Appunti di Algebra 2

12 giugno 2022

Indice

1 Moduli **2**

2 Azioni di gruppi e teoremi di Sylow **26**

3 Campi **47**
3.1 Estensioni di campi 47
3.2 Campi di spezzamento 55
3.3 Separabilità 58
3.4 Teoria di Galois 60
3.5 Equazioni polinomiali 67
3.6 Campi ciclotomici 74
3.7 Discriminante 78
3.8 Polinomi non risolubili per radicali 79

Notazione $\mathbb{N} := \{1, 2, 3, \ldots\}$. Se E è un insieme, $|E|$ o $\#E$ indica la sua cardinalità. Se G è un gruppo, $|G|$ oppure $o(G)$ indica il suo ordine. Il simbolo $A \subset B$ significa che A è sottoinsieme di B, ma non si esclude che $A = B$. Stesso discorso per i sottogruppi normali: se $N \lhd G$, può essere che $N = G$.

Tutti gli anelli considerati sono con unità. Tutti i morfismi di anelli mandano 1 in 1.

Capitolo 1

Moduli

Sia A un anello commutativo. La definizione di modulo su un anello A è identica a quella di spazio vettoriale, basta lasciar cadere la richiesta che gli scalari stiano in un campo accontentandosi che appartengano ad un anello.

Definizione 1. *Un modulo su A (brevemente un A-modulo) è un insieme M munito di due operazioni di somma $+$ e prodotto $\cdot$ che soddisfano le proprietà seguenti:*

1. *$(M, +)$ è un gruppo abeliano;*
2. *per ogni $a, a' \in A$ e $x, x' \in M$*

$$\begin{aligned} (a + a')x &= a + a'x, & (aa')x &= a(a'x) \\ a(x + x') &= ax + ax', & 1x &= x. \end{aligned}$$

Segue

$$\lambda \cdot 0_M = 0_M, \qquad 0 \cdot x = 0_M, \qquad (-1) \cdot x = -x.$$

Se $(M, +)$ è un gruppo abeliano, allora $\mathrm{End}(M, +)$ è un anello. Una struttura di A-modulo su M è equivalente a un morfismo di annelli $\alpha : A \to \mathrm{End}(M, +)$.

Esempi: gruppi abeliani; ideali come A-moduli; caso di A non commutativo: A^{op}, moduli destri e sinistri e bilateri; campi vettoriali; V come $\mathrm{End}\, V$ modulo; V come $k[x]$-modulo.

Sottomoduli. Sottomodulo generato $\langle S\rangle$: è l'insieme delle combinazioni lineari e anche l'intersezione di tutti i sottomoduli contententi S. Generatori. Moduli finitamente generati. Somma di sottomoduli di un modulo fissato. Se $I \subset A$ è un ideale e $M' \subset M$ è un sottomodulo, allora $I \cdot M' = \langle \lambda \cdot x | \lambda \in I, x \in M' \rangle$ è un sottomodulo.

Morfismi. Morfismi (o omomorfismi) di A-moduli: $f : M \to N$. L'inclusione di un sottomodulo è lineare. La composizione di morfismi è un morfismo. Nucleo e immagine sono sottomoduli. Iniettività $\Leftrightarrow \ker f = \{0\}$. Un morfismo biunivoco è un isomorfismo. Un morfismo manda sottomoduli in sottomoduli e le immagini inverse di sottomoduli sono sottomoduli. $f(\langle S\rangle) = \langle f(S)\rangle$.

$\mathrm{Hom}_A(M, N)$ è un modulo.

Modulo quoziente.

Sottomoduli di un modulo quoziente. Sia M' un sottomodulo di M. Indichiamo con $\pi : M \to M/M'$ la proiezione canonica sul quoziente. Se M'' è un sottomodulo di M e $M' \subset M''$, allora M''/M' è un sottoinsieme di M/M'. Infatti $M''/M' = \pi(M'')$. Ogni sottomodulo di M/M' si può scrivere in questo modo e in un unico modo. Infatti se Q è un sottomodulo di M/M', poniamo $M'' := \pi^{-1}(Q)$. Allora M'' contiene M' e $Q = \pi(\pi^{-1}(Q))$ (perché π è suriettiva) cioè $Q = \pi(M'') = M''/M'$. Se poi c'è un altro sottomodulo $M''' \subset M$ che contiene M' e tale che $Q = M'''/M' = \pi(M''')$, allora $M''' \subset \pi^{-1}(Q) = \pi^{-1}(Q) = M''$. Ma vale anche l'inclusione opposta: sia $x \in M''$; allora $\pi(x) \in Q = \pi(M''')$. Dunque esiste $y \in M''$ tale che $\pi(y) = \pi(x)$. Quindi $x - y \in \ker \pi = M' \subset M'''$, per cui $x = (x-y)+y \in M'''$. Quindi effettivamente $M'' \subset M'''$, ossia $M'' = M'''$. Questo dimostra che la rappresentazione $Q = M''/M'$ è unica.

Teorema di omomorfismo. I Teorema di isomorfismo: $\mathrm{im}\, f \cong M/\ker f$. II Teorema di isomorfismo: $(M' + M'')/M'' \cong M'/M' \cap M''$. III Teorema di isomorfismo: se $M'' \subset M' \subset M$, allora

$$\frac{M/M''}{M'/M''} \cong M/M'.$$

Somma diretta e prodotto diretto. Sottomoduli di M in somma diretta (interna). Sia M un A-modulo e siano $M_1, \ldots, M_n$ sottomoduli. Diciamo che sono *in somma diretta* o *indipendenti* se per ogni $i = 1, \ldots, n$ si ha

$$M_i \cap \textstyle\sum_{j \neq i} M_j = \{0\}.$$

Lemma 2. *Le seguenti condizioni sono equivalenti:*

1. *i sottomoduli M_i sono indipendenti;*
2. *se $x_i \in M_i$ per ogni $i = 1, \dots, n$, allora $\sum_i x_i = 0 \Longrightarrow x_i = 0$ per ogni i.*
3. *per ogni $x \in \sum_i M_i$ la scrittura $x = x_1 + \cdots + x_n$ con $x_i \in M_i$ è unica.*

Somma diretta (esterna) di un numero finito di moduli: basta prendere il prodotto cartesiano e definire le operazioni componente per componente.

Proposizione 3. *Siano $M_i \subset M$ sottomoduli per $i = 1, \dots, n$. Consideriamo l'applicazione $f : \oplus_i M_i \to M$ indotta dalle inclusioni $M_i \hookrightarrow M$. Allora*

1. *$f(x_1, \dots, x_n) = \sum_i x_i$;*
2. *$\operatorname{im} f = \sum_i M_i$.*
3. *I sottomoduli M_i sono indipendenti se e solo se f è un isomorfismo.*

Il prodotto cartesiano. $X^n = X^{\{1,\dots,n\}}$. X^Y. Prodotto cartesiano infinito: $\times_{\alpha \in I} Z_\alpha$.

Prodotto diretto di moduli.

Proiezioni $\mathrm{pr}_\beta : \times_\alpha M_\alpha \to M_\beta$.

Proprietà universale del prodotto. Somma diretta. Iniezioni $\mathrm{in}_\beta : M_\beta \hookrightarrow \oplus_\alpha M_\alpha$. Proprietà universale della somma diretta. Esempio che fa vedere la differenza: nel caso infinito la mappa definita sul prodotto diretto non è unica.

Cenni su prodotti e coprodotti in una categoria.

Addendo diretto.

Indipendenza lineare in un modulo.

Basi.

$\mathbb{Z}/n$ non ha nessuna base come $\mathbb{Z}$-modulo! Moduli liberi. A^n è libero. Un modulo libero con una base di n elementi è isomorfo ad A^n. Morfismi da un modulo libero.

Se M è un modulo e $M_1, M_2 \subset M$ sottomoduli, allora l'insieme

$$(M_1 : M_2) := \{a \in A : aM_2 \subset M_1\}$$

è un ideale di A. Definiamo l'annullatore di M come $\operatorname{Ann} M := (0 : M)$.

Annullatore. $\operatorname{Ann} M := \{a \in A : ax = 0, \forall x \in M\}$ è un ideale. Per spazi vettoriali si ha sempre $\operatorname{Ann} V = \{0\}$. M è un $A/\operatorname{Ann} M$-modulo. Più in generale, se $I \subset \operatorname{Ann} M$ allora M è un A/I-modulo con la seguente moltiplicazione per scalare:

$$(a + I) \cdot (x + IM) := ax + IM.$$

Se la struttura di A-modulo su M corrisponde al morfismo di anelli $\alpha : A \to \operatorname{End}(M, +)$, allora $\operatorname{Ann} M = \ker \alpha$. Dunque è chiaro che $\operatorname{Ann} M$ è un ideale e che α induce un morfismo $\tilde{\alpha} : A/\operatorname{Ann} M \to \operatorname{End}(M, +)$, ossia una struttura di $A/\operatorname{Ann} M$-modulo su M. Per esempio se $M = \mathbb{Z}/n$ ed $A = \mathbb{Z}$, allora $\operatorname{Ann} M = n\mathbb{Z}$ e dunque $\mathbb{Z}/n$ è uno $\mathbb{Z}/n$ modulo.

Lemma 4. *Se M è un A-modulo e $I \subset A$ è un ideale, allora M/IM è un A/I-modulo.*

Dimostrazione. IM è un sottomodulo di M, dunque M/IM è un A-modulo. Inoltre $I \subset \operatorname{Ann}(M/IM)$. □

Esercizio 5. *Sia A un anello commutativo e $\mathfrak{m} \subset A$ un ideale massimale. Poniamo $F := A/\mathfrak{m}$. Se M è un A-modulo poniamo $v(M) := M/\mathfrak{m} \cdot M$. Se $f : M \to M'$ è un morfismo di A-moduli, dimostrare che c'è una applicazione lineare $v(f) : v(M) \to v(M')$ ben definita e dimostrare che v è un funtore dalla categoria degli A-moduli a quella degli F-spazi vettoriali. In particolare se due moduli M ed M' sono isomorfi, allora gli spazi vettoriali $v(M)$ e $v(M')$ sono isomorfi.*

6. Moduli *ciclici*. Se M è ciclico, $M = A/I$ e $\operatorname{Ann} M = I$. $A/I \cong A/J$ come moduli $\Leftrightarrow I = J$. Si noti che l'isomorfismo $A/I \cong A/J$ come moduli è più forte del corrispondente isomorfismo come anelli. Esempio $A = \mathbb{C}[X]$ $I = (x)$, $J = (x - 1)$. Altro esempio: sia $\chi : \mathbb{C} \to \mathbb{C}$ il coniugio. Allora è un morfismo di anelli, ma non è $\mathbb{C}$-lineare.

L'insieme $\{0\}$ con le operazioni banali è un anello in cui $0 = 1$. Nel parlare di basi dobbiamo escludere questo caso degenere.

Lemma 7. *Sia A un anello, $A \neq \{0\}$ e sia $I \subsetneq A$ un ideale. Sia poi M un A-modulo libero con base $\mathscr{B} = \{e_\alpha\}_{\alpha \in J}$. ($J$ è un insieme, non necessariamente finito, di indici.) Allora $\overline{\mathscr{B}} = \{e_\alpha + IM\}_{\alpha \in J}$ è una base di M/IM come A/I-modulo.*

Dimostrazione. È evidente che $\overline{\mathscr{B}}$ genera. Vediamo che è linearmente indipendente. Sia

$$\sum_\alpha (\lambda_\alpha + I)(e_\alpha + IM) = 0,$$

dove solo un numero finito degli λ_α sono non nulli. Dunque $\sum_\alpha \lambda_\alpha e_\alpha \in IM$. Dunque esistono $y_j \in M$ e $\mu_j \in I$ tali che $\sum_\alpha \lambda_\alpha e_\alpha = \sum_j \mu_j y_j$. Ma $y_j = \sum_\beta a_{\beta j} e_\beta$ per opportuni $a_{\beta j} \in A$. Dunque

$$\sum_\alpha \lambda_\alpha e_\alpha = \sum_\beta (\sum_j a_{\beta j}\mu_j) e_\beta.$$

Quindi $\lambda_\alpha = \sum_j a_{\alpha j}\mu_j \in I$, cioè $\lambda_\alpha + I = 0$ in A/I. Questo dimostra che $\overline{\mathscr{B}}$ è anche linearmente indipendente, dunque è una base. □

Teorema 8. *Sia $A \neq \{0\}$. Allora tutte le basi di un A-modulo libero hanno la stessa cardinalità, che viene chiamata* dimensione *o* rango *del modulo.*

Dimostrazione. Osserviamo che per spazi vettoriali su un campo questo teorema lo conosciamo. Cerchiamo quindi di ricondurci agli spazi vettoriali, sfruttando gli ultimi due lemmi. Siano $\mathscr{B}_1 = \{e_\alpha\})_{\alpha \in J}$ e $\mathscr{B}_2 = \{f_\beta\}_{\beta \in K}$ due basi di M. Siccome $A \neq \{0\}$ possiamo fissare un ideale massimale $\mathfrak{m} \subsetneq A$. Allora $k := A/\mathfrak{m}$ è un campo e $V := kM/\mathfrak{m}M$ è uno spazio vettoriale su k (Lemma 4). Per il precedente lemma $\overline{\mathscr{B}}_1 = \{e_\alpha + \mathfrak{m}M\})\alpha \in J$ e $\overline{\mathscr{B}}_2 = \{f_\beta + \mathfrak{m}M\}_{\beta \in K}$ sono due basi di V. Ma allora $\overline{\mathscr{B}}_1$ e $\overline{\mathscr{B}}_2$ hanno la stessa cardinalità. Dunque lo stesso vale per $\mathscr{B}_1$ e $\mathscr{B}_2$. □

Osservazione: sia M un A/I-modulo. È anche un A-modulo e i sottomoduli sono gli stessi.

