

Esempio 10.3.3 (caratterizzazione delle estensioni quadratiche su campi con caratteristica diversa da 2)**.** Sia $a \in F$ un non quadrato: ossia, per ogni $b \in F$ si ha $b^2 \neq a$. Questo significa che il polinomio $f(x) = x^2 - a$ è irriducibile in $F[x]$. Osserviamo che la derivata formale di $f(x)$ è $f'(x) = 2x$: quindi se la caratteristica di F non è 2 allora tale derivata è non nulla e $x^2 - a$ è separabile. Allora $E = F[x]/(x^2 - a)$ su F è un'estensione di Galois, in quanto E è il campo di spezzamento di un polinomio separabile su $F[x]$. Il gruppo di Galois dell'estensione ha due elementi e quindi

$$\mathrm{Aut}(E/F) \cong \mathbb{Z}_2.$$

Viceversa, sia E un'estensione di F di grado 2, allora $E = F(\beta)$ con $\beta \in E$ che soddisfa un polinomio di grado due $f(x) = x^2 + \gamma_1 x + \gamma_0$ irriducibile su $F[x]$. Visto che $f(x)$ si fattorizza in $E[x]$, E contiene anche l'altra radice di $f(x)$, dunque è un campo di spezzamento di $f(x)$. Allora l'estensione $F \subset E$ è di Galois.

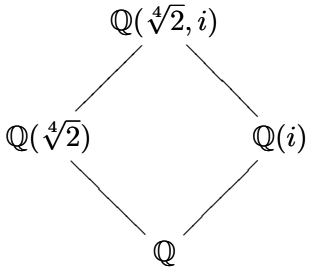
Osserviamo che con il cambiamento di variabile $x \leftarrow x - \frac{\gamma_1}{2}$ si ottiene

$$f\left(x - \frac{\gamma_1}{2}\right) = \left(x - \frac{\gamma_1}{2}\right)^2 + \gamma_1\left(x - \frac{\gamma_1}{2}\right) + \gamma_0 = x^2 - \left(\frac{\gamma_1^2}{4} - \gamma_0\right)$$

e quindi $\alpha = \beta + \frac{\gamma_1}{2}$ soddisfa $x^2 - \left(\frac{\gamma_1^2}{4} - \gamma_0\right) = 0$. Ma allora possiamo scrivere

$$E = F(\beta) = F\left(\beta + \frac{\gamma_1}{2}\right) \cong F[x]/\left(x^2 - \left(\frac{\gamma_1^2}{4} - \gamma_0\right)\right).$$

Esempio 10.3.4. Sia $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, e sia E il suo campo di spezzamento su $\mathbb{Q}$. Ci chiediamo se l'estensione $\mathbb{Q} \subseteq E$ è di Galois e, in caso affermativo, vogliamo calcolarne il gruppo di Galois.
Intanto il polinomio è separabile, in quanto la caratteristica del campo è 0; quindi $E = \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$ è di Galois perché è il campo di spezzamento di un polinomio separabile. La situazione è la seguente:



Calcoliamo il grado dell'estensione:

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8,$$

dove il primo grado da sinistra è 2 in quanto x^2+1 è irriducibile su $\mathbb{Q}(\sqrt[4]{2})$ visto che $i \notin \mathbb{Q}(\sqrt[4]{2})$, mentre il secondo grado è 4 in quanto $x^4 - 2$ è irriducibile in $\mathbb{Q}[x]$ (si può vedere in vari modi, fra cui il criterio di Eisenstein). Quindi il gruppo di Galois è un gruppo di ordine 8; adesso vogliamo esplicitarne la struttura. Osservando lo schema di sopra deve essere

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4$$

e quindi x^4-2 è irriducibile su $\mathbb{Q}(i)$. Sia $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(i)) \subseteq \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ tale che $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ (una tale σ esiste per il Teorema 12.8 delle dispense di Aritmetica, tenendo presente che $\mathbb{Q}(i)(\sqrt[4]{2}) = \mathbb{Q}(i)(\sqrt[4]{2}i)$). Sia inoltre $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(\sqrt[4]{2})) \subseteq \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ tale che $\tau(i) = -i$ (come sopra, una tale τ esiste per il Teorema 12.8 delle dispense di Aritmetica). Osserviamo che σ ha ordine 4 e τ ha ordine 2, quindi $\langle\sigma\rangle \cong \mathbb{Z}_4$ e $\langle\tau\rangle \cong \mathbb{Z}_2$. Essendo $\langle\sigma\rangle$ normale perché ha indice 2 ed essendo $\langle\sigma\rangle \cap \langle\tau\rangle = \{e\}$ (un elemento che appartiene ad entrambi i sottogruppi deve fissare sia i sia $\sqrt[4]{2}$ dunque è l'identità) si ha che il gruppo di Galois è un prodotto semidiretto $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$: le due possibilità sono un gruppo abeliano o il gruppo diedrale. Si verifica che $\tau\sigma = \sigma^{-1}\tau$ e che quindi il gruppo di Galois è D_4.

10.3.1 Complementi: sul teorema, visto già ad Aritmetica, dell'elemento primitivo di un sottogruppo moltiplicativo di un campo

Come avete visto nel corso di Aritmetica, il sottogruppo moltiplicativo di un campo finito è ciclico. Ridimostriamo e generalizziamo questo risultato, utilizzando alcuni risultati studiati nel corso di Algebra 1.

Teorema 10.3.3. *Sia F un campo e G un sottogruppo finito del gruppo moltiplicativo di F. Allora G è ciclico.*

Dimostrazione. Essendo G sottogruppo finito di un campo abbiamo che G è un gruppo abeliano finito, dunque

$$G \cong \prod_{i=1}^{k} N_{p_i},$$

ossia G è il prodotto delle sue parti di p_i–torsione, che coincidono con i p_i sottogruppi di Sylow. Se dimostriamo che per ogni i si ha che N_{p_i} è ciclico abbiamo concluso. Intanto sappiamo dal teorema di struttura per i gruppi abeliani finiti che

$$N_{p_i} \cong \mathbb{Z}_{p_i^{a_1}} \times \mathbb{Z}_{p_i^{a_2}} \times \cdots \times \mathbb{Z}_{p_i^{a_n}},$$

con $0 < a_1 \leq a_2 \leq \cdots \leq a_n$, e affermiamo che c'è una sola componente, la $\mathbb{Z}_{p_1^{a_1}}$. Se per assurdo ci fosse anche la componente $\mathbb{Z}_{p_i^{a_2}}$ troveremmo in G un sottogruppo isomorfo a $\mathbb{Z}_{p_i} \times \mathbb{Z}_{p_i}$. Dunque avremmo almeno p_i^2 radici del polinomio $x^{p_i} - 1$, e questo contraddirrebbe il fatto che un polinomio di grado n a coefficienti in un campo ha al più n radici nel campo. □

10.4 Esercizi

Molti di questi esercizi sono di ripasso...

Esercizio 10.4.1. Dare un esempio di un polinomio irriducibile non separabile.

Esercizio 10.4.2. Sia $\alpha = \sqrt{2 + i\sqrt{2}}$. Determinare il polinomio minimo di α e di $\alpha^2 + 1$ sul campo $\mathbb{Q}$.

Esercizio 10.4.3. Determinare il polinomio minimo di $\alpha = 1 + \sqrt{3}$ su $\mathbb{Q}$.

Esercizio 10.4.4. Determinare il polinomio minimo di ζ_5 su $\mathbb{Q}(i)$.

Esercizio 10.4.5. Sia $\alpha = \sqrt{2 + \sqrt{3}}$. Determinare il polinomio minimo di α e su $\mathbb{Q}$ e il grado del suo campo di spezzamento.

Esercizio 10.4.6. Si consideri il polinomio $x^3 - 3x - 1$ in $\mathbb{Q}[x]$. Si dimostri che è irriducibile in $\mathbb{Q}[x]$ e in $\mathbb{Q}(i)[x]$.

Esercizio 10.4.7. Sia L/K una estensione di campi finita di grado n e sia $f(x) \in K[x]$ irriducibile di grado m. Dimostrare che se n e m sono primi fra loro allora $f(x)$ è irriducibile in $L[x]$.

Esercizio 10.4.8. I due campi $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ sono isomorfi?

Esercizio 10.4.9. È vero o falso che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Esercizio 10.4.10. Sia K il campo di spezzamento del polinomio $X^4 - 6X^2 + 25 \in \mathbb{Q}[X]$ (dunque l'estensione $\mathbb{Q} \subset K$ è di Galois). Calcolare il gruppo di Galois $Aut(K/\mathbb{Q})$.

Capitolo 11

La corrispondenza di Galois (lezioni del 22 e 25 novembre)

11.1 Il teorema di corrispondenza

Presenteremo la "corrispondenza di Galois" tra campi intermedi di un'estensione di Galois e i sottogruppi del gruppo di Galois.

Proposizione 11.1.1. *Sia $F \subseteq E$ un'estensione di Galois. Se H è un sottogruppo di $\mathrm{Aut}(E/F)$ tale che il suo campo fisso $\{a \in E \mid h(a) = a \ \forall h \in H\}$ coincide con F allora $H = \mathrm{Aut}(E/F)$.*

Dimostrazione. Si ha $E = F(a_1, \ldots, a_n)$, dove le a_i sono le radici del polinomio separabile si cui E è campo di spezzamento. Per il teorema dell'elemento primitivo si ha che $E = F(\delta)$. Consideriamo l'orbita $\mathscr{O}$ di δ sotto l'azione di H e costruiamo dunque

$$f(x) = \prod_{\gamma \in \mathscr{O}} (x - \gamma).$$

Ripetendendo il ragionamento della dimostrazione del Teorema 10.3.1 si ha che $f(x)$ è un polinomio a coefficienti in F, separabile e irriducibile in $F[x]$. Dunque $f(x) \in F[x]$ è il polinomio irriducibile di δ. Allora segue che

$$|H| \geq |\mathscr{O}| = \deg f(x) = [E : F] = |\mathrm{Aut}(E/F)|,$$

ma H è un sottogruppo di $\mathrm{Aut}(E/F)$ e dunque si deve avere l'uguaglianza. □

Sia $F \subseteq E$ un'estensione di Galois; vogliamo associare ai campi K tali che $F \subseteq K \subseteq E$ un sottogruppo del gruppo di Galois dell'estensione. Per semplificare le notazioni scriviamo $\mathcal{C} = \{K \text{ campi} \mid F \subseteq K \subseteq E\}$ e $\mathcal{S} = \{G \mid G < \mathrm{Aut}(E/F)\}$.

Definiamo le seguenti due mappe:

$$\begin{array}{rccc} i: & \mathcal{C} & \longrightarrow & \mathcal{S} \\ & K & \longmapsto & \mathrm{Aut}(E/K) \end{array} \quad \text{e} \quad \begin{array}{rccc} j: & \mathcal{S} & \longrightarrow & \mathcal{C} \\ & G & \longmapsto & \{a \in E \mid g(a) = a \ \forall\, g \in G\} \end{array}.$$

La mappa i associa a K il sottogruppo $\mathrm{Aut}(E/K)$ di $\mathrm{Aut}(E/F)$ dato dagli automorfismi di E che lasciano fisso K; la mappa j, invece, associa a G il proprio campo fisso.

Osservazione 11.1.1. **Se $F \subseteq E$ è un'estensione di Galois e $F \subseteq K \subseteq E$ allora anche $K \subseteq E$ è un'estensione di Galois. Infatti E è il campo di spezzamento di un polinomio separabile in $F[x]$, ma allora E sarà anche il campo di spezzamento dello stesso polinomio ma considerato a coefficienti in K (il polinomio rimane separabile, verificate di saper spiegare perchè).**

Teorema 11.1.1 (primo teorema di Galois)**.** *Le mappe i e j sono una l'inversa dell'altra.*

Dimostrazione. Intanto per l'osservazione 11.1.1 si ha che $K \subseteq E$ è un'estensione di Galois; vogliamo mostrare che $j(i(K)) = K$. Basta osservare che

$$j(i(K)) = j(\mathrm{Aut}(E/K)) = K$$

perché $\mathrm{Aut}(E/K)$ ha come campo fisso proprio K, in quanto è di Galois. Adesso dobbiamo mostrare che $i(j(G)) = G$; per definizione

$$i(j(G)) = \mathrm{Aut}(E/j(G)).$$

Sempre per l'osservazione che precede il teorema l'estensione $j(G) \subseteq E$ è di Galois. Ora, G è un sottogruppo di $\mathrm{Aut}(E/j(G))$ e lascia fissi esattamente gli elementi di $j(G)$, e quindi per la Proposizione 11.1.1 $G = \mathrm{Aut}(E/j(G))$. □

Teorema 11.1.2 (secondo teorema di Galois)**.** *Sia $F \subseteq E$ un'estensione di Galois e sia $F \subseteq K \subseteq E$. Allora $F \subseteq K$ è di Galois se e solo se* $\mathrm{Aut}(E/K) \lhd \mathrm{Aut}(E/F)$. *In tale caso* $\mathrm{Aut}(E/F)/\mathrm{Aut}(E/K) \cong \mathrm{Aut}(K/F)$.