Corollario 9. *Se F è un modulo libero e finitamente generato, allora ogni base di F è finita. Se una base contiene n elementi, allora tutte le basi di F contengono n elementi ed F è isomorfo ad A^n. Inoltre A^n è isomorfo ad A^m se e solo se $n = m$.*

Moduli semplici. A è un A-modulo semplice se e solo se A è un campo. Gruppi abeliani semplici. Un modulo ciclico è semplice se e solo se $M = A/\mathfrak{m}$ con $\mathfrak{m}$ massimale.

Torsione Consideriamo moduli su domini. Un elemento $x \in M$ è di torsione se $\mathrm{Ann}(x) \neq \{0\}$. $T(M) = \{\text{tutti gli elementi di torsione}\}$ è un sottomodulo. Se $T(M) = \{0\}$ dico che M è senza torsione (torsion-free).

M è di torsione se $M = T(M)$.

Se M è un gruppo abeliano, $T(M)$ è formato da tutti gli elementi di ordine finito.

$T(M/T(M)) = \{0\}$. (Usa che A è dominio.) Un sottomodulo di un modulo senza torsione è senza torsione.

Un modulo libero è senza torsione.

Moduli su domini a ideali principali.

Teorema 10. *Sia A un dominio a ideali principali e sia F un A-modulo libero di dimensione n. Sia $K \subset F$ un sottomodulo. Allora K è un modulo libero di dimensione $\leq n$.*

Dimostrazione. Sia $e_1, \ldots, e_n$ una base di K. Per $r = 1, \ldots, n$ poniamo $F_r := Ae_1 + \cdots Ae_r$. Vogliamo provare che $K \cap F_r$ è libero di dimensione $\leq r$. Per $r = n$ si otterrà la tesi. Procediamo per induzione. Per $r = 1$ osservo che grazie all'isomorfismo $A \to Ae_1 = F_1, x \mapsto xe_1$ il sottomodulo $K \cap F_1$ risulta isomorfo a un sottomodulo di A, ossia a un ideale $J \subset A$. Ma allora o $J = \{0\}$ (e siamo a posto) oppure $J = (u)$ con $u \neq 0$. In questo secondo caso $\{u\}$ è una base di J (perché A è un dominio di integrità) e ue_1 sarà una base di $K \cap F_1$. Veniamo al passo induttivo. Supponiamo che $K \cap F_r$ ammetta una base $\{v_1, \ldots, v_s\}$ con $s \leq r$. Indichiamo con $\varphi_i : F \to A$ la i-esima coordinata rispetto alla base $\{e_i\}$. Allora $J := \varphi_{r+1}(K \cap F_{r+1})$ è un ideale. Se è l'ideale nullo, vuol dire che $K \cap F_{r+1} = K \cap F_r$ e abbiamo finito il passo induttivo. Altrimenti avremo $J = (u)$ per $u \neq 0$. Fissiamo $w \in K \cap F_{r+1}$ tale che $\varphi_{r+1}(w) = u$. Vogliamo dimostrare che $\mathscr{B} = \{w, v_1, \ldots, v_s\}$ è una base di $K \cap F_{r+1}$. Questo completerà il passo induttivo e la dimostrazione. Sia $x \in K \cap F_{r+1}$. Siccome $\varphi_{r+1}(x) \in J$, si avrà $\varphi_{r+1}(x) = \lambda u$ per qualche $\lambda \in A$. Dunque $\varphi_{r+1}(x - \lambda w) = 0$, cioè $x - \lambda w \in K \cap F_r$. Quindi ci saranno $\lambda_i \in A$ tali che $x = \lambda w + \lambda_1 v_1 + \cdots + \lambda_s v_s$. Abbiamo dimostrato che $\mathscr{B}$ è un sistema di generatori. Ora supponiamo di avere $\lambda, \lambda_i \in A$ tali che $\lambda w + \lambda_1 v_1 + \cdots + \lambda_s v_s = 0$. Allora $\varphi_{r+1}(\lambda w) = 0$, perché $\varphi_{r+1}(v_j) = 0$. Dunque $\lambda u = 0$. Ma allora, siccome A è un dominio, $\lambda = 0$ e quindi $\lambda_1 v_1 + \cdots + \lambda_s v_s = 0$. Segue $\lambda_i = 0$. □

Esercizio 11. *Sia A un dominio di integrità e sia $I \subset A$ un ideale principale. Allora I è un A-modulo libero di dimensione ≤ 1.*

12. Nel teorema precedente l'ipotesi che A sia un dominio a ideali principali è necessaria. Infatti sia A un anello e supponiamo che valga il teorema per gli A-moduli. Prendiamo come modulo $F = A$ e sia K un ideale di A. Allora K è un sottomodulo che deve essere libero di rango al massimo 1. Se $K = \{0\}$ questo è vero banalmente. Se invece $K \neq \{0\}$, deve esistere $a \in K$ tale che $\{a\}$ sia una base di K. Ma allora $K = Aa$, cioè K è un ideale principale. Inoltre $\lambda \cdot a = 0 \Rightarrow \lambda = 0$. Pertanto A è un dominio.

Lemma 13. *Sia A un anello a ideali principali e sia $\mathscr{F}$ una famiglia non vuota di ideali di A. Allora esiste un elemento massimale in $\mathscr{F}$.*

Dimostrazione. Fissiamo $I_1 \in \mathscr{F}$. Se I_1 è massimale in $\mathscr{F}$, abbiamo finito. Altrimenti esiste $I_2 \in \mathscr{F}$ tale che $I_1 \subsetneq I_2$. Se di I_2 è massimale in $\mathscr{F}$ abbiamo finito. Altrimenti esiste I_3 e andiamo avanti. In questo modo produciamo una successione di elementi di $\mathscr{F}$: $I_1 \subsetneq_2 \subsetneq \cdots \subsetneq I_k$. Se a un certo punto I_k è massimale, la successione si ferma e abbiamo finito. Altrimenti otteniamo una successione infinita

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots$$

Vediamo che questo caso non succede. Infatti poniamo $J := \cup_i I_i$. J è un ideale, dunque $J = (a)$ e $a \in \cup_i I_i$, quindi $a \in I_k$. Ma allora $\cup_i I_i = I_k$ e quindi in particolare $I_k = I_{k+1}$, assurdo. □

Lemma 14. *Sia A un dominio di integrità e sia F un A-modulo libero. Se $u \in F$, $u \neq 0$, allora $\lambda u = 0 \Rightarrow \lambda = 0$.*

Dimostrazione. Sia $\{e_\alpha\}$ una base di F e sia $u = \sum_\alpha u_\alpha e_\alpha$. Allora $\lambda u = \sum_\alpha \lambda u_\alpha e_\alpha = 0$ implica che $\lambda u_\alpha = 0$ per ogni α. Siccome $u \neq 0$ esiste $\bar{\alpha}$ tale che $u_{\bar{\alpha}} \neq 0$. Ma allora da $\lambda u_{\bar{\alpha}} = 0$ segue $\lambda = 0$ perché A è un dominio. □

Poniamo $F^* = \mathrm{Hom}(F, A)$. Se F è un modulo libero ed $\{e_1, \ldots, e_n\}$ è una base, definiamo le funzioni coordinate $\varphi_i : F \to A$, mediante la forumula $\varphi_i(x_1 e_1 + \cdots x_n e_n) := x_i$. Le funzioni coordinate sono elementi di F^*.

Lemma 15. *Sia A un dominio a ideali principali. Sia F un modulo libero di dimensione n e sia $K \subset F$ un sottomodulo, $K \neq \{0\}$. Allora possiamo trovare $x \in F$ e $a \in A$ tali che*

1. *se $\varphi : F \to A$ è A-lineare e $(a) \subset \varphi(K)$, allora $(a) = \varphi(K)$;*
2. *$y := ax \neq 0$ e $y \in M$;*
3. *$F = Ax \oplus F'$ per un certo sottomodulo $F' \subset F$;*

4. $K = Ay \oplus K'$ *con* $K' = K \cap F'$.

Dimostrazione. Sia $\mathscr{F} := \{\varphi(K) : \varphi \in F^*\}$. Sia $\alpha \in F^*$ tale che $\alpha(K)$ è massimale in $\mathscr{F}$. Sia $a \in A$ tale che $\alpha(K) = (a)$. Vale per costruzione la proprietà 1. Vogliamo mostrare che $a \neq 0$. Fissiamo una base qualsiasi $\{e_1, \ldots, e_n\}$ di F. Sia $\varphi_i : F \to A$ la funzione coordinata che manda l'elemento $\sum_{j=0}^{n} x_j e_j \in F$ in x_i. Le funzioni φ_i sono elementi di F^*. Siccome $K \neq \{0\}$, esiste almeno un indice i tale che $\varphi_i(K) \neq \{0\}$. Dunque anche $\alpha(K) \neq \{0\}$ e quindi $a \neq 0$ come volevamo. Sia poi $y \in K$ tale che $\alpha(y) = a$. Siccome $a \neq 0$, anche $y \neq 0$. Ora dimostriamo la proprietà seguente: a divide $\varphi(y)$ per ogni $\varphi \in F^*$. Infatti fissiamo $\varphi \in F^*$ e consideriamo l'ideale $I := (a, \varphi(y))$. Siccome A è un dominio a ideali principali esiste $b \in A$ tale che $I = (b)$ e inoltre $b = ua + v\varphi(y)$ per opportuni $u, v \in A$. Sia $\psi := u\alpha + v\varphi \in F^*$. Allora $\psi(y) = b$. Dunque $b \in \psi(K)$. Ma $b|a$ dunque $\alpha(K) = (a) \subset (b) \subset \psi(K)$. Siccome $\alpha(K)$ è massimale, concludiamo che $(a) = (b) = \psi(K)$. Dunque a divide b cioè divide $\varphi(y)$ come desiderato. Sfruttiamo di nuovo la base di F $\{e_1, \ldots, e_n\}$ fissata all'inizio. Come già osservato le funzioni coordinate φ_i sono elementi di F^*. Dunque per la proprietà che abbiamo appena dimostrato, se $y = \sum_i y_i e_i$, tutte le coordinate $y_i = \varphi_i(y)$ sono divise da a, cioè esistono elementi x_i tali che $y_i = ax_i$. Poniamo $x := \sum_i x_i e_i$. Allora $y = ax$ e abbiamo sistemato intanto il punto 2. Inoltre $\alpha(x) = 1$. Poniamo $F' := \ker \alpha$, $K' := K \cap \ker \alpha$. È evidente che $F' \cap Ax = \{0\}$. Dunque anche $K' \cap Ay = \{0\}$. Se $z \in F$. Quindi

$$z = \alpha(z)x + (z - \alpha(z)x),$$

e $z - \alpha(z) \in \ker \alpha$. Dunque $F = Ax \oplus F'$. Se poi $z \in K$, allora $\alpha(z) \in (a)$, dunque $\alpha(z) = \lambda a$. Allora

$$z = \lambda y + (z - \lambda y).$$

E di nuovo $\alpha(z - \lambda y) = \alpha(z) - \lambda a = 0$. Quindi $K = Ay \oplus K'$. □

Teorema 16. *Sia A un dominio a ideali principali e sia F un A-modulo libero di dimensione n. Sia $K \subset F$ un sottomodulo. Allora possiamo trovare una base $\{x_1, \ldots, x_n\}$ di F e degli elementi non nulli $a_1, \ldots, a_m \in A$, con $m \leq n$ e $a_i | a_{i+1}$, tali che $\{a_1 x_1, \ldots, a_m x_m\}$ sia una base di K.*

Dimostrazione. Procediamo per induzione su $\dim F$. Se $\dim F = 0$, $K = \{0\}$ e non c'è niente da dimostrare. Supponiamo vero il risultato per moduli liberi di dimensione $< n$ e sia $\dim F = n$. Siano $x_1 \in F$, $a_1 \in A$, $y_1 := a_1 x_1 \in K$, F' e K' gli oggetti forniti dal lemma precedente. Per il Teorema 10 F'

è un sottomodulo libero e avrà dimensione $n-1$, visto che $F = Ax_1 \oplus F'$. Possiamo applicare l'ipotesi induttiva al sottomodulo $K' \subset F'$: possiamo trovare una base $\{x_2, \dots, x_n\}$ di F' e degli elementi $a_2, \dots, a_m \in A$, $m \leq n$ tali che $\{a_2x_2, \dots, a_mx_m\}$ sia una base di K'. Siccome $F = Ax_1 \oplus F'$, segue, grazie al Lemma 14, che $\{x_1, \dots, x_n\}$ è una base di F e che $\{a_1x_1, \dots, a_mx_m\}$ è una base di K. Resta da dimostrare la condizione di divisibilità. Per l'ipotesi induttiva $a_2|a_3|\cdots|a_m$, quindi basta provare che $a_1|a_2$. Siccome $\{x_i\}$ è una base, esiste un morfismo $\varphi : F \to A$ che soddisfa $\varphi(x_1) = \varphi(x_2) = 1$. Allora $\varphi(y_1) = a_1$. Dunque $a_1 \in \varphi(K)$, quindi $(a_1) \subset \varphi(K)$. Per la proprietà 1 del Lemma 15 concludiamo $(a_1) = \varphi(K)$. Ma e $\varphi(a_2x_2) = a_2$, dunque $a_2 \in (a_1)$, cioè $a_1|a_2$. □

17. Se $A = K$ è un campo, questo teorema afferma che esiste una base dello spazio vettoriale F i cui primi elementi m formano una base del sottospazio $K \subseteq F$. Quindi il teorema può essere visto come una generalizzazione di questo fatto ben noto.

Teorema cinese del resto. *Sia A un anello commutativo e siano $I_1, \dots, I_n$ degli ideali. Supponiamo che $I_i + I_j = A$ per $i \neq j$. Allora*

$$A/I_1 \cdots I_n \cong A/I_1 \oplus \cdots \oplus A/I_n.$$

Lemma 18. *Sia $I \subset A$ un ideale e siano $a_1, \dots, a_n \in I$. Allora $1 - (1 - a_1) \cdots (1 - a_n) \in I$.*

Dimostrazione. Induzione su n. Per $n = 1$ è ovvio. Supponiamo che sia vero per $n-1$. Poniamo $z := (1-a_1)\cdots(1-a_{n-1})$. L'ipotesi induttiva dice che $1 - z \in I$. Ma allora $1 - (1-a_1)\cdots(1-a_n) = 1 - z(1-a_n) = 1 - z + za_n$. Siccome $a_n \in I$, anche $za_n \in I$. Quindi otteniamo che $1 - (1-a_1)\cdots(1-a_n) \in I$ come desiderato. □

Lemma 19. *Nelle ipotesi del teorema cinese del resto, si ha $I_1 \cdots I_{k-1} + I_k = A$ per ogni k.*

Dimostrazione. Per ipotesi se $i < k$ esistono $a_i \in I_k$ e $b_i \in I_i$ tali che $a_i + b_i = 1$. Per il lemma precedente $z := 1 - b_1 \cdots b_{k-1} = 1 - (1-a_1)\cdots(1-a_k) \in I_k$. Mentre $b_1 \cdots b_{k-1} \in I_1 \cdots I_{k-1}$. Quindi $1 = b_1 \cdots b_{k-1} + z \in I_1 \cdots I_{k-1} + I_k$. □

Lemma 20. *Nelle ipotesi del teorema cinese del resto $I_1 \cap \cdots \cap I_K = I_1 \cdots I_k$ per ogni k.*

Dimostrazione. Procediamo per induzione su k. L'inclusione $\supseteq$ vale sempre. Per dimostrare $\subset$ sia $z \in I_1 \cap \cdots \cap I_{k+1} = (I_1 \cdots I_k) \cap I_{k+1}$ (ipotesi induttiva!). Per il lemma precedente $1 = u + v$ per opportuni $u \in I_1 \cdots I_k$ e $v \in I_{k+1}$. Allora $z = zu + zv$ ed entrambi i termini stanno in $I_1 \cdots I_{k+1}$. □

Dimostrazione del teorema cinese del resto. Sia $\pi_i : A \to A/I_i$ la proiezione canonica. Consideriamo la mappa

$$f = \pi_1 \times \cdots \times \pi_n : A \to A/I_1 \oplus \cdots \oplus A/I_n,$$
$$f(x) = (\pi_1(x), \ldots, \pi_n(x)).$$

Il nucleo è $\ker \pi_1 \cap \cdots \cap \ker \pi_n = I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ (Lemma 20). Per il teorema di omomorfismo f induce una mappa

$$\tilde{f} : A/I_1 \cdots I_n \to A/I_1 \oplus \cdots \oplus I_n$$

e questa mappa è automaticamente iniettiva. Basta mostrare che f è suriettiva. Da questo discenderà che anche $\tilde{f}$ lo è, per cui $\tilde{f}$ sarà un isomorfismo. (Equivalentemente, basta usare il I teorema di isomorfismo. La cosa fondamentale è sempre dimostrare che f è suriettiva.) Rivediamo prima la dimostrazione per $n = 2$. Per dimostrare che f è suriettiva dobbiamo far vedere che dati $a + I_1 \in A/I_1$ e $b \in A/I_2$ qualsiasi, esiste $z \in A$ tale che $f(z) = (a + I_1, b + I_2)$. Per ipotesi esistono $x \in I_1$ e $y \in I_2$ tali che $x + y = 1$. Allora

$$a - b = (a - b) \cdot 1 = ax - bx + ay - by,$$
$$a + bx - ax = b + ay - by,$$
$$z := a + (b - a)x = b + (a - b)y.$$

Allora $z - a \in (x) \subset I_1$ e $z - b \in (y) \subset I_2$. Dunque $f(z) = (z + I_1, z + I_2) = (a + I_1, b + I_2)$, come desiderato. Per il caso generale procediamo per induzione su n. Siano $x_i + I_i \in A/I_i$ per $i = 1, \ldots, n$. Vogliamo trovare $w \in A$ tale che $f(w) = (x_1 + I_1, \ldots, x_n + I_n)$. Per l'ipotesi induttiva l'applicazione

$$A \to A/I_1 \oplus \cdots \oplus A/I_{n-1}, \quad x \mapsto (\pi_1(x), \ldots, \pi_{n-1}(x))$$

è suriettiva. Dunque esiste $z \in A$ tale che $z + I_i = x_i + I_i$ per $i < n$. Poniamo $J := I_1 \cdots I_{n-1}$. Per il lemma precedente $J + I_n = A$. Dunque dal caso $n = 2$ discende che anche l'applicazione $A \to A/J \oplus A/I_n$, $x \mapsto (x + J, x + I_n)$ è suriettiva. Quindi esiste $w \in A$ tale che $w + J = z + J$ e $w + I_n = x_n + I_n$. Componendo con l'isomorfismo $A/J \cong A/I_1 \oplus \cdots \oplus A/I_{n-1}$ concludiamo che f è suriettiva. □

21. In realtà abbiamo dimostrato un enunciato più preciso: non solo vale l'isomorfismo del teorema cinese, ma l'isomorfismo è dato dalla mappa f. Se ci accontentiamo dell'esistenza *un* isomorfismo, allora l'induzione è più semplice:

$$A/I_1 \oplus \cdots \oplus A/I_n = (A/I_1 \oplus \cdots \oplus A/I_{n-1}) \oplus A/I_n \cong$$
$$\cong A/J \oplus A/I_n \cong A/J \cdot I_n = A/I_1 \cdots I_n.$$

Tuttavia sapere come è fatto l'isomorfismo è utile, per esempio per ottenere il corollario seguente.

Corollario 22. *Siano $a_1, \ldots, a_n \in \mathbb{Z}$ e supponiamo che per $i \neq j$ i numeri a_i e a_j siano coprimi. Allora dati $m_1, \ldots, m_n \in \mathbb{Z}$ esiste un numero $x \in \mathbb{Z}$ tale che $x \equiv m_i \mod a_i$ per ogni i. Inoltre x è unico a meno di multipli di $a_1 \cdots a_n$.*

Esercizio 23. *Siano M_i moduli ed $N_i \subset M_i$ sottomoduli per $i = 1, 2$. Dimostrare che*

$$\frac{M_1 \oplus M_2}{N_1 \oplus N_2} \cong \frac{M_1}{N_1} \oplus \frac{M_2}{N_2}.$$

Suggerimento: considerare l'applicazione naturale $M_1 \oplus M_2 \to (M_1/N_1) \oplus (M_2/N_2)$ e applicare il I Teorema di isomorfismo.

Sia A un dominio a ideali principali e sia M un A-modulo. Se $\mathfrak{m}$ è un ideale massimale non nullo di A e $\mathfrak{m} = (p)$, poniamo

$$T_p M = T_{\mathfrak{m}} M := \{x \in M : \exists r > 0 : p^r x = 0\} =$$
$$= \{x \in M : \exists r > 0 : \mathfrak{m}^r \subset \mathrm{Ann}(x)\}.$$

Gli elementi di $T_{\mathfrak{m}} M$ sono detti di $\mathfrak{m}$-torsione o semplicemente di p-torsione. (Ovviamente se x è di p-torsione, allora è di q-torsione per ogni q associato a p. Per questo motivo è più preciso parlare di ideali.)

Lemma 24. *$T(M) = \oplus_{\mathfrak{m}} T_{\mathfrak{m}} M$, dove $\mathfrak{m}$ varia su tutti gli ideali primi non nulli di A.*

Dimostrazione. Cominciamo con una osservazione: se $a, b \in A$ sono coprimi e $a, b \in \mathrm{Ann}(x)$, allora $x = 0$. Infatti $va + wb = 1$ per opportuni $v, w \in A$ e dunque $1 \cdot x = 0$. Dunque se $x \in T_p M$ e $x \in \sum_{i=1}^n T_{p_i} M$ dove $(p) \neq (p_i)$ per ogni i, allora esiste un intero $R > 0$ tale che $p^R, (p_1 \cdots p_n)^R \in \mathrm{Ann}(x)$. Dunque $x = 0$. Questo dimostra che i sottomoduli $T_p(M)$ sono indipendenti,

cioè la somma è diretta. Se poi $x \in T(M)$ e $a \in \mathrm{Ann}(x)$, $a \neq 0$, fattorizziamo $a = p_1^{n_1} \cdots p_s^{n_s}$. Procediamo per induzione su s. Se $s = 1$, $x \in T_{p_1}M$. Per $s > 1$, esistono $v, w \in A$ tali che $1 = vp_1^{n_1} + wp_2^{n_2} \cdots p_s^{n_s}$, dunque $x = vp_1^{n_1}x + wp_2^{n_2} \cdots p_s^{n_s}x$. Il secondo termine è in $T_{p_1}M$. Invece l'annullatore del primo termine contiene $p_2^{n_2} \cdots p_s^{n_s}$. Per ipotesi induttiva starà nella somma $T_{p_2}M \oplus \cdots \oplus T_{p_s}M$. □

Esercizio 25. *Siano M ed M' A-moduli e sia $\varphi : M \to M'$ una mappa A-lineare. Sia $\lambda \in M$. Sia $f_\lambda : M \to M$ la moltiplicazione per λ: $f_\lambda(x) := \lambda x$. Sia f'_λ la moltiplicazione per λ su M'. Allora $\varphi(\ker f_\lambda) \subset \ker f'_\lambda$ e $\varphi(\mathrm{im}\, f_\lambda) \subset \mathrm{im}\, f'_\lambda$. In particolare se φ è un isomorfismo, allora $\ker f_\lambda \cong \ker f'_\lambda$ e $\mathrm{im}\, f_\lambda \cong \mathrm{im}\, f'_\lambda$.*

Esercizio 26. *Siano date due liste di numeri interi $0 < n_1 \leq \cdots \leq n_s$ e $0 < m_1 \leq \cdots \leq m_t$. Se per ogni $k \in \mathbb{Z}, k \geq 0$ il numero di indici i tali che $n_i > k$ coincide con il numero di indici j tali che $m_j > k$, allora $s = t$ e $n_i = m_i$ per ogni i.*

Svolgimento. Se prendiamo $k = 0$ otteniamo subito che $s = t$. Possiamo procedere per induzione su s. Se $s = 1$ prendiamo $k = n_1 + 1$. Allora esiste un solo indice i tale che $m_i < k$. Dunque $i = 1$ e $m_1 \leq n_1$. Per simmetria abbiamo la diseguaglianza opposta e abbiamo finito. Per fare il passo induttivo consideriamo di nuovo $k = n_1 + 1$. Sia $j := \max\{i : 1 \leq i \leq s, n_i = n_1\}$. Allora per $i \leq j$, $m_i \leq n_1$. Di nuovo possiamo sfruttare la simmetria e otteniamo $n_i = m_i$ per $1 \leq i \leq j$. Ora buttiamo via i primi j termini di entrambe le liste. Le liste rimanenti soddisfano ancora l'ipotesi e per induzione concludiamo. □

Lemma 27. *Sia A un dominio a ideali principali e sia p un elemento irriducibile di A. Siano $s, t \geq 0$ e siano dati numeri interi $0 < n_1 \leq \cdots \leq n_s$ e $0 < m_1 \leq \cdots \leq m_t$. Se c'è un isomorfismo di A-moduli*

$$\bigoplus_{i=1}^{s} A/(p^{n_i}) \cong \bigoplus_{i=1}^{t} A/(p^{m_i}), \tag{1.1}$$

allora $s = t$ e $n_i = m_i$ per ogni $i = 1, \ldots, s$.