Dimostrazione. ($\Longrightarrow$) Sia $F \subseteq K$ estensione di Galois. Consideriamo

$$\begin{array}{rccc} \Phi: & \mathrm{Aut}(E/F) & \longrightarrow & \mathrm{Aut}(K/F) \\ & \psi & \longmapsto & \psi|_K. \end{array}$$

La mappa Φ è ben definita in quanto $\psi|_K$ è in effetti un automorfismo di K (segue dal Corollario 10.3.1). Inoltre è immediato vedere che Φ è un omomorfismo di gruppi. Per definizione $\ker \Phi = \mathrm{Aut}(E/K)$, in quanto sono gli automorfismi di E

che ristretti a K danno l'identità. Questo mostra che $\mathrm{Aut}(E/K)$ è un sottogruppo normale.
Mostriamo che Φ è surgettivo. Sia $\tau : K \to K$ un automorfismo di $\mathrm{Aut}(K/F)$. Dato che $F \subseteq E$ è un'estensione di Galois avremo che E è il campo di spezzamento di un polinomio separabile $g(x) \in F[x]$. Inoltre $\tilde{\tau}(g(x)) = g(x)$ e dunque sappiamo, per il Teorema 14.10 delle dispense di Aritmetica, che si può estendere τ ad un automorfismo di E, il quale lascerà fisso F. Dunque Φ è surgettivo e per il primo teorema di omomorfismo si conclude che

$$\mathrm{Aut}(E/F)/\mathrm{Aut}(E/K) \cong \mathrm{Aut}(K/F).$$

($\Longleftarrow$) Sia $\mathrm{Aut}(E/K)$ sottogruppo normale in $\mathrm{Aut}(E/F)$. Visto che $K \subseteq E$ è un'estensione di Galois si ha

$$K = \{a \in E \mid \sigma(a) = a \ \forall \sigma \in \mathrm{Aut}(E/K)\},$$

e per la normalità del sottogruppo possiamo anche scrivere, fissato $\psi \in \mathrm{Aut}(E/F)$

$$K = \{a \in E \mid \psi^{-1}\sigma\psi(a) = a \ \forall \sigma \in \mathrm{Aut}(E/K)\}.$$

Osserviamo che se $\psi(a) \in E - K$ allora esiste un σ in $\mathrm{Aut}(E/K)$ che non lo lascia fisso (Corollario 10.2.2), e quindi la sua controimmagine mediante ψ non può essere a. Ma allora possiamo anche riscrivere

$$K = \{a \in E \mid \psi(a) \in K\} = \psi^{-1}(K),$$

e dunque $\psi(K) = K$: questo ci dice che restringendo ψ a K otteniamo un automorfismo di K, e precisamente $\psi|_K \in \mathrm{Aut}(K/F)$. Adesso ci chiediamo chi è il campo fisso di $\mathrm{Aut}(K/F)$: se è F abbiamo concluso. Sia ora $k \in K$ un elemento lasciato fisso da tutti gli elementi di $\mathrm{Aut}(K/F)$, vediamo cosa succede se prendiamo però un automorfismo in $\mathrm{Aut}(E/F)$. Sia $\psi \in \mathrm{Aut}(E/F)$, allora $\psi|_K(k) = k$ poiché k è lasciato fisso da tutti gli automorfismi di $\mathrm{Aut}(K/F)$ e come sappiamo $\psi|_K \in \mathrm{Aut}(K/F)$. Quindi k è lasciato fisso anche da tutti gli elementi di $\mathrm{Aut}(E/F)$. Essendo $F \subseteq E$ un'estensione di Galois, segue che $k \in F$. Questo mostra che il campo fisso di $\mathrm{Aut}(K/F)$ è F stesso e che quindi $K \supseteq F$ è un'estensione di Galois. □

Il seguente teorema chiarisce che l'indice del sottogruppo $\mathrm{Aut}(E/K)$ di $\mathrm{Aut}(E/F)$ coincide con il grado dell'estensione $F \subseteq K$ (anche se il sottogruppo non è normale).

Teorema 11.1.3 (terzo teorema di Galois)**.** *Sia $F \subseteq E$ un'estensione di Galois. Se $F \subseteq K \subseteq E$ allora $|\mathrm{Aut}(E/K)| = [E : K]$ e $[K : F] = i_{\mathrm{Aut}(E/F)}(\mathrm{Aut}(E/K))$.*

Dimostrazione. La prima parte è vera perché $K \subseteq E$ è un'estensione di Galois e quindi avevamo già mostrato questo fatto. Per l'altra parte, infine, basta osservare che

$$|\mathrm{Aut}(E/F)| = [E : F] = [E : K][K : F] = |\mathrm{Aut}(E/K)| \cdot [K : F],$$

e concludere dividendo. □

11.2 Applicazione: teorema fondamentale dell'algebra

Teorema 11.2.1 (fondamentale dell'algebra)**.** *Ogni polinomio non costante a coefficienti complessi ammette una radice complessa.*

Dimostrazione. Dimostrare il teorema equivale a dimostrare che $\mathbb{C} = \mathbb{R}(i)$ ammette estensioni finite solo di grado uno.
Cominciamo con l'osservare che ogni estensione finita di $\mathbb{R}(i)$ è contenuta in un'estensione più grande $E \supseteq \mathbb{R}(i)$ che è di Galois su $\mathbb{R}$. Sia infatti $\mathbb{R}(i) \subseteq L$ un'estensione finita, allora sarà

$$L = \mathbb{R}(i)(\alpha_1, \ldots, \alpha_n)$$

per certi α_i. Ma, per il teorema dell'elemento primitivo, $L = \mathbb{R}(\delta)$ in quanto tutti gli elementi aggiunti sono separabili (siamo in caratteristica 0). Sia dunque $f(x) \in \mathbb{R}[x]$ il polinomio irriducibile di δ su $\mathbb{R}$, e sia E un campo di spezzamento di $f(x)$ che contiene $L = \mathbb{R}(\delta)$. L'estensione E è di Galois su $\mathbb{R}$ perché è campo di spezzamento del polinomio separabile $f(x) \in \mathbb{R}[x]$. Inoltre E contiene $\mathbb{R}(i)$ (visto che $\mathbb{R}(i) \subseteq L$).
Bisogna dunque dimostrare che $E = \mathbb{R}(i)$ (così $L = \mathbb{R}(i)$ e abbiamo dimostrato che L ha grado uno). Sia $G = \mathrm{Aut}(E/\mathbb{R})$, allora

$$|G| = [E : \mathbb{R}] = [E : \mathbb{R}(i)][\mathbb{R}(i) : \mathbb{R}] = 2[E : \mathbb{R}(i)],$$

e quindi G ha ordine pari. Allora consideriamo N_2, un 2–Sylow di G, e, in base alla corrispondenza di Galois, consideriamo il campo fisso di N_2, che abbiamo indicato con $j(N_2)$. Si ha $E \supseteq j(N_2) \supseteq \mathbb{R}$ e quindi per i teoremi di Galois si ha

$$[j(N_2) : \mathbb{R}] = i_{\mathrm{Aut}(E/\mathbb{R})}(\mathrm{Aut}(E/j(N_2))) = i_{\mathrm{Aut}(E/\mathbb{R})}(N_2)$$

che è un numero dispari. Per il teorema dell'elemento primitivo $j(N_2) = \mathbb{R}(\alpha)$ e quindi α è radice di un polinomio irriducibile su $\mathbb{R}$ di grado dispari: allora questo polinomio deve avere grado uno, in quanto non ci sono polinomi irriducibili in $\mathbb{R}[x]$ di grado dispari e maggiore di uno [1]. Ma allora $\alpha \in \mathbb{R}$, dunque $\mathbb{R}(\alpha) = \mathbb{R}$ e quindi

[1] Stiamo usando il fatto che un polinomio a coefficienti in $\mathbb{R}$ di grado dispari ha sempre una radice reale. Assume infatti valori negativi per $x << 0$, positivi per $x >> 0$ ed è una funzione continua...

$j(N_2) = \mathbb{R}$. Da questo segue $N_2 = \mathrm{Aut}(E/\mathbb{R})$ (perchè dalla formula precedente si nota che N_2 ha indice 1 oppure potremmo applicare direttamente la Proposizione 11.1.1). Siamo arrivati a concludere che $\mathrm{Aut}(E/\mathbb{R})$ è un 2–gruppo, diciamo di ordine 2^n.
Sia $G_1 = \mathrm{Aut}(E/\mathbb{R}(i))$: essendo un sottogruppo di $\mathrm{Aut}(E/\mathbb{R})$ sarà un 2–gruppo e ci sono due possibilità. Se $G_1 = \{id\}$ allora

$$[E : \mathbb{R}(i)] = |\mathrm{Aut}(E/\mathbb{R}(i))| = 1$$

e abbiamo finito. Se invece $G_1 \neq \{e\}$, ricordiamo che, per il secondo teorema di Sylow, un 2–gruppo non banale ammette sempre un sottogruppo di indice 2. Prendiamo dunque $G_2 < G_1$ un sottogruppo di indice 2 e consideriamo il suo campo fisso $j(G_2)$. Ma

$$[j(G_2) : \mathbb{R}(i)] = 2$$

per il terzo teorema di Galois. Tale fatto è assurdo: infatti $j(G_2)$ sarebbe un'estensione di grado 2 di $\mathbb{R}(i)$, ma tali estensioni non esistono. Infatti implicherebbero l'esistenza di un polinomio a coefficienti complessi di grado 2 irriducibile, ossia senza radici complesse. La formula risolutiva per i polinomi di secondo grado ci garantisce invece che ci sono sempre radici complesse. □

11.3 Esercizi

Esercizio 11.3.1. Dimostrare che il campo di spezzamento su $\mathbb{Q}$ di $x^4 + 2x^3 - 8x^2 - 6x - 1$ è $\mathbb{Q}(\sqrt{3}, \sqrt{2}) = \mathbb{Q}(\sqrt{3} - \sqrt{2})$. Trovare il polinomio irriducibile di $\sqrt{3} - \sqrt{2}$ su $\mathbb{Q}(\sqrt{3})$.

Esercizio 11.3.2. Sia K il campo di spezzamento del polinomio $(X^4 - 2)(X^3 - 27) \in \mathbb{Q}[x]$ e sia G il suo gruppo di Galois su $\mathbb{Q}$. Calcolare $[K : \mathbb{Q}]$ e descrivere G.

Esercizio 11.3.3. Sia $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$. Dimostrare che $K \supseteq \mathbb{Q}$ è di Galois e determinare $\mathrm{Aut}(K/\mathbb{Q})$. Determinare inoltre tutti i campi F con $\mathbb{Q} \subseteq F \subseteq K$ tali che $[F : \mathbb{Q}] = 6$.

Esercizio 11.3.4. Studiare la struttura del campo di spezzamento E di $x^4 - 2$ su $\mathbb{Q}$ e stabilire la corrispondenza tra sottogruppi del gruppo di Galois e sottocampi di E.

Esercizio 11.3.5. Determinare il gruppo di Galois di $x^6 - 2x^4 - 8x^2 + 16$ su $\mathbb{Q}$, su $\mathbb{F}_3$ e su $\mathbb{F}_9$. In ciascuno dei tre casi elencare i campi intermedi fra il campo base e il campo di spezzamento.

Esercizio 11.3.6. Calcolare, al variare di $m \in \mathbb{Z}$, il gruppo di Galois del polinomio $(x^4+1)(x^2-m)$ su $\mathbb{Q}$.

Esercizio 11.3.7. Sia K un campo finito di caratteristica p e sia $[K:\mathbb{Z}_p] = n$. Come sappiamo dal Capitolo 14 delle dispense del corso di Aritmetica, K è il campo di spezzamento su $\mathbb{Z}_p$ del polinomio $x^{p^n} - x$ e dunque l'estensione $\mathbb{Z}_p \subset K$ è di Galois. Dimostrare che il gruppo di Galois $Aut(K/\mathbb{Z}_p)$ è isomorfo a $\mathbb{Z}_n$ ed è generato dall'isomorfismo di Frobenius $F : K \to K$ definito da

$$F(a) = a^p \quad \forall a \in K.$$

Esercizio 11.3.8. Sia $q(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p, con p numero primo. Supponiamo che $q(x)$ abbia esattamente due radici non reali in $\mathbb{C}$. Allora il gruppo di Galois (di un campo di spezzamento) di $q(x)$ su $\mathbb{Q}$ è isomorfo a S_p.

Esercizio 11.3.9. Sia F una estensione di k, sia K una estensione di Galois di k, e sia L un campo che contiene sia K sia F. Dimostrare che le estensioni $F \subseteq KF$ e $(K \cap F) \subseteq K$ sono di Galois. Sia

$$\Phi \ : \ Aut(KF/F) \to Aut(K/k)$$

l'omomorfismo dato dalla restrizione. Dimostrare che Φ induce un isomorfismo fra $Aut(KF/F)$ e $Aut(K/(K \cap F))$.

Esercizio 11.3.10. Siano K_1 e K_2 estensioni di Galois del campo k, e sia L un campo che contiene sia K_1 sia K_2. Dimostrare che l'estensione $k \subseteq K_1K_2$ è di Galois[2]. Dimostrare inoltre che l'omomorfismo

$$\Phi \ : \ Aut(K_1K_2/k) \to Aut(K_1/k) \times Aut(K_2/k)$$

dato dalla restrizione su ogni componente, è iniettivo, e infine dimostrare che se $K_1 \cap K_2 = k$ allora Φ è un isomorfismo.

[2]Ricordiamo che il *campo composto* K_1K_2 è definito come il più piccolo sottocampo di L che contiene K_1 e K_2.

Capitolo 12

Sui polinomi ciclotomici (lezione del 30 novembre)

12.1 I polinomi ciclotomici e il loro campo di spezzamento

Sia $f(x) = x^n - 1$ ($n \geq 1$) il polinomio le cui radici in $\mathbb{C}$ sono tutte le radici n–esime dell'unità.

Definizione 12.1.1. Una radice ω di $f(x)$ si dice *radice primitiva n–esima dell'unità* se $\omega^k \neq 1$ per ogni $1 \leq k \leq n-1$.

Osservazione 12.1.1. Le radici n–esime dell'unità sono i numeri complessi $e^{i\frac{2k\pi}{n}}$ per $k = 0, \ldots, n-1$. La radice $e^{i\frac{2k\pi}{n}}$ è primitiva se e solo se $(k, n) = 1$. Dunque le radici primitive n–esime dell'unità sono $\varphi(n)$.

Definizione 12.1.2. Chiamiamo n–esimo *polinomio ciclotomico* il polinomio

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i),$$

dove α_i sono le radici primitive n–esime dell'unità.

Definizione 12.1.3. Per ogni intero positivo n poniamo $\zeta_n = e^{\frac{2\pi\imath}{n}}$.

Osserviamo che con la definizione precedente si ha dunque

$$f(x) = \prod_{d|n} \Phi_d(x),$$

e questa, a priori, è una fattorizzazione in $\mathbb{C}[x]$. In realtà è una fattorizzazione è in $\mathbb{Z}[x]$:

Teorema 12.1.1. *Per ogni $n \geq 1$ il polinomio $\Phi_n(x)$ è a coefficienti interi ed è irriducibile in $\mathbb{Z}[x]$ (e quindi in $\mathbb{Q}[x]$). Dunque la fattorizzazione di $f(x)$ in irriducibili in $\mathbb{Z}[x]$ è*

$$f(x) = \prod_{d|n} \Phi_d(x).$$

Il campo di spezzamento di $\Phi_n(x)$ su $\mathbb{Q}$ coincide con $\mathbb{Q}(\zeta_n)$, ha grado $\varphi(n)$ su $\mathbb{Q}$ e il gruppo di Galois $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ è isomorfo a $\mathbb{Z}_n^*$.

Dimostrazione. Cominciamo dallo studio del campo di spezzamento di $\Phi_n(x)$ su $\mathbb{Q}$. Tale campo coincide con $\mathbb{Q}(\zeta_n)$; infatti $\mathbb{Q}(\zeta_n)$ contiene le potenze di ζ_n e quindi contiene in particolare tutte le radici n-esime primitive dell'unità. Osserviamo che $\mathbb{Q}(\zeta_n)$ è anche il campo di spezzamento del polinomio $x^n - 1$, che è separabile (la caratteristica del campo è 0) e a coefficienti in $\mathbb{Q}$, dunque l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ è di Galois.
Intanto mostriamo che esiste un omomorfismo iniettivo di gruppi

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*.$$

Sia $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, allora definiamo la sua immagine come $\sigma|_{\langle\zeta_n\rangle}$ (con questa notazione intendiamo σ ristretta al sottogruppo moltiplicativo generato da ζ_n). Tale applicazione è ben definita in quanto $\langle\zeta_n\rangle$ è il gruppo che contiene tutte le radici del polinomio $x^n - 1$ e quindi σ le deve permutare: la restrizione è dunque un automorfismo di $\langle\zeta_n\rangle$. Inoltre l'omomorfismo è iniettivo perché se $\sigma|_{\langle\zeta_n\rangle} = id_{\langle\zeta_n\rangle}$ allora $\sigma = id$, visto che σ tiene fisso tutto $\mathbb{Q}$ e anche ζ_n. Quindi $|\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| \leq \varphi(n)$. Ci servirà il seguente:

Esercizio 12.1.1. Sia p un numero primo. In $\mathbb{Z}_p[x]$, per ogni polinomio $g(x)$, vale $g(x^p) = (g(x))^p$.

[È una conseguenza del fatto che, dati $a(x), b(x) \in \mathbb{Z}_p[x]$, vale

$$(a(x) + b(x))^p = (a(x))^p + (b(x))^p$$

visto che p divide $\binom{p}{i}$ per ogni $1 \leq i \leq p-1$ (dispense di Aritmetica, pagina 52). Si può procedere per induzione sul grado di g.]

Lemma 12.1.1. *Per ogni numero intero positivo n, sia ω una radice n-esima primitiva di 1, e sia $q(x) \in \mathbb{Z}[x]$ il suo polinomio minimo (primitivo). Allora per ogni p primo tale che p non divide n, ω^p è una radice di $q(x)$.*

Dimostrazione. Per il Lemma di Gauss sappiamo che $f(x) = q(x)g(x)$ per un certo $g(x) \in \mathbb{Z}[x]$ primitivo. Inoltre studiando i coefficienti di grado massimo si conclude che $q(x), g(x)$ sono monici. Sia ora p tale che $p \nmid n$. Se ω^p non fosse radice di $q(x)$ allora deve esserlo di $g(x)$. Dunque $q(x) \mid g(x^p)$ (entrambi hanno

ω come radice). Allora $g(x^p) = q(x)h(x)$ con $h(x)$ a coefficienti interi primitivo e monico. A questo punto, "proiettando" su $\mathbb{Z}_p[x]$ e utilizzando l'Esercizio 12.1.1 si ottiene che (indichiamo con $\tilde{f}(x), \tilde{g}(x), \tilde{q}(x)$ le proiezioni):

$$(\tilde{g}(x))^p = \tilde{g}(x^p) = \tilde{q}(x)\tilde{h}(x),$$

e quindi il massimo comun divisore tra $\tilde{g}(x)$ e $\tilde{q}(x)$ non è 1. Allora $\tilde{f}(x) = \tilde{q}(x)\tilde{g}(x)$ ha almeno una radice multipla. Ma

$$\tilde{f}'(x) = nx^{n-1},$$

e dunque $(\tilde{f}(x), \tilde{f}'(x)) = 1$ in quanto (ricordiamo che n è invertibile in $\mathbb{Z}_p$) si ha per l'algoritmo euclideo

$$\tilde{f}(x) - xn^{-1}\tilde{f}'(x) = (x^n - 1) - xn^{-1}nx^{n-1} = -1.$$

Ma questo, per il criterio della derivata, è in contraddizione con il fatto che $\tilde{f}(x)$ abbia radici multiple. □

Terminiamo la dimostrazione del teorema: sia $q(x) \in \mathbb{Z}[x]$, in accordo con la notazione usata nel lemma precedente, il polinomio minimo (monico) associato alla radice n–esima primitiva ζ_n. Le radici n–esime primitive dell'unità sono tutte della forma ζ_n^k con k primo con n. Sia $k = p_1^{a_1} \cdots p_r^{a_r}$ la fattorizzazione in primi di k; possiamo ottenere ζ_n^k attraverso elevamenti successivi a una potenza che è un numero primo e primo con n:

$$\zeta_n \to \zeta_n^{p_1} \to (\zeta_n^{p_1})^{p_1} \to \ldots \to \left(\zeta_n^{p_1^{a_1}\cdots p_r^{a_r-1}}\right)^{p_r} = \zeta_n^k$$

Per il lemma appena mostrato sappiamo che $\zeta_n^{p_1}$ è una radice di $q(x)$. A questo punto, siccome $q(x)$ è anche il polinomio minimo di $\zeta_n^{p_1}$, che è una radice n–esima primitiva dell'unità, possiamo applicare ancora il lemma e ottenere che $(\zeta_n^{p_1})^{p_1}$ (stiamo supponendo, tanto per fare un esempio, che $a_1 \geq 2$) è una radice di $q(x)$ e così via. In questa maniera si dimostra che, per ogni k primo con n, ζ_n^k è una radice del polinomio $q(x)$.
Allora tutte le radici n–esime primitive sono radici di $q(x)$, quindi $\Phi_n(x) \mid q(x)$ in $\mathbb{C}[x]$. Ma sappiamo che

$$\deg q(x) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \varphi(n).$$

Dunque $\deg \Phi_n(x) = \deg q(x)$ ed essendo entrambi monici, si conclude che $\Phi_n(x) = q(x)$. Questo dimostra anche che $\Phi_n(x)$ è a coefficienti interi ed è irriducibile in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$.
Inoltre possiamo osservare a questo punto che $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$; come conseguenza, l'omomorfismo iniettivo $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ per ragioni di cardinalità deve essere un isomorfismo. □

Osservazione 12.1.2. Se p è un primo osserviamo che il p–esimo polinomio ciclotomico è $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$.

Osservazione 12.1.3. Ecco una lista dei primi polinomi ciclotomici:

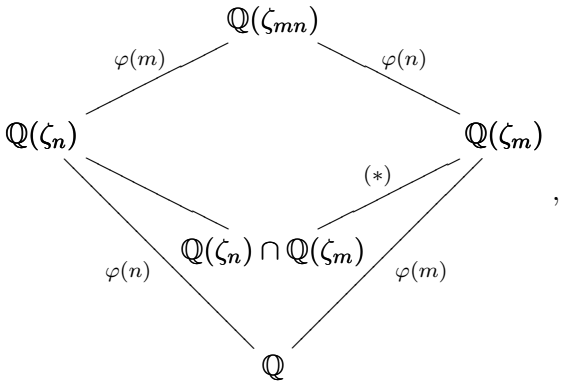
$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x+1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1.
\end{aligned}$$

Osserviamo che i polinomi ciclotomici nella lista qui sopra hanno tutti 0, 1 o -1 come coefficienti. Questo non vale in generale, ma il primo polinomio ciclotomico con coefficienti diversi da questi è $\Phi_{105}(x)$.

Proposizione 12.1.1. *Se n e m sono due interi positivi primi tra loro allora*

$$(1)\ \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{mn}) \qquad (2)\ \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

Dimostrazione. (1) Vale l'inclusione $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_n, \zeta_m)$ in quanto $\mathbb{Q}(\zeta_n, \zeta_m)$ contiene la radice primitiva mn–esima dell'unità $\zeta_n\zeta_m$. L'altra inclusione si ottiene osservando che ζ_{mn}^m è una radice n-esima primitiva dell'unità e che ζ_{mn}^n è una radice m-esima primitiva dell'unità.
(2) Per questo consideriamo il diagramma seguente:



,

già completato con i gradi. Le estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ e $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$ hanno i gradi indicati per quanto abbiamo mostrato prima (Teorema 12.1.1). Per la stessa ragione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{mn})$ è un'estensione di grado $\varphi(mn)$. Questo ci permette di ricavare gli altri due gradi indicati. Adesso, il grado dell'estensione contrassegnata con $(*)$ non può essere minore di $\varphi(m)$: se infatti fosse

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)] = d < \varphi(m)$$

allora il polinomio minimo $p(x)$ di ζ_m su $\mathbb{Q}(\zeta_n)$ dovrebbe avere grado minore o uguale a d e dunque l'estensione $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$ dovrebbe avere grado minore o uguale d. Assurdo. Dunque $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)] = \varphi(m)$ e allora il grado di $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$ su $\mathbb{Q}$ è 1, da cui la tesi. □

12.2 Verso il teorema della progressione aritmetica

Il teorema della progressione aritmetica di Dirichlet[1] afferma che, se a e b sono due interi primi fra loro (e $a \neq 0$), allora ci sono infiniti primi della forma $an + b$ (con $n \in \mathbb{Z}$). Dal corso di Aritmetica sappiamo già dimostrare che sono infiniti i primi della forma $4n + 3$ e quelli della forma $4n + 1$ (riguardate le dimostrazioni!).