Dimostrazione. Se $s = 0$ si intende che non ci sono addendi, dunque il modulo a sinistra è nullo. Se fosse $t > 0$, $m_1 > 0$, dunque $A/(p^{m_1}) \neq \{0\}$. Quindi necessariamente anche $t = 0$. Eliminato questo caso banale possiamo supporre $s, t > 0$. Chiamiamo M il modulo a sinistra e M' quello a destra. Sia $\varphi : M \to M'$ l'isomorfismo. Fissiamo $k \in \mathbb{Z}$, $k \geq 0$. Indichiamo con

p^kM l'immagine della mappa da M in M data dalla moltiplicazione per p^k. Quindi p^kM è un sottomodulo di M. Nella notazione dell'esercizio 25 $p^kM := \operatorname{im} f_{p^k}$, quindi $\varphi(p^kM) = p^kM'$ e c'è un isomorfismo

$$p^kM \cong p^kM'$$

per ogni k. L'ideale $\mathfrak{m} := (p)$ è massimale in A e $F := A/\mathfrak{m}$ è un campo. Per il Lemma 4 il quoziente $p^kM/\mathfrak{m} \cdot p^kM$ è uno spazio vettoriale su F. Dall'esercizio 5 otteniamo che

$$\dim \frac{p^kM}{\mathfrak{m} \cdot p^kM} = \dim \frac{p^kM'}{\mathfrak{m} \cdot p^kM'}. \tag{1.2}$$

D'altro canto siamo in grado di calcolare queste dimensioni. Osserviamo prima di tutto che se $n \in \mathbb{Z}, 0 < n \leq k$ $p^kA/(p^n) = \{0\}$. Se invece $k < n$

$$\frac{p^kA/(p^n)}{\mathfrak{m} \cdot p^kA/(p^n)} = \frac{p^kA/(p^n)}{p^{k+1}A/(p^n)} \cong \frac{p^kA}{p^{k+1}A} \cong A/(p) = F. \tag{1.3}$$

Il primo isomorfismo è dato dal III Teorema di isomorfismo. Il secondo si ottiene applicando il I Teorema di isomorfismo al morfismo $A \to p^kA$, $x \mapsto p^k \cdot x$. Fin qui abbiamo fatto ragionamenti completamente generali, indipendenti dalle ipotesi. Ora sfruttiamo la descrizione di M in (1.1). Grazie a (1.3) otteniamo

$$p^kM = \bigoplus_{i:n_i>k} p^kA/(p^{n_i}),$$
$$\frac{p^kM}{\mathfrak{m} \cdot p^kM} = \bigoplus_{i:n_i>k} \frac{p^kA/(p^{n_i})}{\mathfrak{m} \cdot p^kA/(p^{n_i})} = \bigoplus_{i:n_i>k} F.$$

Dunque la dimensione dello spazio vettoriale $p^kM/p^{k+1}M$ è data dal numero di indici i tali che $n_i > k$. Per (1.2) questo numero coincide con quello degli indici i tali che $m_i > k$. L'esercizio 26 permette di concludere. □

Teorema 28 (di struttura dei moduli finitamente generati su un dominio a ideali principali)**.** *Sia A un anello a ideali principali e sia M un A-modulo finitamente generato.*

a) Esistono elementi non nulli e non invertibili $a_1, \ldots, a_m \in A$ ed un intero $r \geq 0$ tali che

$$M \cong A^r \oplus A/(a_1) \oplus \cdots \oplus A/(a_m) \quad e \quad a_1 | \cdots | a_m. \tag{1.4}$$

b) $T(M) \cong A/(a_1) \oplus \cdots \oplus A/(a_m)$.

c) $\operatorname{Ann} T(M) = (a_m)$.

d) r *è univocamente determinato da* M *e viene chiamato* rango *di* M.

e) Esistono degli elementi irriducibili $p_1, \ldots, p_s \in A$ *e numeri interi* $t_i > 0$ *e* $l_{ik} > 0$ *per* $1 \leq i \leq s, 1 \leq k \leq t_i$ *tali che* $l_{i1} \leq \cdots \leq l_{it_i}$ *e*

$$T(M) \cong \bigoplus_{i=1}^{s} \bigoplus_{k=1}^{t_i} A/(p_i^{l_{ik}}). \tag{1.5}$$

f) $\operatorname{Ann} T(M) = (p_1^{l_{1t_1}} \cdots p_s^{l_{st_s}})$.

g) I p_i *sono univocamente determinati a meno dell'ordine e di associati.*

h) I numeri t_i *e* l_{ik} *sono univocamente determinati. Gli elementi* $p_i^{l_{ik}}$ *sono detti* divisori elementari *di* M.

i) Gli elementi a_i *sono unici a meno di associati. Sono chiamati* fattori invarianti *di* M.

Dimostrazione. M è finitamente generato. Siano $z_1, \ldots, z_n$ dei generatori. Allora esiste un morfismo $f : F := A^n \to M$ che manda e_i in z_i. Dunque f è suriettivo. Sia $K = \ker f$. Allora $M \cong F/K$. Applichiamo il Teorema 16 e l'esercizio 23. Allora

$$M \cong F/K = A/(a_1) \oplus \cdots \oplus A/(a_m) \oplus A^{n-m}.$$

Potrebbe succedere che alcuni degli a_i siano invertibili. Sarebbero per forza all'inizio. In quel caso li possiamo semplicemente buttar via perché $A/(1) = \{0\}$. Abbiamo dimostrato (a). Per dimostrare (b) basta verificare che

$$T(A^r \oplus A/(a_1) \oplus \cdots \oplus A/(a_m)) = A/(a_1) \oplus \cdots \oplus A/(a_m). \tag{1.6}$$

Si vede facilmente che se $x \in A^r \oplus A/(a_1) \oplus \cdots \oplus A/(a_m)$ è di torsione, allora la componente di x lungo A^r è nulla. Infatti se questa componente è $(y_1, \ldots, y_r)$ e che $\lambda x = 0$ per un certo $\lambda \neq 0$, otteniamo $\lambda y_i = 0$ e dunque $y_i = 0$ per ogni i. Dunque

$$T(A^r \oplus A/(a_1) \oplus \cdots \oplus A/(a_m)) \subsetneq A/(a_1) \oplus \cdots \oplus A/(a_m).$$

Viceversa la condizione di divisibilità assicura che a_m annulla $A/(a_1) \oplus \cdots \oplus A/(a_m)$ a da questo segue l'inclusione opposta. Quindi la (1.6) e il punto (b)

sono dimostrati. Segue che $a_m \in \operatorname{Ann} T(M)$. D'altronde se $x \in \operatorname{Ann} T(M)$, allora x annulla $1 + (a_m)$ in $A/(a_m)$, dunque $a_m | x$, dunque $x \in (a_m)$. Segue (c).

Da (1.4) e (1.6) segue che $M/T(M) \cong A^r$. Quindi r dipende solo da M e la (d) è dimostrata.

Sia $a_m = p_1^{n_{1m}} \cdots p_s^{n_{sm}}$ la fattorizzazione di a_m, dove $p_1 \ldots, p_s$ sono irriducibili e $n_{im} > 0$ per $i = 1, \ldots, s$. Fissiamo ora $j < m$. Siccome $a_j | a_m$, a meno di sostituire a_j con un elemento associato, avremo $a_j = p_1^{n_{1j}} \cdots p_s^{n_{sj}}$ per opportuni numeri interi n_{ij} con $0 \leq n_{ij} \leq n_{im}$. Alcuni degli n_{ij} potrebbero essere nulli. Inoltre n_{ij} è crescente in j perché $a_j | a_{j+1}$. Dal Teorema cinese del resto segue che

$$A/(a_j) = A/(p_1^{n_{1j}}) \oplus \cdots \oplus A/(p_s^{n_{sj}}).$$

In questa scomposizione i termini in cui $n_{ij} = 0$ sono banali e possiamo eliminarli. Mettiamo insieme tutte queste scomposizioni e raggruppiamo i termini con lo stesso primo. In questo modo otteniamo la scomposizione (1.5).

Vediamo invece come ricostruire la scomposizione (1.4) quando è nota la (1.5). Poniamo $m := \max_i t_i$, ossia m è il massimo numero di addendi relativi ad uno stesso primo. Facciamo una tabellina in cui mettiamo nella prima colonna gli elementi $p_1, \ldots, p_s$. A destra mettiamo una matrice $s \times m$ fatta così: nella riga a destra di p_i mettiamo le potenze $p_i^{l_{i1}}, \ldots, p_i^{l_{it_i}}$ aggiungendo a sinistra una serie di 1 in modo che la riga sia lunga m quadratini. Se $t_i = m$ per un certo i fissato, la tabellina è fatta così:

p_1	1	$\cdots$	1	$p_1^{l_{11}}$	$p_1^{l_{12}}$	$\cdots$	$p_1^{l_{1t_1}}$
$\vdots$	$\vdots$		$\vdots$	$\cdots$		$\vdots$	$\vdots$
p_i	$p_i^{l_{i1}}$	$p_i^{l_{i2}}$	$p_i^{l_{i3}}$	$\cdots$	$\cdots$		$p_i^{l_{it_i}}$
$\vdots$	$\vdots$		$\vdots$	$\cdots$		$\vdots$	$\vdots$
p_s	1	$\cdots$	$p_s^{l_{s1}}$	$\cdots$	$\cdots$		$p_s^{l_{st_s}}$
	a_1	a_2	$\cdots$	$\cdots$		$\cdots$	a_m

A questo punto a_i è il prodotto dei termini nella colonna sopra di lui. Per il teorema cinese del resto

$$\bigoplus_{j=1}^{m} A/(a_j) \cong \bigoplus_{i=1}^{s} \bigoplus_{k=1}^{t_i} A/(p_i^{l_{ik}}).$$

Per esempio consideriamo il caso $A = \mathbb{Z}$, $s = 3$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ e

$$M = \mathbb{Z}/(2^3) \oplus \mathbb{Z}/(3^2) \oplus \mathbb{Z}/(3^2) \oplus \mathbb{Z}/(3^2) \oplus \mathbb{Z}/(5^2) \oplus \mathbb{Z}/(5^3).$$

Allora $t_1 = 1, t_2 = 3, t_3 = 2$, $l_{11} = 3$, $l_{21} = l_{22} = l_{23} = 2$, $l_{31} = 2$, $l_{32} = 3$. Dunque $m = 3$ e la tabellina è

2	1	1	2^3
3	3^2	3^2	3^2
5	1	5^2	5^3
	a_1	a_2	a_3

Quindi $a_1 = 9$, $a_2 = 25 \cdot 9$, $a_3 = 8 \cdot 9 \cdot 125$. La (f) discende a questo punto dalla (c). Dalla (f) discende immediatamente la (g).

Supponiamo ora di avere due scomposizioni come (1.5). Per il punto (g) possiamo supporre che gli elementi irriducibili siano gli stessi, dunque avremo

$$\bigoplus_{i=1}^{s} \bigoplus_{k=1}^{t_i} A/(p_i^{l_{ik}}) \cong \bigoplus_{i=1}^{s} \bigoplus_{k=1}^{t'_i} A/(p_i^{l'_{ik}}).$$

Per ogni i la p_i-torsione del modulo a sinistra sarà isomorfa alla p_i-torsione del modulo a destra, ossia

$$\bigoplus_{k=1}^{t_i} A/(p_i^{l_{ik}}) \cong \bigoplus_{k=1}^{t'_i} A/(p_i^{l'_{ik}}).$$

A questo punto applichiamo il Lemma (27) e otteniamo che i divisori elementari sono univocamente determinati a meno di associati. Per il procedimento descritto sopra, l'unicità dei divisori elementari dà l'unicità dei fattori-invarianti. □

Corollario 29. *Se M è un modulo finitamente generato su un dominio a ideali principali, allora M è somma diretta di un numero finito di A-moduli ciclici.*

Dimostrazione. Infatti $A/I = A \cdot (1 + I)$ è sempre un modulo ciclico. □

Corollario 30. *Se M è un modulo finitamente generato su un dominio a ideali principali, allora $M/T(M)$ è libero e la sua dimensione è il rango di M.*

Esercizio 31. *Se M è un modulo finitamente generato su un anello a ideali principali, allora il rango di M è il più grande intero r tale che esistono elementi $v_1, \dots, v_r \in M$ linearmente indipendenti.*

Svolgimento. Infatti siano $v_1 \dots, v_s \in M$ linearmente indipendenti. Scrivo $M \cong F \oplus T$, $v_i = x_i + t_i$, $x_i \in F$, $t_i \in T$. Sostengo che $x_1, \dots, x_s$ sono indipendenti. Infatti se $\sum_i \lambda_i x_i = 0$, scelto $z \neq 0$ tale che $zt_i = 0$ per ogni i, abbiamo

$$\sum_i (z\lambda_i) v_i = z \sum_i \lambda_i x_i = 0.$$

Dunque per l'indipendenza si $\{v_i\}$ concludo che $z\lambda_i = 0$ e quindi che $\lambda_i = 0$ per ogni i. Questo dimostra che $\{x_i\}$ sono indipendenti. Quindi $s = \dim\langle x_i \rangle \leq r = \dim F$. □

Esercizio 32. *Sia A un dominio a ideali principali e siano $a, b \in A$.*
(1) Sia $f_b : A/(a) \to A/(a)$ la moltiplicazione per b: $f_b(x + (a)) := bx + (a)$. Allora

$$\ker f_b = \frac{(a/\operatorname{MCD}(a,b))}{(a)} \cong A/(\operatorname{MCD}(a,b)).$$

(2) Supponiamo poi che $M := \oplus_{i,j} A/(p_i^{l_{ij}})$ con $\{p_1, \dots, p_s\}$ elementi irriducibili a due a due non associati. Fissiamo k ed $n \geq \max_j l_{kj}$. Allora

$$\ker(f_{p_k^n} : M \to M) = \oplus_j A/(p_k^{l_{kj}}).$$

Svolgimento. (1) Sia $c := \operatorname{MCD}(a,b)$ e sia $a = a_1 c$, $b = b_1 c$. Allora $f_n(x + (a)) = 0$ se e solo se $bx \in (a)$ se e solo se $b_1 x \in (a_1)$. Questo l'uguaglianza. L'isomorfismo segue applicando il I Teorema di isomorfismo alla mappa $A \to A/(a_1), x \mapsto a_1 x + (a)$.
(2) La mappa $f_{p_k^n}$ rispetta la scomposizione, cioè manda ciascun addendo in sé stesso. Dunque il nucleo è la somma diretta dei nuclei della moltiplicazione su ciascun addendo. Basta quindi applicare il punto (1). □

Corollario 33. *Se G è un gruppo abeliano finitamente generato, allora G è prodotto di un numero finito gruppi ciclici. Inoltre G è di torsione se e solo se è finito. In tal caso $|G|$ è uguale al prodotto dei fattori invarianti e anche al prodotto dei divisori elementari.*

Quanti gruppi abeliani di ordine m esistono? Scriviamo $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Dato $n \in \mathbb{N}$ una *partizione* di n è un successione $n_1, \dots n_k \in \mathbb{N}$ tale che $n_1 + \cdots + n_k = n$. L'ordine dei numeri n_i non conta. Possiamo metterli in ordine crescente. Il simbolo $p(n)$ indica il numero di partizioni di n. Per questo numero non è nota una formula chiusa. Un gruppo abeliano di ordine m sarà della forma

$$G = \prod_{i=1}^{s} \prod_{j=}^{t_i} \mathbb{Z}/p_i^{l_{ij}}$$

con $l_{ij} \in \mathbb{N}$ tali che $\sum_{j=1}^{t_i} l_{ij} = \alpha_i$ (qui usiamo la notazione moltiplicativa). Dunque $\{l_{i1}, \dots, l_{it_i}\}$ è una partizione di α_i. Quindi il numero di gruppi abeliani di ordine m è $p(\alpha_1) \cdots p(\alpha_s)$. Per esempio esistono 14 gruppi abeliani di ordine $2^5 \cdot 3^2 \cdot 7$.

Forma canonica razionale Sia ora F un campo e sia $A = F[x]$. Sia V uno spazio vettoriale su F. Se fissiamo un operatore lineare $T \in \operatorname{End} V$, possiamo dare a V la struttura di A-modulo nel modo seguente. Se $p(x) = \sum_{i=0}^{d} a_i x^i \in A$, allora

$$p(t) := \sum_{i=0}^{d} a_i T^i \in A.$$

L'applicazione $p(x) \mapsto p(T)$ è un morfismo di anelli (e anche una applicazione F-lineare) da A in $\operatorname{End} V$. Siccome $\operatorname{End}(V, +) \subset \operatorname{End} V$, otteniamo su V una struttura di A-modulo. Detto in altri termini la struttura di A-modulo è data dalla regola

$$p(x) \cdot v := p(T)(v).$$

Indichiamo con V_T l'insieme V provvisto di questa struttura di A-modulo.

Esercizio 34. *Un sottospazio vettoriale W di V è un sottomodulo di V_T se e solo se W è T-invariante, cioè $T(W) \subset W$.*

Lemma 35. *Se V e V' sono F-spazi vettoriali e $T \in \operatorname{End} V$, $T' \in \operatorname{End} V'$, allora un isomorfismo A-lineare $f : V_T \to V'_{T'}$ non è altro che un isomorfismo di spazi vettoriali che soddisfa $fT = T'f$.*

Dimostrazione. Se f è un isomorfismo di A-moduli, e $v \in V$, allora $f(T(v)) = f(x \cdot v) = x \cdot f(v) = T'(f(v))$. Viceversa, se vale $fT = T'f$, allora per ogni polinomio $p(x) \in A$, vale $fp(T) = p(T')f$, dunque $f(p(x) \cdot v) = f(p(T)(v)) = p(T')(f(v)) = p(x) \cdot f(v)$. □

Corollario 36. *Due operatori $T, T' \in \operatorname{End} V$ sono simili se e solo se i moduli V_T e $V_{T'}$ sono isomorfi.*

Se $\dim_F V = n < \infty$, allora V_T è un A-modulo finitamente generato e di torsione. Dunque c'è un isomorfismo A-lineare

$$\varphi : V_T \xrightarrow{\cong} \bigoplus_{i=1}^{m} A/(f_i), \tag{1.7}$$

per certi polinomi non costanti $f_1 | \cdots | f_m$ che sono i fattori invarianti del modulo V_T. Possiamo scegliere i fattori invarianti in modo che siano tutti monici. Con questa proprietà aggiuntiva i fattori invarianti sono davvero unici, non solo a meno di associati. I quozienti $A/(f_i)$ sono F-spazi vettoriali oltre che A-moduli, perché F è incluso in A, φ è anche F-lineare e tramite φ l'endomorfismo T va a finire nella moltiplicazione per x.

Inoltre $\operatorname{Ann} V_T = \{p(x) \in A : p(T) = 0\} = (f_m)$. Osserviamo che $\operatorname{Ann} V_T$ dipende solo da T. Il suo generatore monico si chiama *polinomio minimo* di T e si indica con q_T. Dunque Dunque

$$q_T = f_m. \tag{1.8}$$

Sia V_i il sottospazio di V tale che $\varphi(V_i) = A/(f_i)$. V_i è T-invariante, perché $A/(f_i)$ è un sottomodulo..

Ora procederemo studiando la restrizione di T a ciascuno dei sottospazi V_i. Per comodità consideriamo una situazione un po' più generale.

Endomorfismi ciclici Supponiamo che $V_T \cong A/(f)$, dove $f \in A$ è un qualsiasi polinomio non costante, non necessariamente un fattore invariante. In questo caso diciamo che T è un *endomorfismo ciclico*.

Sia $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ un polinomio monico di grado $d > 0$. La matrice

$$B_f := \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & -a_2 \\ & & \ddots & 0 & -a_{d-2} \\ & & & 1 & -a_{d-1} \end{pmatrix}$$

è detta la *matrice compagna* di f.

Lemma 37. *Se f è monico, il polinomio caratteristico di B_f è $p_{B_f} = (-1)^{\deg f} f$.*

Dimostrazione. Per definizione

$$p_{B_f}(x) = \det(B_f - xI_d) = \begin{vmatrix} -x & & & & -a_0 \\ 1 & -x & & & -a_1 \\ & 1 & \ddots & & -a_2 \\ & & \ddots & -x & -a_{d-2} \\ & & & 1 & -a_{d-1} - x \end{vmatrix}.$$

Procediamo per induzione su d. Se $d = 1$, $p_{B_f}(x) = \det(-x - a_0) = -f$. Supponiamo che valga $p_{B_g} = (-1)^{\deg g+1}$ per polinomi di grado $< d$. Sviluppando lungo la prima riga

$$p_{B_f}(x) = -x \begin{vmatrix} -x & & & -a_1 \\ 1 & \ddots & & -a_2 \\ & \ddots & -x & -a_{d-2} \\ & & 1 & -a_{d-1} - x \end{vmatrix} + (-1)^d a_0 \begin{vmatrix} 1 & -x & & \\ & 1 & \ddots & \\ & & \ddots & -x \\ & & & 1 \end{vmatrix}.$$

La prima matrice è uguale a $B_g - xI_{d-1}$ dove $g(x) = a_1 + a_2x + \cdots + a_{d-1}x^{d-2} + x^{d-1}$. Dunque per ipotesi induttiva il suo determinante è $(-1)^{d-1}g(x)$. Quindi $p_{B_f}(x) = -x(-1)^{d-1}g(x) + (-1)^d a_0 = (-1)^d(xg(x) + a_0)$. Siccome $xg(x) + a_0 = f(x)$, segue la tesi. □

Teorema 38. *Sia $T \in \operatorname{End} V$ ciclico con $V_T \cong A/(f)$, con f monico. Allora esiste una base di V rispetto alla quale T è rappresentato dalla matrice B_f. Inoltre $q_T = f$ e $p_T = (-1)^{\deg f} f$.*

Dimostrazione. Sia $d = \deg f$. I polinomi $1, x, x^2, \ldots, x^{d-1}$ formano una base dello spazio vettoriale $A/(f)$. Infatti una relazione di dipendenza lineare fra di essi significherebbe che un polinomio di grado $< d$ appartiene a (f), il che è assurdo. Dunque $\dim V = \dim A/(f) = d$. L'operatore su $A/(f)$ dato dalla moltiplicazione per x è rappresentato dalla matrice B_f. Siccome l'isomorfismo $\varphi : V_T \to A/(f)$ scambia T e la moltiplicazione per x, nella base $\{\varphi^{-1}(1), \ldots, \varphi^{-1}(x^{d-1})\}$ l'operatore T è rappresentato da B_f. Siccome $V_T \cong A/(f)$, f è l'unico fattore invariante, dunque $q_T = f$. L'ultima affermazione discende dal Lemma 37. □

Forma canonica razionale.

39. Ora che abbiamo sistemato gli endomorfismi ciclici possiamo passare a quelli qualsiasi. Infatti il Teorema 28 e il fatto che V_T è di torsione se

$\dim V < \infty$ garantiscono che abbiamo le scomposizioni

$$V_T \cong \bigoplus_{i=1}^{m} A/(f_i) \cong \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} A/(p_i^{l_{ij}}), \tag{1.9}$$

dove $f_1 | \cdots | f_m$ sono i fattori invarianti e $\{p_i^{l_{ij}}\}$ sono i divisori elementari.