In questo paragrafo dimostreremo una forma debole del teorema di Dirichlet, ossia il caso in cui $b = 1$. Cominciamo dal seguente lemma, in cui gioca un ruolo essenziale il fatto che i polinomi ciclotomici sono a coefficienti interi.

Lemma 12.2.1. *Dato un numero intero positivo a, siano p un primo e n un intero tali che $p \mid \Phi_a(n)$ ma $p \nmid \Phi_d(n)$ per ogni d divisore proprio di a. Allora $p \equiv 1 \pmod{a}$.*

Dimostrazione. Per prima cosa osserviamo che p è primo con n. Infatti dall'informazione $p \mid \Phi_a(n)$ ricaviamo subito $p \mid (n^a - 1)$, visto che il polinomio $\Phi_a(x)$ divide $x^a - 1$ in $\mathbb{Z}[x]$. Dunque se p dividesse n, avremmo l'assurdo che $p \mid (n^a - 1)$ e $p \mid (n^a)$.

Il punto essenziale consiste ora nel dimostrare che $[n]$ ha ordine a in $\mathbb{Z}_p$. Allora $a \mid (p - 1)$ e dunque si ha la tesi. Ovviamente l'ordine di $[n]$ divide a in quanto in $\mathbb{Z}_p$ vale

$$[n]^a - [1] = \prod_{d|a} \Phi_d([n]) = [0],$$

poiché $\Phi_a([n]) = [0]$ per ipotesi. Inoltre l'ordine di $[n]$ deve essere almeno a in quanto, dato $d < a$ con $d \mid a$, in $\mathbb{Z}_p$ abbiamo

$$[n]^d - [1] = \prod_{d'|d} \Phi_{d'}([n]),$$

[1] Johann P. G. Lejeune Dirichlet, 1805-1859 matematico tedesco.

con $\Phi_{d'}([n]) \neq [0]$ per l'ipotesi che $p \nmid \Phi_{d'}(n)$ per ogni d' divisore proprio di a (osserviamo che d' è un divisore proprio di a visto che $d' \mid d$, e d è divisore proprio di a). $\square$

Teorema 12.2.1 (forma debole del teorema di Dirichlet della progressione aritmetica)**.** *Per ogni intero $a \neq 0$ fissato, ci sono infiniti primi della forma $an + 1$ (con $n \in \mathbb{Z}$).*

Dimostrazione. Osserviamo che basta considerare il caso in cui a è positivo. Inoltre se $a = 1$ il teorema è banalmente vero. Supponiamo quindi $a > 1$ e supponiamo anche che esista solo un numero finito di primi congrui a 1 modulo a, che chiameremo $p_1, \ldots, p_q$. Se, dato a, trovassimo un intero n e un primo p tali che a, n e p soddisfino le ipotesi del lemma precedente, potremmo concludere che $p \equiv 1 \pmod{a}$. Ma questo non basterebbe ancora per affermare di aver trovato un assurdo, perché p potrebbe essere uno dei p_i.
Consideriamo allora

$$A = a \cdot p_1 \cdots p_q.$$

Se, dato A, troviamo un intero n e un primo p tali che A, n e p soddisfano le ipotesi del lemma precedente, possiamo concludere che $p \equiv 1 \pmod{A}$ e questo implica in particolare che $p \equiv 1 \pmod{a}$, ma stavolta saremo sicuri che $p \neq p_i$ per ogni i. Ora, i due polinomi $\Phi_A(x)$ e $Q(x) = \prod_{d|A,\, d\neq A} \Phi_d(x)$ sono primi tra loro in $\mathbb{C}[x]$ in quanto non hanno radici in comune; dunque sono primi tra loro anche in $\mathbb{Q}[x]$. Per il lemma di Bezout possiamo scrivere

$$1 = U(x)\Phi_A(x) + V(x)Q(x),$$

con $U, V \in \mathbb{Q}[x]$. Osserviamo che esiste un $n \in \mathbb{Z}$ tale che $nU(x)$ e $nV(x)$ siano a coefficienti interi, e affermiamo che possiamo ulteriormente scegliere n in modo che $\Phi_A(n) \neq 0$ e $\Phi_A(n) \neq \pm 1$: infatti gli n tali che $nU(x)$ e $nV(x)$ siano in $\mathbb{Z}[x]$ sono infiniti e i polinomi $\Phi_A(x)$ e $\Phi_A(x) \mp 1$, avendo grado positivo, hanno un numero finito di radici. Scelto un tale n possiamo scrivere:

$$n = nU(x)\Phi_A(x) + nV(x)Q(x),$$

e dunque in particolare

$$n = nU(n)\Phi_A(n) + nV(n)Q(n). \tag{12.1}$$

Sia p un primo che divide $\Phi_A(n)$; un tale primo esiste per la scelta fatta su n (scelto in modo che $\Phi_A(n) \neq 0$ e $\Phi_A(n) \neq \pm 1$). Allora $p \mid \left(n^A - 1\right)$, ossia $[n]^A = 1$ in $\mathbb{Z}_p$, quindi $[n]$ è invertibile, che equivale a dire $MCD(n, p) = 1$ (questa osservazione del resto la avevamo già fatta all'inizio della dimostrazione del Lemma 12.2.1). Ma

se fosse che $p \mid Q(n)$ allora avremmo dalla (12.1) che $p \mid n$, e ciò è assurdo. Visto che non divide $Q(n)$, p non divide nessuno dei $\Phi_d(n)$ con $d \mid A$ e $d < A$. Ma allora per n, A e p scelti sono soddisfatte le ipotesi del Lemma 12.2.1, come volevamo. □

12.3 Esercizi

Suggerimento: guardare gli esercizi svolti nel Capitolo 7, Paragrafo 7 di [DM].

Esercizio 12.3.1. Trovare il polinomio minimo di ζ_5 su $\mathbb{Q}(\imath)$ e su $\mathbb{Q}(\sqrt{5})$.

Esercizio 12.3.2. Sia ζ_7 una radice primitiva settima di 1, e siano $\alpha = \zeta_7 + \zeta_7^{-1}$ e $\beta = \zeta_7 + \zeta_7^2 + \zeta_7^4$. Osservare che le estensioni $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_7)$ e $\mathbb{Q}(\beta) \subset \mathbb{Q}(\zeta_7)$ sono di Galois e trovare i rispettivi gruppi di Galois. Trovare tutti i sottocampi della estensione di Galois $\mathbb{Q} \subset \mathbb{Q}(\zeta_7)$.

Esercizio 12.3.3. Osservare che se α è una radice di $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$, allora anche $\alpha^2 - 2$ e $2 - \alpha - \alpha^2$ sono radici del polinomio. Sia $E \subset \mathbb{C}$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$. Esiste $\sigma \in Aut(E/\mathbb{Q})$ che scambia fra loro α e $\alpha^2 - 2$?

Esercizio 12.3.4. Dato un numero primo p, consideriamo l'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta_3, \zeta_5, \sqrt{p})$. Trovare, al variare di p fra i numeri primi, il gruppo di Galois dell'estensione e il numero di sottocampi di grado 2 su $\mathbb{Q}$.

Esercizio 12.3.5. Sia E il campo di spezzamento su $\mathbb{Q}$ del polinomio $x^7 - 3$. Determinare il gruppo di Galois $Aut(E/\mathbb{Q})$.

Esercizio 12.3.6. Si consideri $\beta = \zeta_7 + \zeta_7^2 + \zeta_7^4$. Calcolare il gruppo di Galois $Aut(\mathbb{Q}(\gamma, \zeta_5)/\mathbb{Q})$.

Esercizio 12.3.7. Sia $\mathbb{F}$ un campo finito e siano α e β algebrici su $\mathbb{F}$ con polinomi minimi di grado rispettivamente 5 e 4. Dimostrare che $[\mathbb{F}(\alpha\beta) : \mathbb{F}] = 20$.

Esercizio 12.3.8. Calcolare, al variare dell'intero positivo m, i gruppi di Galois del campo di spezzamento di $x^5 - m$ su $\mathbb{Q}$ e su $\mathbb{Z}_{19}$.

Capitolo 13

Il problema inverso di Galois (lezione del 7 dicembre)

13.1 Problema inverso di Galois

Una domanda naturale e interessante in teoria di Galois è la seguente: dato un gruppo finito G, esiste un'estensione di Galois $F \subseteq E$ tale che $\mathrm{Aut}(E/F) \cong G$? Si tratta della forma debole del *problema inverso di Galois*: mostreremo in questo paragrafo che la risposta è affermativa. Il vero problema inverso di Galois consiste nel chiedersi se esiste un'estensione E di $\mathbb{Q}$ tale che $\mathrm{Aut}(E/\mathbb{Q}) \cong G$, con G gruppo finito dato. Questo problema in generale è ancora aperto, ma nelle prossime pagine daremo una risposta affermativa nel caso dei gruppi abeliani.

Per cominciare ad affrontare la questione osserviamo che, dato che ogni gruppo G si può immergere in S_n per un certo n, possiamo intanto porci il problema di trovare un'estensione $F' \subseteq E'$ di Galois in cui $\mathrm{Aut}(E'/F') \cong S_n$.

Sia F un campo, e consideriamo

$$F(x_1, \ldots, x_n) =$$

$$= \left\{ \frac{f(x_1, ..., x_n)}{g(x_1, ..., x_n)} \mid f(x_1, ..., x_n), g(x_1, ..., x_n) \in F[x_1, ..., x_n],\ g(x_1, ..., x_n) \neq 0 \right\}$$

il campo delle funzioni razionali su F nelle variabili $x_1, \ldots, x_n$. Il gruppo S_n agisce su $F(x_1, \ldots, x_n)$ permutando le variabili. L'azione è descritta da

$$\begin{array}{ccc} S_n \times F(x_1, \ldots, x_n) & \longrightarrow & F(x_1, \ldots, x_n) \\ (\sigma, f(x_1, \ldots, x_n)) & \longmapsto & \sigma(f(x_1, \ldots, x_n)) = f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) \end{array}$$

In realtà σ agisce come un automorfismo di $F(x_1, \ldots, x_n)$ in quanto valgono

$$\sigma(fg) = \sigma(f)\sigma(g), \quad \sigma(f+g) = \sigma(f) + \sigma(g)$$

Visto che $\sigma(k) = k \ \forall k \in F$, allora $\sigma \in \mathrm{Aut}(F(x_1, \ldots, x_n)/F)$, dunque possiamo vedere S_n come sottogruppo di $\mathrm{Aut}(F(x_1, \ldots, x_n)/F)$. Osserviamo che l'estensione $F \subset F(x_1, \ldots, x_n)$ non è finita. Denotiamo con $S(x_1, \ldots, x_n)$ il campo fisso del sottogruppo S_n:

$$F \subseteq S(x_1, \ldots, x_n) \subseteq F(x_1, \ldots, x_n).$$

Vista la sua importanza diamo la seguente:

Definizione 13.1.1. $S(x_1, \ldots, x_n)$ è detto *campo delle funzioni razionali simmetriche* su F nella variabili $x_1, ..., x_n$.

L'estensione che ci interessa è $S(x_1, \ldots, x_n) \subseteq F(x_1, \ldots, x_n)$.

Teorema 13.1.1. *L'estensione $S(x_1, \ldots, x_n) \subseteq F(x_1, \ldots, x_n)$ è di Galois, e il suo gruppo di Galois è isomorfo a S_n.*

Dimostrazione. Intanto mostriamo che l'estensione è finita. Consideriamo l'anello di polinomi $F(x_1, \ldots, x_n)[t]$ e il polinomio

$$q(t) = \prod_{i=1}^{n}(t - x_i) = t^n - \left(\sum_{i=1}^{n} x_i\right) t^{n-1} + \ldots + (-1)^n \prod_{i=1}^{n} x_i. \tag{13.1}$$

Osserviamo che in realtà $q(t) \in S(x_1, \ldots, x_n)[t]$ e il suo campo di spezzamento è proprio $F(x_1, \ldots, x_n)$. Questo dimostra che l'estensione è finita (al massimo il grado è $n!$) e, poiché il polinomio $q(t)$ è separabile (non ha radici multiple), l'estensione è di Galois. Visto che S_n, sottogruppo di $\mathrm{Aut}(F(x_1, \ldots, x_n)/S(x_1, \ldots, x_n))$, ha come campo fisso proprio $S(x_1, \ldots, x_n)$ allora deve coincidere con tutto il gruppo (per la Proposizione 11.1.1). □

Osservazione 13.1.1. Sappiamo che il grado del campo di spezzamento di un polinomio di grado n è al massimo $n!$. Osserviamo che nel teorema precedente abbiamo costruito un campo di spezzamento di grado esattamente $n!$: infatti, dopo aver mostrato che l'estensione è di Galois, possiamo concludere che il grado dell'estensione, dovendo coincidere con l'ordine del gruppo di Galois, è proprio $n!$.