Consideriamo prima la scomposizione con i fattori elementari. Sia V_i la controimmagine di $A/(f_i)$. Allora $V = V_1 \oplus \cdots \oplus V_m$ e i V_i sono sottospazi T-invarianti, sui quali T agisce ciclicamente. Per ogni i c'è una base di V_i rispetto alla quale la matrice di $T_{|V_i}$ è B_{f_i}. Incollando queste basi otteniamo una base di V rispetto alla quale la matrice di T sarà

$$\begin{pmatrix} B_{f_1} & & \\ & \ddots & \\ & & B_{f_m} \end{pmatrix}. \tag{1.10}$$

La rappresentazione matriciale (1.10) viene chiamata *forma canonica razionale* dell'operatore T.

Otteniamo il seguente raffrozamento del teorema di Hamilton-Cayley.

Teorema 40 (di Hamilton-Cayley)**.** *$p_T(T) = 0$ ossia $q_T \,|\, p_T$. Inoltre ogni fattore irriducibile di p_T compare in q_T.*

Dimostrazione. Dalla forma canonica razionale otteniamo subito che $p_T = \pm f_1 \cdots f_m$. Siccome $f_m = q_T$ concludiamo che $q_T | p_T$, dunque $p_T(T) = 0$. Ricordando le proprietà di divisibilità dei fattori invarianti: $f_1 | \cdots | f_m$ otteniamo subito che ogni divisore irriducibile di p_T divide $f_m = q_T$. □

41. Due operatori $T, T' \in \operatorname{End} V$ hanno la stessa la forma canonica razionale se e solo se i moduli V_T e $V_{T'}$ hanno gli stessi fattori invarianti, ossia (per il Teorema 28) se e solo se i moduli V_T e $V_{T'}$ sono isomorfi ossia (per il Corollario 36) se e solo se T e T' sono simili. Riassumendo: due matrici sono simili se e solo se hanno la stessa forma canonica razionale.

Lemma 42. *Un endomorfismo $T \in \operatorname{End} V$ è ciclico se e solo se $p_T = \pm q_T$. In tal caso $V_T \cong A/(q_T)$.*

Dimostrazione. Supponiamo T ciclico: $V_t \cong A/(f)$. Allora $\operatorname{Ann} V_T = (f)$ dunque $q_T = f$. Per il lemma precedente $p_T = \pm f$. Viceversa dato $T \in \operatorname{End} V$ spezziamo V_T secondo i fattori elementari, cioè $V_T \cong \oplus_{i=1}^{m} A/(f_i)$. Allora $q_T = f_m$, mentre $p_T = \pm f_1 \cdots f_m$. Se $p_T = \pm q_T$, allora $m = 1$, quindi T è ciclico. □

Possiamo applicare il procedimento usato in 39 alla seconda scomposizione in (1.9), invece che alla prima: possiamo cioè usare i divisori elementari anziché i fattori invarianti. Anche in questo caso la matrice di T in una opportuna base è una matrice a blocchi. I blocchi saranno (in generale) più piccoli di quelli di prima, perché i sottospazi T-invarianti W_{ij} corrispondenti agli addendi $A/(p_i^{l_{ij}})$ danno una scomposizione più raffinata di quelli V_i corrispondenti agli addendi $A/(f_i)$. I blocchi lungo la diagonale saranno le matrici compagne $B_{p_i^{l_{ij}}}$, $1 \le i \le s$, $1 \le j \le t_i$, i blocchi fuori della diagonale saranno tutti nulli. Anche questa rappresentazione viene chiamata forma canonica razionale di T.

Osserviamo che

$$q_T = \prod_{i=1}^{s} p_i^{\max_j l_{ij}}, \qquad p_T = \prod_{i=1}^{s} \prod_{j=1}^{t_i} p_i^{l_{ij}}. \tag{1.11}$$

Di nuovo ritroviamo il teorema di Hamilton-Cayley.

Forma canonica di Jordan L'ultima scomposizione descritta diventa interessante se il polinomio minimo q_T si spezza in fattori lineari su F, per esempio se F è algebricamente chiuso. In tal caso $p_i(x) = x - \lambda_i$, e lo spettro di T (che coincide con l'insieme delle radici di p_T o equivalentemente di q_T) è $\{\lambda_1, \dots, \lambda_s\}$.

Riprendiamo la scomposizione

$$V = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} W_{ij},$$

dove W_{ij} è l'addendo corrispondente a $A/(p_i^{l_{ij}})$. La somma $V_i := \oplus_i W_{ij}$ è la p_i-torsione di V_T. Poniamo

$$l_i := \max_j l_{ij} \tag{1.12}$$

Allora $\operatorname{Ann} V_i = (p_i^{l_i})$. Se $k \neq i$ Il nucleo della moltiplicazione per $p_i^{l_i}$ su V_k, è nullo. Questo segue dall'Esercizio 32 o anche considerando dal fatto che $\operatorname{Ann} V_i \cap \operatorname{Ann} V_k = \{0\}$. Quindi

$$V_i = \oplus_j W_{ij} = \ker p_i(T)^{l_i} = \ker (T - \lambda_i)^{l_i}. \tag{1.13}$$

Per procedere con l'analisi, ci concentriamo di nuovo su un singolo addendo: sia $T \in \operatorname{End} W$ e supponiamo che ci sia un solo divisore elementare: $(x-\lambda)^k$.

Ossia $W \cong A/(x-\lambda)^k$. Scegliamo come base $\{1, x-\lambda, (x-\lambda)^2, \ldots, (x-\lambda)^{k-1}\}$. Ricordiamo che T coincide con la moltiplicazione per x. Dunque $T(x-\lambda)^i = x(x-\lambda)^i = (x-\lambda)^{i+1} + \lambda(x-\lambda)^i$. Dunque la matrice di T rispetto a questa base è

$$\begin{pmatrix} \lambda & & & & 0 \\ 1 & \lambda & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ 0 & & & 1 & \lambda \end{pmatrix}$$

Questo è un *blocco di Jordan* di ordine k e lo indichiamo con $J_k(\lambda)$. Se applichiamo questo procedimento ad ogni sottospazio W_{ij} troviamo una base di V rispetto alla quale la rappresentazione matriciale di T è una matrice a blocchi che ha sulla diagonale i blocchi di Jordan $J_{l^{ij}}(\lambda_i)$ per $i = 1, \ldots, s$ e $j = 1, \ldots, t_i$ e zero fuori della diagonale:

$$\begin{pmatrix} J_{l_{11}}(\lambda_1) & & & & & & \\ & \ddots & & & & 0 & \\ & & J_{l_{1t_1}}(\lambda_1) & & & & \\ & & & \ddots & & & \\ & & & & J_{l_{s1}}(\lambda_s) & & \\ & 0 & & & & \ddots & \\ & & & & & & J_{l_{st_s}}(\lambda_s) \end{pmatrix}. \tag{1.14}$$

Questa si chiama *forma canonica di Jordan* dell'operatore T. Anche per questa vale che due operatori $T, T \in \operatorname{End} V$ sono simili se e solo se hanno la stessa forma canonica di Jordan, a meno di riordinamento dei blocchi.

Osserviamo da vicino un blocco di Jordan $J_k(\lambda)$ e supponiamo che rappresenti T rispetto ad una base $e_1, \ldots, e_k$. Si vede subito che e_k è l'unico autovettore di T all'interno del blocco. Anzi $\ker T = \langle e_k \rangle$. Segue che la molteplicità geometrica di λ come autovalore di T è uguale al numero di blocchi con $\lambda = \lambda_i$. In altre parole la

$$\text{molteplicità geometrica di } \lambda_i = t_i.$$

Invece la molteplicità algebrica di λ_i è uguale al somma di tutte le dimensioni dei blocchi di Jordan relativi a λ_i:

$$\text{molteplicità algebrica di } \lambda_i = \sum_{j=1}^{t_i} l_{ij}.$$

Proposizione 43. *Sia V uno spazio vettoriale di dimensione finita sul campo F. Supponiamo che p_T si spezzi in fattori lineari su F. Allora T è diagonalizzabile se e solo se il polinomio minimo q_T non ha radici multiple.*

Dimostrazione. Un blocco di Jordan è diagonalizzabile se e solo se ha dimensione 1. Dunque T è diagonalizzabile se e solo $l_{ij} \equiv 1$, ossia - vedi (1.12) - se e solo se $l_i = 1$ per ogni i. Per concludere basta ricordare la (1.11). $\square$

Capitolo 2

Azioni di gruppi e teoremi di Sylow

Se X è un insieme non vuoto, S_X indica l'insieme di tutte le applicazioni biunivoche di X in sé. Questo insieme è un gruppo rispetto alla composizione.

Un'azione del gruppo G sull'insieme non vuoto X è un morfismo $\alpha : G \to S_X$.

In modo equivalente possiamo definire una azione di G su X come una applicazione $A : G \times X \to X$ che soddisfa le due proprietà

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

Il legame fra le due definizioni è nella formula $A(g, x) = \alpha(g)(x)$. Nella pratica si ragiona spesso con l'applicazione A che viene indicata semplicemente con il puntino: $g \cdot x = A(g, x)$.

Se $x \in X$ l'insieme $G_x := \{g \in G : g \cdot x = x\}$ è un sottogruppo di G e viene chiamato *stabilizzatore* o *sottogruppo di isotropia* di x. ("Isotropia" = stesso posto, perché lascia x nello stesso posto.)

Le G-orbita passante per $x \in X$ è l'insieme

$$G \cdot x := \{y \in X : \exists g \in G : y = g \cdot x\}.$$

Un sottoinsieme $Y \subset X$ è detto G-invariante se per ogni $y \in Y$ e per ogni $g \in G$ si ha $g \cdot y \in Y$.

Le orbite di G su X formano una partizione di X. La relazione corrispondente è

$$x \sim y \iff y \in G \cdot x.$$

Le classi di equivalenza di $\sim$ sono le orbite. Il quoziente $X/\sim$ è indicato con il simbolo X/G. In questo modo l'azione di un gruppo su un insieme X dà luogo ad una relazione di equivalenza su X. Molte delle più importanti relazioni di equivalenza provengono da azioni di gruppo. Per esempio se V è uno spazio vettoriale su k, la relazione di equivalenza su $V - \{0\}$ che dà luogo al proiettivo, cioè $v \sim v'$ se e solo se $v = \lambda \cdot v$ per $]la \in k^*$ è la relazione corrispondente all'azione di k^* (moltiplicativo) su $V - \{0\}$ per moltiplicazione.

Ogni gruppo agisce su sé stesso in vari modi:

1. per moltiplicazione a sinistra:

$$G \times G \longrightarrow G, \qquad (g, x) \mapsto gx.$$

2. Per coniugio:

$$G \times G \longrightarrow G, \qquad (g, x) \mapsto \mathrm{inn}_g(x) := gxg^{-1}.$$

   Questa azione è speciale perché $\mathrm{inn}_g \in \mathrm{Aut}\, G$. Dunque l'azione rispetta la struttura di gruppo.

3. Per moltiplicazione a destra:

$$G \times G \longrightarrow G, \qquad (g, x) \mapsto xg^{-1}.$$

Consideriamo l'azione di G su G per coniugio. Se $x \in G$, lo stabilizzatore di x per questa azione viene chiamato *centralizzante* di x in G e viene indicato col simbolo $C(x)$ o $Z_G(x)$. Dunque

$$C(x) = Z_G(x) := \{g \in G : gx = xg\}.$$

Evidentemente $x \in Z(G)$ se e solo se $C(x) = G$. Inoltre x sta sempre nel centro del gruppo $C(x)$. Questo è il motivo del nome.

A partire da una azione è possibile costruire tante altre azioni. Il modo più stupido è restringere l'azione a un sottogruppo. Se $A : G \times X \to X$ è l'applicazione che definisce l'azione e H è un sottogruppo di G, allora $A_{|H \times X}$ è l'azione ristretta al sottogruppo H.

Per esempio, sia $H \subset G$ un sottogruppo. Consideriamo l'azione per moltiplicazione destra e restringiamola ad H. Ci ritroviamo con una azione di H su G:

$$H \times G \longrightarrow G, \qquad (h, x) \mapsto xh^{-1}.$$

Le orbite di questa azione sono esattamente i laterali sinistri di H: $H \cdot x = xH$. Dunque l'insieme dei laterali sinistri, che viene indicato con G/H è proprio il quoziente di G per H tramite questa azione e dunque la notazione G/H è compatibile con quella introdotta sopra.

Osserviamo che G agisce su G/H mediante la regola

$$G \times G/H \longrightarrow G/H, \qquad (g, aH) \mapsto aH.$$

Infatti questa mappa è ben definita e soddisfa le proprietà di un'azione.