Finora abbiamo visto come trovare un'estensione di Galois che abbia come gruppo di Galois proprio S_n. Adesso prendiamo un gruppo finito G e torniamo al problema inverso di Galois (nella forma debole, che non richiede che il campo base sia $\mathbb{Q}$): sappiamo che possiamo immergere G in un S_N (teorema di Cayley).
Consideriamo dunque $S(x_1, \ldots, x_N) \subseteq F(x_1, \ldots, x_N)$, che è di Galois. Allora $G \hookrightarrow S_N \cong \mathrm{Aut}(F(x_1, \ldots, x_N)/S(x_1, \ldots, x_N))$. Possiamo quindi considerare il campo fisso $j(G)$ di G visto come sottogruppo degli automorfismi. In questo modo

$$G = i(j(G)) = \mathrm{Aut}(F(x_1, \ldots, x_N)/j(G))$$

e dunque l'estensione $J(G) \subset F(x_1, \ldots, x_N)$ risolve il problema.

Cosa possiamo dire a riguardo del problema inverso di Galois nel caso in cui si richieda anche che il campo base sia $\mathbb{Q}$? Come preannunciato, si tratta di un problema tuttora aperto; noi lo affronteremo nel caso dei gruppi abeliani, cominciando dai gruppi ciclici.

Teorema 13.1.2. *Dato n intero positivo esiste un'estensione di Galois di $\mathbb{Q}$ il cui gruppo di Galois è isomorfo a $\mathbb{Z}_n$.*

Dimostrazione. A parte i casi banali ($n = 1$ o $n = 2$), il risultato si può dimostrare come segue. Per prima cosa si sceglie un primo p tale che $p \equiv 1 \pmod{n}$, e questo è sempre possibile, come mostra la forma debole del teorema di Dirichlet. Poi si considera l'estensione di Galois $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$. Il suo gruppo di Galois $\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, come sappiamo, è isomorfo a $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$.
Ora, $n \mid (p-1)$, ossia vale $p-1 = nk$ per un certo k. Se scegliamo in $\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ il sottogruppo H isomorfo a $\mathbb{Z}_k$, allora, visto che H è normale (siamo in un contesto abeliano), per il teorema fondamentale della teoria di Galois il campo fisso E di H è di Galois su $\mathbb{Q}$. Inoltre il gruppo di Galois $\mathrm{Aut}(E/\mathbb{Q})$ è isomorfo al quoziente $\mathbb{Z}_{p-1}/\mathbb{Z}_k \cong \mathbb{Z}_n$. □

Esempio 13.1.1. Se vogliamo trovare una estensione E di $\mathbb{Q}$ di Galois il cui gruppo di Galois sia $\mathbb{Z}_7$, basta considerare $p = 29$ e l'estensione di Galois $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{29})$ il cui gruppo di Galois è isomorfo a $\mathbb{Z}_{28}$. A questo punto si prende il campo fisso E del sottogruppo H di $\mathbb{Z}_{28}$ che è generato (additivamente) da [7], e che è isomorfo a $\mathbb{Z}_4$.

Corollario 13.1.1 (Risoluzione del problema inverso di Galois per i gruppi abeliani)**.** *Sia A un gruppo abeliano finito. Allora esiste una estensione $\mathbb{Q} \subset E$ di Galois tale che il gruppo di Galois $Aut(E/\mathbb{Q})$ sia A.*

Dimostrazione. Se A è banale possiamo prendere $E = \mathbb{Q}$. Supponiamo dunque che A non sia banale; per il teorema di classificazione dei gruppi abeliani finitamente generati sappiamo che A è isomorfo ad un prodotto di gruppi ciclici:

$$A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$$

per certi numeri interi $d_i \geq 2$ (e tali che, se $i < j$, d_i divide d_j). Per la forma debole del teorema della progressione aritmetica di Dirichlet sappiamo che possiamo trovare dei numeri primi distinti fra loro $p_1, ..., p_t$ tali che $p_i \equiv 1 \pmod{d_i}$ per ogni i. Per ogni i possiamo dunque trovare degli interi m_i tali che $p_i - 1 = m_i d_i$.

Chiamiamo $s = p_1 p_2 \cdots p_t$; applicando la Proposizione 12.1.1 si osserva che l'estensione di Galois $\mathbb{Q} \subset \mathbb{Q}(\zeta_s)$ ha gruppo di Galois

$$\mathbb{Z}_s^* \cong \mathbb{Z}_{p_1}^* \times \mathbb{Z}_{p_2}^* \times \cdots \times \mathbb{Z}_{p_t}^* \cong \mathbb{Z}_{p_1-1} \times \mathbb{Z}_{p_2-1} \times \cdots \times \mathbb{Z}_{p_t-1}$$

In ogni fattore $\mathbb{Z}_{p_i-1}$ possiamo trovare un sottogruppo di ciclico H_i di ordine m_i (il sottogruppo generato da $[d_i]$). Ora osserviamo che il sottogruppo $H = H_1 \times H_2 \times \cdots \times H_t$ del gruppo di Galois $Aut(\mathbb{Q}(\zeta_s)/\mathbb{Q})$ è normale (siamo in un contesto abeliano). Dunque, per il secondo teorema di Galois, indicando come sempre con $j(H)$ il campo fisso di H, sappiamo che l'estensione di Galois $\mathbb{Q} \subset j(H)$ è di Galois e

$$Aut(j(H)/\mathbb{Q}) \cong \frac{\mathbb{Z}_{p_1-1} \times \mathbb{Z}_{p_2-1} \times \cdots \times \mathbb{Z}_{p_t-1}}{H_1 \times H_2 \times \cdots \times H_t} \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$$

ossia $Aut(j(H)/\mathbb{Q}) \cong A$ come volevamo. □

13.2 Esercizi di teoria di Galois

Esercizio 13.2.1. Sia $\mathbb{F}_q$ il campo finito con $q = p^n$ elementi. Per quali gruppi G esiste una estensione di Galois $\mathbb{F}_q \subset E$ tale che $Aut(E/\mathbb{F}_q) \cong G$?

Esercizio 13.2.2. Sia K il campo di spezzamento di $x^5 - 3$ su $\mathbb{Q}$. Determinare il grado di K su $\mathbb{Q}$ e descrivere il gruppo di Galois $Aut(K/\mathbb{Q})$. Determinare i sottocampi F di K che hanno grado 5 su $\mathbb{Q}$.

Esercizio 13.2.3. Si consideri l'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta_{49}, \sqrt{7})$. Dimostrare che è una estensione di Galois e descrivere il gruppo di Galois.

Esercizio 13.2.4. Si consideri il campo di spezzamento K su $\mathbb{Q}$ di $x^6 + 2$. Determinare il grado $[K : \mathbb{Q}]$, descrivere il gruppo di Galois $Aut(K/\mathbb{Q})$. Il polinomio $x^2 - 6$ è irriducibile o no su K?

Esercizio 13.2.5. Si consideri il campo di spezzamento K su $\mathbb{Q}$ di $x^{10} - 5$. Determinare il grado $[K : \mathbb{Q}]$ e descrivere il gruppo di Galois $Aut(K/\mathbb{Q})$.

Esercizio 13.2.6. Si consideri il campo di spezzamento K su $\mathbb{Q}$ di $x^{12} - 3$. Determinare il grado $[K : \mathbb{Q}]$ e descrivere il gruppo di Galois $Aut(K/\mathbb{Q})$.

Esercizio 13.2.7. Si consideri il campo di spezzamento K su $\mathbb{Q}$ di $x^4 - 12x^2 + 25$. Dimostrare che $[K : \mathbb{Q}] = 4$, e individuare tutti i sottocampi di K.

Esercizio 13.2.8. Si consideri il campo di spezzamento K su $\mathbb{Q}$ di $x^4 - 2x^2 - 2$. Determinare il grado $[K : \mathbb{Q}]$ e descrivere il gruppo di Galois $Aut(K/\mathbb{Q})$.

Esercizio 13.2.9. Dimostrare che $\mathbb{Q}(i, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(i + \sqrt{3} + \sqrt{5})$. Determinare il grado $[\mathbb{Q}(i, \sqrt{3}, \sqrt{5}) : \mathbb{Q}]$, descrivere il gruppo di Galois $Aut(\mathbb{Q}(i, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ ed individuare tutti i sottocampi di $\mathbb{Q}(i, \sqrt{3}, \sqrt{5})$ di grado 2 su $\mathbb{Q}$.

Esercizio 13.2.10. Si consideri il campo di spezzamento K su $\mathbb{Q}$ di $x^7 - 2$. Qual è il grado di $K \cap \mathbb{R}$ su $\mathbb{Q}$? L'estensione $\mathbb{Q} \subset K \cap \mathbb{R}$ è di Galois? Se sì calcolare il gruppo di Galois, se no individuare il massimo sottocampo L di $K \cap \mathbb{R}$ (massimo rispetto all'inclusione) tale che $\mathbb{Q} \subset L$ sia di Galois.

Capitolo 14

Qualche approfondimento su anelli PID e UFD

In questa lezione faremo un breve ripasso sugli anelli UFD e discuteremo una questione rimasta in sospeso nel corso di Aritmetica, ossia la dimostrazione del fatto che un anello PID è UFD.[1] Per questa dimostrazione introdurremo gli anelli noetheriani, che verranno poi studiati in maniera approfondita in vari corsi successivi.

14.1 Campo delle frazioni di un dominio di integrità

Dato un dominio di integrità D consideriamo l'insieme:

$$\Gamma = \{(a, b) \in D \times D \mid b \neq 0\} \subseteq D \times D.$$

Sull'insieme Γ definiamo la seguente relazione:

$$(a, b) \sim (c, d) \iff ad = bc.$$

Lasciamo al lettore la verifica che quella data è una relazione di equivalenza, commentando però la verifica della proprietà transitiva. Sia $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$: queste due significano $ad = bc$ e $cf = de$. Moltiplicando la prima per f e la seconda per b e ricordando che D è commutativo, possiamo scrivere $afd = bcf = bed$. Ora, D è un dominio di integrità, quindi $(af - be)d = 0$ implica $af = be$ in quanto $d \neq 0$. Dunque $(a, b) \sim (e, f)$ e questa verifica è dipesa in maniera sostanziale dal fatto che D è un dominio.
Denotiamo con K l'insieme delle classi di equivalenza della relazione $\sim$ e indichiamo con $\frac{a}{b}$ la classe di equivalenza della coppia (a, b). Dotiamo K di due operazioni,

[1] Siete caldamente incoraggiati a ripassare la parte sugli anelli PID nelle dispense di Aritmetica.

somma e prodotto:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \quad \text{e} \quad \frac{a}{b}\frac{c}{d}=\frac{ac}{bd},$$

per ogni $a, b, c, d \in D$ e $b, d \neq 0$.

Esercizio 14.1.1. Dimostrare che le operazioni di somma e prodotto in K sono ben definite.

Proposizione 14.1.1. *K dotato di somma e prodotto è un campo.*

Dimostrazione. La verifica è lasciata per esercizio. □

Definizione 14.1.1. Sia D un dominio di integrità. Allora K costruito come sopra si dice *campo delle frazioni* di D.

Se si compie la costruzione di K partendo dall'anello $\mathbb{Z}$ il campo delle frazioni che si ottiene è isomorfo a $\mathbb{Q}$. Se si parte dall'anello $F[x_1, ..., x_n]$ (con F campo) si ottiene un campo delle frazioni isomorfo a $F(x_1, ..., x_n)$, il campo delle funzioni razionali su F nelle variabili $x_1, ..., x_n$, che abbiamo incontrato nel capitolo precedente. Osserviamo anche che in generale il campo K contiene una copia isomorfa a D:

Proposizione 14.1.2. *Ogni dominio di integrità si può immergere in un campo.*

Dimostrazione. Sia D un dominio di integrità e K il suo campo delle frazioni. Allora abbiamo l'applicazione:

$$\begin{array}{rccc} \phi: & D & \longrightarrow & K \\ & d & \longmapsto & \frac{d}{1}. \end{array}$$

Tale applicazione è un omomorfismo iniettivo di D in K, che quindi contiene una copia isomorfa di D. □

14.2 Domini a fattorizzazione unica

Definizione 14.2.1. Un anello commutativo R soddisfa la ACC ("ascending chain condition", la "*condizione della catena ascendente*") se non esiste una successione infinita di ideali di R in cui ogni ideale contiene propriamente il precedente.