Esercizio 44. *Sia X un insieme su cui agiscono due gruppi G ed H. Supponiamo che le due azioni* commutino *ossia per ogni $g \in G$, $h \in H$ ed $x \in X$*

$$g \cdot (h \cdot x) = h \cdot (g \cdot x).$$

Verificare che questa condizione equivale al fatto che tutte le trasformazioni $x \mapsto g \cdot x$ sono H-equivarianti. Dimostrare che allora c'è una unica azione di G sul quoziente X/H tale che la proiezione canonica $X \to X/H$ sia G-equivariante.

Se $Y \subset X$ è G-invariante, allora $A(G \times Y) \subset Y$ e possiamo restringere dominio e codominio di A in modo da ottenere una mappa $G \times Y \to Y$ che è una azione, l'azione ristretta ad Y.

Per esempio se $\mathcal{O} = G \cdot x$ è un'orbita, posso restringere l'azione ad $\mathcal{O}$.

Se G agisce su X un *punto fisso* è un punto $x \in X$ tale che $g \cdot x = x$ per ogni $g \in G$. In altre parole $G_x = G$.

L'azione di G su X è detta *fedele* se il morfismo $G \to S_X$ è iniettivo. L'azione è detta *libera* se $g \cdot x = x$ implica $g = e$. Equivalentemente per ogni $x \in X$ lo stabilizzatore è $G_x = \{e\}$. Se l'azione è libera l'applicazione $G \to G \cdot x$, $\mapsto g \cdot x$ è biunivoca per ogni x. Infine l'azione è transitiva se c'è una unica orbita, ossia dati $x, y \in X$ esiste sempre un elemento $g \in G$ tale che $y = g \cdot x$. Segue che per ogni $x \in X$ si ha $X = G \cdot x$.

Esempi: se A è uno spazio affine e G è il gruppo delle affinità, allora l'azione è transitiva. Se $H \subset G$ è il gruppo delle traslazioni, allora l'azione di H su A è libera e transitiva.

Esercizi 1.

1. *Se $x \in X$, $g \in G$ e $H := \langle g \rangle$, allora $g \cdot x = x$ se e solo se $x \in X^H$.*
2. *Sia V uno spazio vettoriale. Allora* $\mathrm{Gl}(V)$ *agisce su V. Quali sono le orbite?*

3. *Sia $(V, \langle , \rangle)$ uno spazio vettoriale euclideo, cioè uno spazio vettoriale su $\mathbb{R}$ con un prodotto scalare definito positivo. Sia $G = \mathrm{O}(V, \langle\,\rangle)$ il gruppo ortogonale di V. Quali sono le orbite di G?*

Un insieme X munito di un'azione del gruppo G si chiama G-insieme. I G-insieme (per G fissato) formano una categoria. I morfismi fra due G-insiemi X e Y sono le *applicazioni G-equivarianti* ossia le mappe $f : X \to Y$ tali che

$$f(g \cdot x) = g \cdot f(x).$$

In questa categoria un isomorfismo è chiamato G-isomorfismo. In altre parole un G-isomorfismo è una applicazione biunivoca G-equivariante. L'inversa è automaticamente equivariante.

Lemma 45. *Se G agisce su X e $x \in X$, allora l'applicazione $G/G_x \to G \cdot x$ definita dalla formula $aG_x \mapsto a \cdot x$ è ben definita, biunivoca ed equivariante*

Dimostrazione. Sia $\tilde{f} : G \to G \cdot x$ l'applicazione $\tilde{f}(a) := a \cdot x$. Questa applicazione è suriettiva per definizione. Inoltre si verifica subito che $\tilde{f}(a) = \tilde{f}(b) \Leftrightarrow$ □

Il seguente Corollario è una generalizzazione del teorema di Lagrange secondo il quale l'ordine di un sottogruppo divide l'ordine del gruppo.

Corollario 46. *Se il gruppo finito G agisce sull'insieme X e $x \in X$ allora*

$$|G \cdot x| = \frac{|G|}{|G_x|}.$$

Un'altra costruzione è la seguente. Se G agisce su X e $E \subset X$, poniamo $g \cdot E = g(E) = \{g \cdot x | x \in E\}$. Allora

$$G \times P(X) \longrightarrow P(X), \qquad (g, E) \mapsto g \cdot E$$

è una azione di G su $P(X)$, l'insieme delle parti di X. Un caso particolarmente importante è il seguente: consideriamo $X = G$ e facciamo agire G su sé stesso per conoiugio. Siccome è una azione per automorfismi, se $H \subset G$ è un sottogruppo, allora anche $g(H) = \mathrm{inn}_g(H) = gHg^{-1}$ è un sottogruppo, coniugato di H. Dunque otteniamo una azione di G sull'insieme $\mathscr{S}(G)$ dei suoi sottogruppi

$$G \times \mathscr{S}(G) \longrightarrow \mathscr{S}(G), \qquad (g, H) \mapsto gHg^{-1}.$$

L'orbita di H attraverso questa azione è l'insieme di tutti i sottogruppi di G coniugati ad H. Lo stabilizzatore di H per questa azione è il sottogruppo

$$N_G(H) := \{g \in G : gHg^{-1} = H\}. \tag{2.1}$$

Questo sottogruppo è chiamato *normalizzante* del sottogruppo H in G. Per definizione abbiamo $H \lhd N_G(H)$. Se H' è un sottogruppo di G che contiene H e $H \lhd H'$, allora $H' \subset N_G(H)$. Infine H è normale in G se e solo se $N_G(H) = G$.

Esercizio 47. *Sia G un gruppo, $x \in G$ e $H = \langle x \rangle$. Dimostrare che $Z_G(x) \subset N_G(H)$. È vero anche il viceversa? (Suggerimento: pensare a S_3.)*

Supponiamo ora che G ed X siano finiti. Sia $x_1, \ldots, x_n$ un insieme di rappresentanti per le orbite, nel senso che $X/G = \{G \cdot x_i\}$ e $G \cdot x_i \neq G \cdot x_j$ per $i \neq j$. Allora la cosiddetta *Equazione delle Orbite*

$$|X| = \sum_{i=1}^{n} [G : G_{x_i}] = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}.. \tag{2.2}$$

Infatti $X = \sqcup_i G \cdot x_i$, dunque $|X| = \sum_i |G \cdot x_i|$. Per concludere basta applicare il Corollario 46.

Se G agisce su X una *funzione invariante* è una funzione $f : X \to Y$ tale che $f(g \cdot x) = f(x)$ per ogni $g \in G$ e $x \in X$.

Esercizio 48. *Sia k un campo. Consideriamo l'insieme $M(m,n)$ delle matrici $m \times n$ a coefficienti in k e il gruppo $G := \mathrm{Gl}(m,k) \times \mathrm{Gl}(n,k)$ che agisce su $M(m,n)$ in base alla regola*

$$(a,b) \cdot C := aCb^{-1}.$$

Dimostrare che il rango è una funzione invariante $M(m,n) \to \mathbb{N}$. Se due matrici $C, D \in M(m,n)$ hanno lo stesso rango, sono nella stessa orbita?

Esercizio 49. *Sia p un numero primo e sia $k := F_p$ il campo finito con p elementi. Indichiamo con $M(n)$ l'insieme delle matrici quadrate di ordine n a coefficienti in k. Facciamo agire $\mathrm{Gl}(n,k)$ agisce per coniugio su $M(n)$. Per $n \geq 4$ calcolare la cardinalità del quoziente $M(n)/\mathrm{Gl}(n,k)$. (Suggerimento: sfruttare la forma canonica razionale.)*

Teorema 50 (di Cayley)**.** *Ogni gruppo è un gruppo di trasformazioni, cioè agisce effettivamente su qualche spazio. Ogni gruppo finito è un sottogruppo di S_n per $n = |G|$.*

Dimostrazione. Sia G un gruppo. Allora G agisce su sé stesso per traslazioni sinistre: $G \times G \to G$, $(g, x) \mapsto gx$. Questa azione è effettiva: infatti se $g \cdot x = x$ per ogni $x \in G$, allora scegliendo $x = e$ otteniamo $g = ge = g \cdot e = e$. Dunque l'unico elemento che agisce su G lasciando fissi tutti gli elementi è l'elemento neutro e. In altre parole il morfismo $\alpha : G \to S_G$ è iniettivo. □

Sottogruppi di gruppi abeliani finiti

Proposizione 51. *Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n. Allora*

1. $o(g^s) = \frac{n}{(n,s)}$.
2. $\langle g^s \rangle = \langle g^{(n,s)} \rangle$.
3. *G contiene esattamente $\varphi(n)$ generatori.*
4. *Se $H \subset G$ è un sottogruppo di ordine d, allora $d|n$, H è ciclico e $H = \langle g^{n/d} \rangle$.*
5. *Se $d|n$, G contiene un unico sottogruppo di ordine d.*
6. *Formula di Gauss:*

$$n = \sum_{d|n} \varphi(d). \tag{2.3}$$

Dimostrazione. (1) Scriviamo $c := (n, s)$, $n = n_1 c$, $s = s_1 c$. Allora $(g^s)^k = g^{sk} = 1$ sse $n = cn_1 | sk = cs_1 k$ sse $n_1 | s_1 k$ sse $n_1 | k$. Dunque $o(g^s) = n_1 = n/c$.
(2) Ovviamente $\langle g^s \rangle \subset \langle g^{(n,s)} \rangle$ visto che $(n, s)|s$. D'altronde esistono numeri interi a, b tali che $(n, s) = an + bs$. Dunque $g^{(n,s)} = (g^n)^a \cdot (g^s)^b = (g^s)^b$. Quindi $\langle g^{(n,s)} \rangle \subset \langle g^s \rangle$.
(3) Sia $0 \leq s < n$. Allora $o(g^s) = n$ se e solo se $(n, s) = 1$. Quindi i generatori di G sono esattamente gli elementi g^s con $0 \leq s < n$ e s primo con n. Per definizione il numero è $\varphi(n)$.
(4) Se $d = 1$ è ovvio. Altrimenti $m := \min\{i > 0 : g^i \in H\} > 0$. Sia $s \in \mathbb{Z}$ tale che $g^s \in H$. Allora $s = qm + r$ con $0 \leq r < m$. Ma allora $r = 0$, ossia $g^s \in H$ se e solo se $m|s$. Dunque $H = \langle g^m \rangle$ e $m|n$. Dunque $d = o(g^m) = n/m$ divide n. Inoltre H è generato da $g^m = g^{n/d}$.
(5) L'unicità segue immediatamente da (4). Per l'esistenza basta osservare che $o(g^{n/d}) = d$.
(6) Raggruppiamo gli elementi di G in base all'ordine: $G_d := \{x \in G : o(x) = d\}$. Allora $G = \sqcup_{d|n} G_d$. Poniamo $H_d := \langle g^{n/d} \rangle$. Allora $G_d \subset H_d$, anzi G_d è formato esattamente dai generatori di H_d. Dunque $|G_d| = \varphi(d)$. □

Proposizione 52. *Se G è un gruppo abeliano finito di ordine n e $m|n$, allora esiste un sottogruppo $H \subset G$ con ordine $o(H) = m$.*

Dimostrazione. Cominciamo dal caso in cui G è un p-gruppo: $o(G) = p^a$. Allora per il Teorema 28

$$G \cong \oplus_{i=1}^{s} \mathbb{Z}/(p^{n_i}), \qquad a = \sum_{i=1}^{s} n_i.$$

Se $m|n = p^a$, allora $m = p^b$. Scelgo m_i tali che $0 \leq m_i \leq n_i$ e $\sum_{i=1}^{s} m_i = b$. Per la Proposizione 51 esiste un sottogruppo $H_i \subset \mathbb{Z}/(p^{n_i})$ di ordine m_i. Dunque $H = \oplus_{i=1}^{s} H_1$ è un sottogruppo di ordine m. Per il caso generale, sempre per il Teorema 28,

$$G = G_1 \times \cdots \times G_s$$

dove G_i è un p_i-gruppo e p_1, lds, p_s sono primi distinti. Dunque se $o(G_i) = p_i^{a_i}$ e $m|n = p_1^{a_1} \cdots p_s^{a_s}$, allora $m = p_1^{b_1} \cdots p_s^{b_s}$. Dunque scelgo sottogruppi $H_i \subset G_i$ di ordine $p_i^{b_i}$ e $H = H_1 \times \cdots \times H_s$ è il sottogruppo cercato. □

L'ipotesi che il gruppo sia abeliano è essenziale, altrimenti il teorema è falso come si vede dal seguente esercizio.

Esercizio 53. *Dimostrare che A_4 non ha sottogruppi di ordine 6.*

Nel caso non abeliano ci si deve accontentare di meno, cioè della esistenza dei sottogruppi di Sylow, che ora definiamo.