Osservazione 14.2.1. Se abbiamo $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots I_n \subseteq \ldots$ e R soddisfa la ACC, allora deve esistere m tale che $I_k = I_m$ per ogni $k \geq m$. Si dice che *la catena di ideali si stabilizza.*

Definizione 14.2.2. Gli anelli commutativi che soddisfano la ACC si dicono *anelli noetheriani*.[2]

Vedremo nel Paragrafo 14.3 un'altra definizione (equivalente) di anello noetheriano.

Esempio 14.2.1. L'anello $\mathbb{Z}$ è a ideali principali ed è noetheriano. Prendiamo $I \subset \mathbb{Z}$ ideale, che sarà generato da un certo $n \in \mathbb{Z}$ con $n \geq 0$: se n è primo l'unico ideale di $\mathbb{Z}$ che lo contiene è $\mathbb{Z}$ stesso. Se n non è primo possiamo trovare ideali che contengono $n\mathbb{Z}$ solo prendendo come generatori dei divisori di n, che sono in numero finito. Fra poco del resto daremo la dimostrazione che ogni dominio a ideali principali è noetheriano.

Esempio 14.2.2. L'anello $R = F[x_1, x_2, \ldots, x_n, \ldots]$ dei polinomi su infinite variabili non è noetheriano. Possiamo infatti esibire una catena di ideali che non soddisfa la ACC:

$$(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n) \subset \cdots .$$

Ma R è un dominio e dunque avrà un campo delle frazioni, che invece è noetheriano[3]. Questo esempio mostra che un sottoanello di un anello noetheriano non necessariamente è noetheriano.

Esempio 14.2.3. Consideriamo $C(\mathbb{R})$, insieme delle funzioni continue da $\mathbb{R}$ in $\mathbb{R}$. Sia poi $I_1 = \{f \in C(\mathbb{R}) \mid f([-1,1]) = 0\}$ e sia

$$I_n = \left\{ f \in C(\mathbb{R}) \mid f\left(\left[-\frac{1}{n}, \frac{1}{n}\right]\right) = 0 \right\}.$$

Si vede facilmente che I_n è ideale per ogni $n > 0$. Inoltre vale anche $I_i \subsetneq I_{i+1}$ per ogni $i > 0$ e quindi $C(\mathbb{R})$ non è noetheriano.

Teorema 14.2.1. *Sia R un dominio a ideali principali. Allora R è noetheriano.*

Dimostrazione. Prendiamo una catena infinita di ideali $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ in R e sia

$$I = \bigcup_{i=1}^{\infty} I_i.$$

Non è difficile verificare che I è un ideale di R. Infatti, dati $a, b \in I$ esistono i e j tali che $a \in I_i$ e $b \in I_j$: se per esempio $i \geq j$ allora $b \in I_i$ e dunque $a + b \in I_i \subseteq I$; lo stesso accade per la moltiplicazione. Ora R è un dominio a ideali principali,

[2] In onore di Emmy Noether, matematica tedesca, 1882-1935.

[3] Un campo ha infatti solo due ideali: $\{0\}$ e tutto il campo.

dunque $I = (c)$ per un certo $c \in R$, ma $c \in I$ e dunque $c \in I_k$ per un certo k. Da ciò segue

$$I = (c) \subseteq I_k \subseteq I$$

dunque deve essere $I = I_k$. In conclusione per $m \geq k$ la catena si stabilizza. □

Teorema 14.2.2. *Ogni dominio a ideali principali R è un dominio a fattorizzazione unica.*

Dimostrazione. Nella prima parte mostreremo l'esistenza della fattorizzazione in irriducibili per gli elementi non nulli e non invertibili[4], mentre nella seconda faremo vedere l'unicità. Sia $a \in R$ non nullo e non invertibile; mostriamo per prima cosa che a ha un fattore irriducibile. Abbiamo due possibilità: o a è irriducibile, e quindi abbiamo il fattore irriducibile voluto, o a non è irriducibile. In questo secondo caso $a = a_1 b_1$ con $a_1, b_1 \notin U(R)$ (cioè si ha una vera fattorizzazione). Dunque $(a) \subseteq (a_1)$, ma non può valere l'uguaglianza altrimenti b_1 sarebbe invertibile: infatti se valesse l'uguale $a_1 = a\gamma$ e quindi

$$a_1(1 - b_1\gamma) = 0 \Longrightarrow b_1\gamma = 1$$

perché $a_1 \neq 0$ e siamo in un dominio di integrità. In definitiva $(a) \subsetneq (a_1)$. Per a_1 valgono ancora le stesse possibilità: se a_1 è irriducibile allora abbiamo trovato il fattore irriducibile, sennò $a_1 = a_2 b_2$ con $a_2, b_2 \notin U(R)$, e avremo $(a) \subsetneq (a_1) \subsetneq (a_2)$ per ragioni analoghe. Questo procedimento deve avere termine perché R, essendo un dominio a ideali principali, è noetheriano.[5] Alla fine quindi troviamo r tale che a_r è irriducibile e $a_r \mid a$.
Cerchiamo ora una fattorizzazione in prodotto di irriducibili per a. Se a è irriducibile abbiamo finito; se a non è irriducibile, per quanto appena dimostrato, lo scriviamo come $a = p_1 c_1$ con p_1 irriducibile (quindi non invertibile) e $c_1 \notin U(R)$ perché altrimenti a sarebbe irriducibile. Dunque $(a) \subseteq (c_1)$ e dal fatto che $p_1 \notin U(R)$ segue (per lo stesso ragionamento già fatto sopra) che $(a) \subsetneq (c_1)$. Se c_1 è irriducibile allora $a = p_1 c_1$ è una fattorizzazione in irriducibili di a e abbiamo finito; se c_1 non è irriducibile allora $c_1 = p_2 c_2$ con p_2 irriducibile e $c_2 \notin U(R)$: analogamente a prima $(a) \subsetneq (c_1) \subsetneq (c_2)$. Tale procedimento deve finire e si giunge dunque a scrivere $a = p_1 p_2 \cdots p_s$ con tutti i fattori irriducibili.
Adesso dobbiamo mostrare l'unicità della fattorizzazione di a. Siano

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

[4]In questa parte si utilizza l'assioma DC (*dependent choice*), una forma debole dell'assioma della scelta; per approfondire questa frase attendete i corsi di teoria degli insiemi o elementi di logica.

[5]In questo passaggio per esempio si utilizza l'assioma DC.

con p_i e q_j irriducibili (ossia primi, dato che R è PID [6]) e $s \geq r$ due fattorizzazioni di a. Prendiamo p_1: notiamo che $p_1 \mid q_1 q_2 \cdots q_s$ e quindi $p_1 \mid q_j$ per un certo j; a meno di riordinare supponiamo $p_1 \mid q_1$. Dunque $q_1 = p_1 u_1$ con $u_1 \in U(R)$ (visto che q_1 è irriducibile):

$$p_1 p_2 \cdots p_r = p_1 u_1 q_2 \cdots q_s$$

Quindi, dato che siamo in un dominio di integrità, $p_2 \cdots p_r = u_1 q_2 \cdots q_s$. Procedendo in modo analogo si otterrà $1 = u_1 \cdots u_r (q_{r+1} \cdots q_s)$, ma se $s > r$ avremmo un assurdo perché i q_j erano irriducibili e quindi non possono essere invertibili. Allora si conclude che $r = s$ e che i p_i e i q_j sono tra loro associati a coppie. □

Esercizio 14.2.1. Dimostrare che in un UFD i concetti di elemento irriducibile e di elemento primo coincidono.

Osservazione 14.2.2. Ricordiamo che in un dominio a fattorizzazione unica ogni coppia di elementi non entrambi nulli ammette un massimo comun divisore e un minimo comune multiplo (si possono usare le fattorizzazioni degli elementi, e scegliere, per esempio per il massimo comun divisore, gli irriducibili che compaiono in entrambe col minimo esponente...il tutto a meno di associati...). Tali massimo comun divisore e minimo comune multiplo saranno definiti a meno di invertibili, ossia a meno di associati.

Osservazione 14.2.3. Nel corso di Aritmetica avete imparato che $\mathbb{Z}[x]$ è un UFD che non è un PID.

Senza dimostrazione enunciamo il seguente importante risultato (chi è interessato trova la dimostrazione sull'Herstein [He], sostanzialmente basata sull'analogo del Lemma di Gauss che avete visto ad Aritmetica nel caso $\mathbb{Z}[x]$):

Teorema 14.2.3. *Sia R un UFD. Allora anche $R[x]$ è un UFD.*

Corollario 14.2.1. *Sia R un UFD. Allora l'anello $R[x_1, x_2, \ldots, x_n]$ è un UFD. In particolare, se K è un campo, $K[x_1, x_2, \ldots, x_n]$ è un UFD.*

Ricordiamo che nel Capitolo 11, Paragrafo 5, delle dispense di Aritmetica si studia una famiglia di anelli in cui ci sono vari esempi di anelli non UFD.

14.3 Sulla definizione di anello noetheriano

Il seguente teorema mostra che (sempre accettando l'assioma DC) possiamo dare un'altra definizione equivalente di anello noetheriano (e ne vedrete almeno un'altra in corsi futuri).

[6] Stiamo usando il fatto, noto dal corso di Aritmetica, che nei PID i concetti di elemento irriducibile e di elemento primo coincidono. È facile osservare che tali concetti coincidono negli UFD (vedi esercizio 14.2.1), ma in questo momento ancora non sappiamo che R è un UFD...

Teorema 14.3.1. *Per un anello commutativo R sono equivalenti i seguenti fatti:*

1. *R soddisfa la ACC;*

2. *ogni ideale di R è generato da un numero finito di elementi.*

Dimostrazione. Supponiamo che R soddisfi la ACC. Sia I un ideale di R: dimostreremo che è generato da un numero finito di elementi. Se $I = \{0\}$ allora I è generato da un elemento. Supponiamo che I sia diverso da $\{0\}$ e sia $0 \neq a_1 \in I$. Se $I = (a_1)$ allora I è generato da un elemento, altrimenti $(a_1) \subsetneq I$ e scegliamo $a_2 \in I - (a_1)$. Se $I = (a_1, a_2)$ allora I è generato da due elementi, altrimenti $(a_1, a_2) \subsetneq I$ e scegliamo $a_3 \in I - (a_1)$. Se potessimo continuare all'infinito creeremmo una catena di ideali:

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots$$

Per la ACC questo è assurdo, dunque dopo un numero finito N di passaggi troviamo $I = (a_1, a_2, a_3, \ldots, a_N)$ e I è finitamente generato.

Viceversa, supponiamo che ogni ideale di R sia generato da un numero finito di elementi e, supponiamo di avere una catena infinita di ideali:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq ...$$

Dobbiamo dimostrare che da un certo intero positivo M in poi la catena si stabilizza. Osserviamo innanzitutto, in maniera analoga a quanto visto nella dimostrazione del Teorema 14.2.1, che

$$I = \bigcup_{i=1}^{\infty} I_i$$

è un ideale di R. Per la nostra ipotesi, è finitamente generato: $I = (a_1, ..., a_s)$. Esiste dunque un minimo N tale che I_N contiene tutti gli elementi $a_1, ..., a_s$ e quindi vale

$$I = (a_1, ..., a_s) \subseteq I_N$$

L'inclusione

$$I_N \subseteq I$$

è vera per la definizione di I, dunque possiamo concludere che $I = I_N$ e la catena di ideali si stabilizza da I_N in poi. □

14.4 Esercizi (solo un piccolo ripasso)

Esercizio 14.4.1. Mostrare che $\mathbb{Z} \times \mathbb{Z}$ non è un dominio di integrità ma i suoi ideali sono principali.

Esercizio 14.4.2. Determinare gli invertibili di $\mathbb{R}[x]/(x^2+1)$.

Esercizio 14.4.3. Determinare i divisori di zero e gli invertibili in $\mathbb{Q}[x]/(x^2-1)$.

Esercizio 14.4.4. Sia R un dominio, sia $a \in R$ e sia $\phi : R[x] \to R$ l'*omomorfismo di valutazione* in a, quello che manda $p(x)$ in $p(a)$. Dimostrare che $R[x]/(x-a) \cong R$.

Esercizio 14.4.5. Dimostrare che $\mathbb{Z}[x]/(x-2,3) \cong \mathbb{Z}_3$.

Capitolo 15

Gli automorfismi di S_n seconda parte: gli automorfismi esterni di S_6

Questo capitolo è facoltativo. Ne raccomandiamo la lettura. Lo chiederemo all'esame solo a chi dichiarerà che lo ha studiato bene.

15.1 Premessa

Come sappiamo, per $n \geq 3$ e $n \neq 6$, il gruppo $Aut(S_n)$ coincide con $Int(S_n)$, ossia tutti gli automorfismi del gruppo simmetrico sono interni, e $Int(S_n) \cong S_n$. Per $n = 2$, $S_2 \cong \mathbb{Z}_2$ e dunque $Aut(S_2) = \{e\}$. Ma cosa accade quando $n = 6$? In effetti in questo caso non è più vero che tutti gli automorfismi sono interni. Nelle pagine seguenti descriviamo un metodo (fra i moltissimi possibili[1]), per costruire e contare gli automorfismi esterni di S_6.

15.2 Spazi di configurazioni

Dato un campo K, consideriamo la retta proiettiva $\mathbb{P}(K)$ ottenuta, come sapete dal corso di Geometria 2, quozientando lo spazio $K^2 - \{(0,0)\}$ rispetto alla relazione:

$$(x, y) \sim (\gamma, \delta) \text{ se e solo se esiste } k \in K - \{0\} \text{ tale che } k(x, y) = (\gamma, \delta).$$

Definizione 15.2.1. Lo *spazio delle configurazioni* di $\mathbb{P}(K)$ di dimensione n è l'insieme

$$Conf_n(\mathbb{P}(K)) = \{(p_1, p_2, \ldots, p_n) \in \mathbb{P}(K)^n \mid p_i \neq p_j \text{ se } i \neq j\}$$

[1]Se siete interessati potete per esempio guardare l'articolo "Outer Automorphisms of S_6" di Janusz e Rotman in *The American Mathematical Monthly* 89 (1982), pagg. 407-410.

Osservazione 15.2.1. Se $\mathbb{P}(K)$ è finito e ha q elementi, l'insieme $Conf_n(\mathbb{P}(K))$ è vuoto se $n > q$. Se invece $n = q$ allora $Conf_n(\mathbb{P}(K))$ ha esattamente $n! = q!$ elementi.

In questo paragrafo giocherà un ruolo importante lo spazio $Conf_6(\mathbb{P}(\mathbb{F}_5))$, dove $\mathbb{F}_5$ è il campo con 5 elementi. Lo spazio proiettivo $\mathbb{P}(\mathbb{F}_5)$ ha 6 elementi; li elenchiamo, scrivendo ognuno di essi anche in coordinate proiettive:

$$\begin{array}{cc} 0 & [1,0] \\ 1 & [1,1] \\ 2 & [1,2] \\ 3 & [1,3] \\ 4 & [1,4] \\ \infty & [0,1] \end{array}$$

Dunque $Conf_6(\mathbb{P}(\mathbb{F}_5))$ ha 6! elementi.

Entrano adesso in scena le proiettività. Osserviamo che il gruppo $PGL(K)$ delle proiettività di $\mathbb{P}(K)$ agisce sull'insieme $Conf_n(\mathbb{P}(K))$ con l'azione naturale componente per componente: se $\phi \in PGL(K)$ allora

$$\phi \cdot (p_1, p_2, \ldots, p_n) = (\phi(p_1), \phi(p_2), \ldots, \phi(p_n)).$$

Definizione 15.2.2. Chiamiamo $\mathcal{M}_n(K)$ l'insieme delle orbite di $Conf_n(\mathbb{P}(K))$ rispetto all'azione di $PGL(K)$:

$$\mathcal{M}_n(K) = Conf_n(\mathbb{P}(K))/PGL(K)$$

Qui stiamo utilizzando la notazione, piuttosto diffusa, per cui se un gruppo G agisce su un insieme X l'insieme delle orbite viene indicato con X/G. In questi appunti studieremo in particolare

$$\mathcal{M}_6(\mathbb{F}_5) = Conf_6(\mathbb{P}(\mathbb{F}_5))/PGL(\mathbb{F}_5) =$$

$$= \{(p_1, p_2, p_3, p_4, p_5, p_6) \in \mathbb{P}(\mathbb{F}_5)^6 \mid p_i \neq p_j \text{ se } i \neq j\}/PGL(\mathbb{F}_5)$$

Quanti sono gli elementi di questo insieme? Come è noto, una proiettività è univocamente determinata una volta che viene assegnato il suo valore su tre punti della retta proiettiva, dunque preso un qualunque elemento $(p_1, p_2, p_3, p_4, p_5, p_6)$ di una $PGL(\mathbb{F}_5)$-orbita in $Conf_6(\mathbb{P}(\mathbb{F}_5))$, c'è una e una sola proiettività $\phi \in PGL(\mathbb{F}_5)$ tale che $\phi(p_1) = 0, \phi(p_2) = 1, \phi(p_6) = \infty$. Per ogni $PGL(\mathbb{F}_5)$-orbita possiamo dunque scegliere uno e un solo rappresentante della forma

$$(0, 1, q_1, q_2, q_3, \infty) \quad \text{con } q_i \neq q_j \text{ se } i \neq j \text{ e } q_i \neq 0, 1, \infty \ \forall i$$

Gli elementi di $\mathcal{M}_6(\mathbb{F}_5)$ sono tanti quanti i rappresentanti delle orbite, che a questo punto si contano facilmente: abbiamo 3 scelte per q_1 (infatti deve essere diverso da $0, 1, \infty$), 2 per q_2 e q_3 a quel punto è determinato. In conclusione $\mathcal{M}_6(\mathbb{F}_5)$ ha 6 elementi...un ottimo terreno per una azione di S_6..

15.3 L'azione di S_6 su $\mathcal{M}_6(\mathbb{F}_5)$

Facciamo agire S_n su $Conf_n(\mathbb{P}(K))$ permutando le coordinate: se $\sigma \in S_n$ allora

$$\sigma \cdot (p_1, p_2, \ldots, p_n) = (p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(n)}).$$

È immediato verificare che questa azione commuta con l'azione di $PGL(K)$ descritta nel paragrafo precedente. Consideriamo infatti $P = (p_1, p_2, \ldots, p_n) \in Conf_n(\mathbb{P}(K))$, $\sigma \in S_n$ e $\phi \in PGL(K)$ e verifichiamo che $\sigma \cdot (\phi \cdot P) = \phi \cdot (\sigma \cdot P)$:

$$(p_1, p_2, \ldots, p_n) \stackrel{\phi\cdot}{\to} (\phi(p_1), \phi(p_2), \ldots, \phi(p_n)) \stackrel{\sigma\cdot}{\to} (\phi(p_{\sigma(1)}), \phi(p_{\sigma(2)}), \ldots, \phi(p_{\sigma(n)}))$$

$$(p_1, p_2, \ldots, p_n) \stackrel{\sigma\cdot}{\to} (p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(n)}) \stackrel{\phi\cdot}{\to} (\phi(p_{\sigma(1)}), \phi(p_{\sigma(2)}), \ldots, \phi(p_{\sigma(n)}))$$

Dunque l'azione di S_n "passa" allo spazio delle orbite $\mathcal{M}_n(K)$: se $\mathscr{O} \in \mathcal{M}_n(K)$ (dunque è una $PGL(K)$-orbita in $Conf_n(\mathbb{P}(K))$) e $Q \in Conf_n(\mathbb{P}(K))$ è un suo rappresentante possiamo definire, $\forall \sigma \in S_n$,

$$\sigma \cdot \mathscr{O} = \text{l'orbita a cui appartiene } \sigma \cdot Q$$

La commutatività fra le azioni di S_n e $PGL(K)$ garantisce che questa è una buona definizione: se $\phi \cdot Q$ (con $\phi \in PGL(K)$) è un altro rappresentante della $PGL(K)$-orbita $\mathscr{O}$, allora $\sigma \cdot (\phi \cdot Q) = \phi \cdot (\sigma \cdot Q)$ che è nella stessa $PGL(K)$-orbita di $\sigma \cdot Q$.

Venendo al caso che ci interessa, abbiamo dunque un'azione di S_6 su $\mathcal{M}_6(\mathbb{F}_5)$. Questa azione dà origine ad un automorfismo esterno di S_6. Per verificarlo ordiniamo i 6 elementi di $\mathcal{M}_6(\mathbb{F}_5)$:

$$L_1 = \text{orbita con rappresentante } (0, 1, 2, 3, 4, \infty)$$

$$L_2 = \text{orbita con rappresentante } (0, 1, 2, 4, 3, \infty)$$

$$L_3 = \text{orbita con rappresentante } (0, 1, 3, 2, 4, \infty)$$

$$L_4 = \text{orbita con rappresentante } (0, 1, 3, 4, 2, \infty)$$

$$L_5 = \text{orbita con rappresentante } (0, 1, 4, 2, 3, \infty)$$

$$L_6 = \text{orbita con rappresentante } (0, 1, 4, 3, 2, \infty)$$

Consideriamo la trasposizione $(1, 2) \in S_6$ e calcoliamo $(1, 2) \cdot L_1$. Sul rappresentante dell'orbita abbiamo:

$$(1, 2) \cdot (0, 1, 2, 3, 4, \infty) = (1, 0, 2, 3, 4, \infty)$$

Dobbiamo capire a quale orbita appartiene $(1, 0, 2, 3, 4, \infty)$. Per farlo basta trovare la proiettività che riporta questo elemento ad un rappresentante canonico, ossia la proiettività ϕ tale che $\phi(1) = 0, \phi(0) = 1, \phi(\infty) = \infty$.

Pensando le proiettività nella forma $\frac{ax+b}{cx+d}$ (con $ad - bc \neq 0$) la proiettività in questione è la $\phi = 1 - x$. Applicandola a $(1, 0, 2, 3, 4, \infty)$ troviamo $(0, 1, 4, 3, 2, \infty)$ che è il rappresentante dell'orbita L_6 (ricordiamo che i numeri che compaiono sono elementi di $\mathbb{F}_5$ dunque per esempio $1 - 2 = 4$). Dunque $(1, 2) \cdot L_1 = L_6$.

A questo punto, dato che l'azione di S_6 è ben definita, sappiamo anche che $(1, 2) \cdot L_6 = L_1$. Calcoliamo adesso $(1, 2) \cdot L_3$. Sul rappresentante dell'orbita abbiamo:

$$(1, 2) \cdot (0, 1, 3, 2, 4, \infty) = (1, 0, 3, 2, 4, \infty)$$

Per capire a che orbita appartiene dobbiamo anche questa volta applicare la $\phi = 1 - x$ e otteniamo $(0, 1, 3, 4, 2, \infty)$ che è il rappresentante dell'orbita L_4. Dunque $(1, 2) \cdot L_3 = L_4$ e $(1, 2) \cdot L_4 = L_3$.

Continuando allo stesso modo otteniamo che $(1, 2) \cdot L_5 = L_2$ e $(1, 2) \cdot L_2 = L_5$.

Sappiamo già abbastanza per capire che siamo in presenza di un automorfismo esterno di S_6. Questa azione infatti induce un omomorfismo (vedi Corollario 2.2.1)

$$\theta : S_6 \to S_{|\mathcal{M}_6(\mathbb{F}_5)|} = S_6$$

e abbiamo calcolato che $\theta((1, 2)) = (1, 6)(2, 5)(3, 4)$. Se dimostriamo che θ è un automorfismo possiamo subito concludere che è esterno: infatti un automorfismo interno, ossia il coniugio per un elemento $\sigma \in S_6$, manda trasposizioni in trasposizioni.

Per ragioni di cardinalità ci basta dimostrare che l'omomorfismo θ è iniettivo.

Come sappiamo A_6 è semplice allora $Ker\ \theta \cap A_6$ è uguale a $\{e\}$ oppure ad A_6. Se fosse $Ker\ \theta = A_6$ allora l'immagine di θ conterrebbe al più 2 elementi, cosa che si esclude calcolando per esempio anche $\theta((3, 4))$ e scoprendo che $\theta((34)) = (1, 3)(2, 5)(4, 6)$.

Se invece $Ker\ \theta \cap A_6 = \{e\}$ e $Ker\ \theta \neq \{e\}$, allora sia $x \in Ker\ \theta$ una permutazione diversa da e: dunque x deve essere dispari. Ma x^2 è pari, e quindi è uguale a e. Allora x deve avere ordine 2 e ci sono solo due possibilità: può essere una trasposizione o un prodotto di tre trasposizioni disgiunte. Nel primo caso, siccome $Ker\ \theta$ è normale, allora dovrebbe contenere tutte le trasposizioni, e dunque tutto S_6, assurdo perché siamo nell'ipotesi $Ker\ \theta \cap A_6 = \{e\}$. Nel secondo caso $Ker\ \theta$ dovrebbe contenere tutti i prodotti di tre trasposizioni disgiunte: ma allora apparterrebbe a $Ker\ \theta$ anche

$$(1, 2)(3, 5)(4, 6)(4, 6)(1, 3)(2, 5) = (1, 5)(2, 3)$$

in contraddizione con $Ker\ \theta \cap A_6 = \{e\}$.

Dunque dobbiamo avere $Ker\ \theta = \{e\}$ e θ è un automorfismo esterno.

Esercizio 15.3.1. Dimostrare che $Int(S_6)$ ha indice 2 in $Aut(S_6)$, e dunque che $Aut(S_6)$ ha ordine 1440.

Capitolo 16

Esercizi aggiuntivi

Esercizio 16.0.1. Si consideri un gruppo G che agisce su un insieme X. Siano x, y elementi di X che appartengono a una stessa orbita. Dimostrare che $Stab(x)$ e $Stab(y)$ sono sottogruppi coniugati di G.

Esercizio 16.0.2. Data la permutazione $\sigma \in S_{15}$:

$$\sigma = (1, 2, 3, 4)(5, 6, 7, 8)(9, 10)$$

Calcolare la cardinalità del centralizzante $C(\sigma)$ in S_{15} e descrivere tutti i suoi elementi.

Esercizio 16.0.3. Data la permutazione $\tau \in S_{15}$:

$$\tau = (1, 2, 3, 4)(5, 6, 7, 8)(9, 10, 11, 12)(13, 14)$$

Calcolare la cardinalità del centralizzante $C(\tau)$ in S_{15} e descrivere tutti i suoi elementi.

Esercizio 16.0.4. Dimostrare che se un gruppo G non è abeliano, allora $G/Z(G)$ non è un gruppo ciclico.

Esercizio 16.0.5. Si considerino due gruppi G_1 e G_2 e un omomorfismo **surgettivo** $\phi : G_1 \to G_2$. Dimostrare che se un sottogruppo H di G_1 è normale allora $\phi(H)$ è un sottogruppo normale di G_2. Dare un controesempio se l'omomorfismo non è surgettivo.

Esercizio 16.0.6. Si considerino due gruppi G_1 e G_2 e un omomorfismo $\phi : G_1 \to G_2$. Dimostrare che se un sottogruppo K di G_2 è normale allora $\phi^{-1}(K)$ è un sottogruppo normale di G_1.

Esercizio 16.0.7. Qual è il minimo n per cui Q_8 può essere immerso in S_n?

Esercizio 16.0.8. Data la permutazione $\tau \in S_{15}$:

$$\tau = (1,2,3,4)(5,6,7,8)(9,10,11,12,13,14)$$

Calcolare la cardinalità del centralizzante $C(\tau)$ in S_{15}. Esprimere $C(\tau)$ come prodotto semidiretto.

Esercizio 16.0.9. Data la permutazione $\tau \in S_{16}$:

$$\tau = (1,2,3,4)(5,6,7,8)(9,10,11,12)(13,14)(15,16)$$

Calcolare la cardinalità del centralizzante $C(\tau)$ in S_{16}. Esprimere $C(\tau)$ come prodotto semidiretto.

Esercizio 16.0.10. Data la permutazione $\tau \in S_{10}$:

$$\tau = (1,2,3)(4,5,6)(7,8)(9,10)$$

Calcolare la cardinalità del centralizzante $C(\tau)$ in S_{16}. Esprimere $C(\tau)$ come prodotto semidiretto.

Esercizio 16.0.11 (Esercizio svolto anche a esercitazioni)**.** Sia $G = \mathbb{Z}_4 \times \mathbb{Z}_2$.
a) Dimostrare che un automorfismo ϕ di G è determinato se si conoscono $\phi([1],[0])$ e $\phi([1],[1])$.
b) Dimostrare che $Aut(G)$ ha al più 8 elementi.
c) Consideriamo $r : G \to G$ e $s : G \to G$ definite da

$$r(([x],[y])) = x([1],[1]) + y([2],[1])$$

$$s(([x],[y])) = x([1],[0]) + y([2],[1])$$

Dimostrare che le mappe r e s sono ben definite e che si tratta di elementi di $Aut(G)$.
d) Dimostrare che $Aut(G) \cong D_4$.

Esercizio 16.0.12. Dimostrare che un gruppo di ordine 144 non è semplice.

Esercizio 16.0.13. Dato $n \geq 3$, dimostrare che in S_n non esiste alcun elemento σ tale che $\sigma^3 = (1,2,3)$.

Esercizio 16.0.14. Dimostrare che $Aut(S_3 \times \mathbb{Z}_3) \cong S_3 \times \mathbb{Z}_2$.

Esercizio 16.0.15. Rivedere la dimostrazione di questo risultato, già dimostrato nel corso di Aritmetica:

$$Aut(\mathbb{Z}_p^n) \cong GL(n, \mathbb{Z}_p)$$

e in particolare

$$Aut(\mathbb{Z}_2^2) \cong S_3$$

Quanti elementi ha $Aut(\mathbb{Z}_p^n)$?

Esercizio 16.0.16. Individuare in $Aut(\mathbb{Z}_3^2)$ almeno un sottogruppo isomorfo a $\mathbb{Z}_3$. La stessa domanda con $\mathbb{Z}_3$ sostituito da $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_6$, S_3.

Esercizio 16.0.17. Trovare tutti gli elementi $\sigma \in S_6$ tali che $\sigma^4 = (1, 2, 3)$.

Esercizio 16.0.18 (compare infine il cosidetto "secondo teorema di isomorfismo per gruppi")**.** Siano H e K sottogruppi di un gruppo G, con K normale in G. Dimostrare (imitando il Lemma 4.1.1) che HK è un sottogruppo di G. Dimostrare che $K \lhd HK$, $K \cap H \lhd H$ e che

$$\frac{H}{K \cap H} \cong \frac{HK}{K}$$

Esercizio 16.0.19. Siano A e B gruppi abeliani diversi da $\{0\}$. Sia $\tau : B \to Aut(A)$ un omomorfismo diverso da quello banale. È vero o falso che il gruppo $A \rtimes_\tau B$ è non abeliano?

Esercizio 16.0.20 (Un risultato di embedding per gruppi semplici)**.** Sia G un gruppo semplice. Dimostrare che, se G ammette un sottogruppo di indice n, allora esiste un omomorfismo iniettivo da G ad A_n.

Esercizio 16.0.21. Dimostrare che un gruppo di ordine 112 non è semplice. [Suggerimento: usare il risultato di embedding dell'esercizio precedente.]

Esercizio 16.0.22 (ecco il cosidetto "terzo teorema di isomorfismo per gruppi")**.** Sia G un gruppo, e siano H e K due suoi sottogruppi normali tali che $H \subset K$. Allora vale

$$\frac{G/H}{K/H} \cong G/K$$

Esercizio 16.0.23. Con le definizioni date in queste dispense, è vera o falsa la seguente affermazione: una estensione di campi $F \subseteq E$ è di Galois se e solo se E è il campo di spezzamento di un polinomio $f(x) \in F[x]$ irriducibile e separabile?

Esercizio 16.0.24. Esibire un polinomio $f(x)$ di grado 5 in $\mathbb{Q}[x]$ tale che il gruppo di Galois del suo campo di spezzamento su $\mathbb{Q}$ sia S_5.

Esercizio 16.0.25. Sia $\{G_i \mid i \in I\}$ una collezione di gruppi (con $|I| > 1$) non banali (ossia $|G_i| > 1$ per ogni i). Dimostrare che il prodotto libero $\mathcal{G}$ dei gruppi G_i è non abeliano, contiene un elemento di ordine infinito e che il centro $Z(\mathcal{G})$ è banale.

Esercizio 16.0.26. Siano m e n due interi maggiori di 1 e consideriamo i gruppi $G \cong \mathbb{Z}_m$ e $H \cong \mathbb{Z}_n$. Dimostrare che gli unici elementi di $G * H$ che hanno ordine finito sono gli elementi di G e di H e tutti i loro coniugati.

Esercizio 16.0.27. Sia $\{G_i \,|\, i \in I\}$ una collezione di gruppi (con $|I| > 1$) non banali (ossia $|G_i| > 1$ per ogni i). Sia $\mathcal{G}$ il prodotto libero dei gruppi G_i. Dimostrare che per ogni coppia di elementi distinti $i, j \in I$ i sottogruppi G_i e G_j non sono coniugati. [Suggerimento: potete utilizzare il fatto, valido in generale, che se un sottogruppo H è contenuto nel nucleo di un omomorfismo di gruppi, allora anche ogni coniugato di H è contenuto nel nucleo...]

Esercizio 16.0.28. Sia $E \subset \mathbb{C}$ il campo di spezzamento di x^3-2 su $\mathbb{Q}$. Individuare il gruppo di Galois $Aut(E/\mathbb{Q})$ e identificare tutti i sottocampi K con $\mathbb{Q} \subset K \subset E$.

Esercizio 16.0.29. Sia $F \subset E$ una estensione di campi. Dimostrare che l'insieme K degli elementi di E che sono separabili su F è un campo.

Esercizio 16.0.30. Sia $n \in \mathbb{N} - \{0\}$ e sia K una estensione di $\mathbb{Q}$ che contiene le radici ennesime di 1. Sia $K \subset L$ una estensione di Galois il cui gruppo di Galois $Aut(L/K)$ sia isomorfo a $\mathbb{Z}_n$, e sia generato dall'automorfismo ϕ. Supponiamo di sapere che per un elemento $\alpha \in L$ vale $\phi(\alpha) = \zeta\alpha$. Dimostrare che $L = K(\alpha)$ e che il polinomio minimo di α su K è del tipo $x^n - a$ per $a \in K$.

Esercizio 16.0.31 (Generalizzazione della Proposizione 12.1.1)**.** Dati due interi positivi s, t, dimostrare che

$$\mathbb{Q}(\zeta_s, \zeta_t) = \mathbb{Q}(\zeta_{mcm(s,t)})$$

$$\mathbb{Q}(\zeta_s) \cap \mathbb{Q}(\zeta_t) = \mathbb{Q}(\zeta_{MCD(s,t)}).$$

Esercizio 16.0.32. Sia $K = \mathbb{Q}(\sqrt{3})$. Dire se è vero o falso che

$$K(\zeta_3) \cap K(\zeta_4) = K$$

Esercizio 16.0.33. Sia n un intero positivo e sia p un primo che non divide n. Sia E il campo di spezzamento del polinomio $x^n - 1$ su $\mathbb{F}_p$. Dimostrare che il grado di E su $\mathbb{F}_p$ è uguale all'ordine moltiplicativo di $[p]$ in $\mathbb{Z}_n^*$. Qual è il gruppo di Galois $Aut(E/\mathbb{F}_p)$?

Esercizio 16.0.34. Eventualmente utilizzando il risultato dell'esercizio precedente, fattorizzare $x^7 - 1$ in $\mathbb{F}_p[x]$ con $p = 2, 3, 13, 29$.

Esercizio 16.0.35. Sia n un intero positivo e sia p un primo che non divide n. Sia E il campo di spezzamento del polinomio $x^n - 1$ su $\mathbb{F}_{p^m}$. Qual è il grado di E su $\mathbb{F}_{p^m}$?

Esercizio 16.0.36. Sia n un intero positivo e sia p un primo che non divide n. Indichiamo con $\overline{\Phi}_n(x)$ la proiezione del polinomio ciclotomico $\Phi_n(x)$ in $\mathbb{Z}_p[x]$. Dimostrare che i fattori irriducibili di $\overline{\Phi}_n(x)$ in $\mathbb{Z}_p[x]$ sono distinti fra loro e ognuno ha grado uguale all'ordine moltiplicativo di $[p]$ in $\mathbb{Z}_n^*$.

Esercizio 16.0.37. Dimostrare che $\Phi_8(x) = x^4 + 1$ non è irriducibile in $\mathbb{Z}_p[x]$ per ogni primo p. Fattorizzarlo per i primi $p = 2, 3, 5, 7, 11, 17$.

Esercizio 16.0.38. Sia E il campo di spezzamento su $\mathbb{Q}$ del polinomio $(x^2 - x - 1)(x^4 + 5)$. Determinare il grado di E su $\mathbb{Q}$ e il gruppo di Galois dell'estensione $\mathbb{Q} \subset E$.

Esercizio 16.0.39. Sia $K \subset E$ una estensione di Galois di campi tale che

$$Aut(E/K) \cong D_{12}$$

Quanti sono i sottocampi di E che contengono K e hanno grado 2 su K?

Esercizio 16.0.40 (facile, e discusso in classe varie volte, controllate di saperlo fare)**.** Siano n_1, n_2 due interi diversi da 0 e 1 e liberi da quadrati. Se $n_1 \neq n_2$, dimostrare che l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ è di Galois e calcolare il gruppo di Galois.

Bibliografia

[DM] P. Di Martino, *Algebra*, Pisa University Press 2013.

[He] I.N. Herstein, *Algebra*, Editori Riuniti, 1982 o ristampe. Titolo originale: *Topics in algebra*.