Definizione 54. *Se p è un numero primo, un p-*gruppo *è un gruppo di ordine una potenza di p. Se G è un gruppo finito, un p-*sottogruppo *di G è un sottogruppo che è un p-gruppo. Se $o(G) = n = p^a m$ e $p \nmid m$, un p-*sottogruppo di Sylow *o semplicemente un p-*Sylow *di G è un sottogruppo $H \subset G$ di ordine p^a.*

Teorema 55 (di Sylow)**.** *Sia G un gruppo finito e p un numero primo.*

1. *(Sylow I) Esiste un p-Sylow di G.*
2. *Se $H \subset G$ è un p-sottogruppo, allora H è contenuto in un p-Sylow.*
3. *(Sylow II) Tutti i p-Sylow di G sono coniugati.*
4. *Se P è un p-Sylow di G e n_p è il numero dei p-Sylow di G, allora*

$$n_p = [G : N_G(P)].$$

5. (Sylow III) $n_p \equiv 1 \mod p$ *e* $n_p | o(G)$.

56. Dalla prima formula in (3) discende che $p \nmid n_p$. Dunque se $o(G) = p^a m$ e $(p, m) = 1$, segue che $n_p | m$.

57. Per dimostrare i Teoremi di Sylow useremo un tipo particolare di azione che ora descriviamo. Fissiamo due sottogruppi di G, che chiameremo U ed H. Consideriamo l'azione del gruppo $U \times H$ sull'insieme G definita dalla formula seguente:

$$(u, h) \cdot x := uxh^{-1}.$$

L'orbita di x per questa azione si indica con UxH e si chiama *laterale doppio*. Ci interessa capire come è fatto lo stabilizzatore di un punto $x \in G$ rispetto a questa azione:

$$(u, h) \cdot x = x \iff h = x^{-1}ux.$$

Dunque

$$(U \times H)_x = \{(u, x^{-1}ux) : u \in U, x^{-1}ux \in H\}$$

Ma $x^{-1}ux \in H$ sse $u \in xHx^{-1}$. Quindi

$$(U \times H)_x = \{(u, x^{-1}ux) : u \in U \cap xHx^{-1}\} \cong U \cap xHx^{-1} \cong (x^{-1}Ux) \cap H.$$

Pertanto grazie alla Formula delle Orbite (2.2) scelti rappresentanti $\{x_1, \ldots, x_k\}$ otteniamo

$$|G| = \sum_{i=1}^{k} \frac{|U| \cdot |H|}{|(x_i^{-1}Ux_i) \cap H|}. \tag{2.4}$$

Il secondo ingrediente della dimostrazione del Teorema di Sylow è lo studio di un gruppo particolare molto importante: sia F il campo con p elementi e sia $\mathrm{Gl}(n, p) := \mathrm{Gl}(n, F)$ il gruppo lineare generale a coefficienti in F.

Sia poi P il sottogruppo di $\mathrm{Gl}(n, p)$ formato dalle matrici triangolari superiori che hanno 1 sulla diagonale, ossia le matrici della forma

$$\begin{pmatrix} 1 & * & \ldots & * \\ & \ddots & & \vdots \\ & & \ddots & * \\ 0 & & & 1 \end{pmatrix} \tag{2.5}$$

Lemma 58. *Gli ordini dei gruppi* $\mathrm{Gl}(n,p)$ *e* P *sono dati dalle formule seguenti:*

$$|\,\mathrm{Gl}(n,p)| = \prod_{i=0}^{n-1}(p^n - p^i) = p^{\frac{n(n-1)}{2}} \cdot \prod_{j=1}^{n}(p^j - 1),$$

$$|P| = p^{\frac{n(n-1)}{2}}.$$

In particolare P *è un* p*-Sylow di* $\mathrm{Gl}(n,p)$*.*

Dimostrazione. Per contare gli elementi di P basta osservare che ci sono $n(n-1)/2$ elementi della matrice che possiamo scegliere come ci pare (gli elementi indicati con $*$ nella (2.5)) e ciascuno può assumere come valore i p diversi elementi del campo F. Dunque ci sono $p^{n(n-1)/2}$ scelte possibili per individuare un elemento di P. Questo dimostra la seconda formula. Per contare gli elementi di $\mathrm{Gl}(n,p)$ procediamo così. Sia $A \in \mathrm{Gl}(n,p)$. Indichiamo con v_j la j-esima colonna di A. Costruiamo A una colonna alla volta. La prima colonna v_1 è un qualsiasi vettore non nullo. Siccome $|F^n| = p^n$ abbiamo $p^n - 1$ scelte per v_1. Per la seconda colonna dobbiamo scegliere un qualsiasi vettore v_2 linearmente indipendente da v_1, dunque un vettore di F^n che non appartiene alla retta $\langle v_1\rangle$ generata da v_1. Siccome una retta di F^n è isomorfa ad F, essa contiene p elementi. Quindi $|F^n - \langle v_1\rangle| = p^n - p$ e dunque per v_2 abbiamo $p^n - p$ scelte. Procedendo in questo modo, dopo k passi avremo fissato i vettori linearmente indipendenti $v_1, \ldots, v_k$ e dovremo scegliere v_{k+1} in $F^n - \langle v_1, \ldots, v_k\rangle$. Siccome $\langle v_1, \ldots, v_k\rangle \cong F^k$, l'insieme $F^n - \langle v_1, \ldots, v_k\rangle$ contiene $p^n - p^k$ elementi. Questo dimostra la prima formula per $|\,\mathrm{Gl}(n,p)|$. Quindi osserviamo che $p^n - p^i = p^i(p^{n-i} - 1)$. Per dimostrare la seconda formula usiamo che

$$\prod_{i=0}^{n-1}(p^{n-i} - 1) = \prod_{j=1}^{n}(p^j - 1).$$

Per concludere basta osservare che p non divide $(p-1)\cdots(p^n-1)$, perché $(p-1)\cdots(p^n-1) \equiv 1 \mod p$. □

Fissiamo $n \in \mathbb{N}$ e un primo p. Sia $e_1, \ldots, e_n$ la base canonica di F^n. Definiamo

$$A : S_n \longrightarrow \mathrm{Gl}(n,p),$$

nel modo seguente: se $\sigma \in S_n$, $A(\sigma)$ è la matrice che ha come colonna j-esima $e_{\sigma(j)}$. Se indichiamo con $a_{ij}(\sigma)$ gli elementi della matrice $A(\sigma)$ allora

$$a_{ij}(\sigma) = \delta_{i\sigma(j)}.$$

Se τ è un'altra permutazione allora

$$\sum_k a_{ik}(\sigma)a_{kj}(\tau) = \sum_k \delta_{i\sigma(k)}\delta_{k\tau(j)} = \sum_k \delta_{\sigma^{-1}(i)k}\delta_{k\tau(j)} = \delta_{i\sigma(\tau(j))} = a_{ij}(\sigma\tau).$$

Questo dimostra che $A : S_n \to \mathrm{Gl}(n,p)$ è un morfismo di gruppi evidentemente iniettivo. Abbiamo dimostrato il seguente

Lemma 59. *Per ogni $n \in \mathbb{N}$ e per ogni primo p esiste un morfismo iniettivo $S_n \longrightarrow \mathrm{Gl}(N,p)$.*

Corollario 60. *Se G è un gruppo finito e p è un numero primo, esiste un morfismo iniettivo $G \to \mathrm{Gl}(n,p)$ dove $n = |G|$.*

Dimostrazione. Basta applicare il Teorema di Cayley e il Lemma precedente. □

Lemma 61. *Se G è un gruppo finito, $H \subset G$ è un sottogruppo e P è un p-Sylow di G, allora esiste $x \in G$ tale che $xPx^{-1} \cap H$ sia un p-Sylow di H.*

Dimostrazione. Supponiamo che $|G| = p^a m$ con $(p,m) = 1$ e che $|H| = p^b n$ con $b \leq a$ e $n \leq m$. Ovviamente $|P| = p^a$. Applichiamo la formula (2.4) con $U = P$: scelti i rappresentanti $x_1, \ldots, x_k$ si ha

$$p^a m = |G| = \sum_{i=1}^{k} \frac{|P| \cdot |H|}{|(x_i^{-1}Px_i) \cap H|} = \sum_{i=1}^{k} \frac{p^a \cdot p^b n}{|(x_i^{-1}Px_i) \cap H|}$$

$$m = \sum_{i=1}^{k} \frac{p^b n}{|(x_i^{-1}Px_i) \cap H|}.$$

Ricordiamo che tutti i termini della somma a destra sono interi, perché sono uguali all'indice di $(P \times H)_{x_i}$ in $P \times H$. Almeno uno di essi non è divisibile per p, visto che la loro somma è uguale ad m e $p \nmid m$. Supponiamo che sia il primo a non essere divisibile per p:

$$p \nmid \frac{p^b n}{|(x_1^{-1}Px_1) \cap H|}.$$

Poniamo $Q := x_1^{-1}Px_1 \cap H$. Allora Q è un sottogruppo di H. Inoltre l'automorfismo inn_{x_1} manda Q sul sottogruppo $P \cap x_1 H x_1^{-1}$, che è contenuto in P. Per il teorema di Lagrange $o(Q) = o(P \cap x_1 P x_1^{-1}) = p^c$ con $c \leq a$. Ma Q è sottogruppo di H, dunque $c \leq b$. Ma allora

$$\frac{p^b n}{|P \cap x_1 H x_1^{-1}|} = \frac{p^b n}{p^c} = p^{b-c} n.$$

Siccome questo numero non è diviso da p, concludiamo che $c = b$, dunque $o(Q) = p^b$ e quindi Q è un p-Sylow di H. L'elemento x cercato è dunque $x = x_1$. □

Dimostrazione del Teorema di Sylow. Per il Corollario 60 G è isomorfo a un sottogruppo di $\mathrm{Gl}(n, p)$ dove $n = |G|$. Il Lemma 61 garantisce che se un gruppo ha un p-Sylow, ogni suo sottogruppo ha un p-Sylow. Per il Lemma 58 il gruppo $\mathrm{Gl}(n, p)$ ha un p-Sylow. Dunque anche G, che è isomorfo a un sottogruppo di $\mathrm{Gl}(n, p)$ ha un p-Sylow. Questo dimostra Sylow I.
Ora fissiamo un p-Sylow $P \subset G$ e un p-sottogruppo $H \subset G$. Applichiamo di nuovo il Lemma 61: esiste $x \in G$ tale che $x^{-1}Px \cap H$ è un p-Sylow di H. Ma un p-Sylow di un p-sottogruppo coincide necessariamente col sottogruppo. Quindi $x^{-1}Px \cap H = H$ ossia $H \subset x^{-1}Px$. Dunque H è contenuto in xPx^{-1} che è un p-Sylow di G. Questo dimostra (2).
Se P' è un altro p-Sylow di G, allora P' in particolare è un p-sottogruppo, quindi possiamo applicare di nuovo il ragionamento appena sfruttato e otteniamo $x \in G$ tale che $P' \subset xPx^{-1}$. Ma allora $P' = xPx^{-1}$. Quindi i p-Sylow sono tutti coniugati. Questo dimostra Sylow II.
Indichiamo con X l'insieme di tutti i p-Sylow di G. Abbiamo appena imostrato che X è una unica orbita per l'azione di coniugio di G sui suoi sottogruppi. Ossia, se $P \in X$, $X = \{gPg^{-1} | g \in G\} = G \cdot P$. Ma $G \cdot P \cong G/G_P$ come per ogni azione. In questo caso lo stabilizzatore di P è il normalizzante $G_P = N_G(P)$, vedi (2.1). Dunque

$$n_p := |X| = [G : N_G(P)].$$

Questo dimostra (4).
Supponiamo $n = o(G) = p^a m$ con $(p, m) = 1$. Siccome $N_G(P) \supset P$, avremo $|N_G(P)| = p^a m'$ con $m'|m$. Dunque $n_p = m/m'$ divide m e e quindi n. Rimane da dimostrare che $n_p \equiv 1 \mod p$. Per questo poniamo $N := N_G(P)$. Incominciamo dimostrando il seguente fatto:

$$x \in G \text{ e } x^{-1}Px \subset N \Longrightarrow x \in N. \tag{2.6}$$

Infatti se $x^{-1}Px \subset N$, allora P e $x^{-1}Px \subset N$ sono due p-Sylow di N. Per Sylow II questi sono coniugati in n, dunque esiste $y \in N$ tale che $x^{-1}Px = y^{-1}Py$. Ma $y \in N \Rightarrow y^{-1}Py = P$, dunque $x^{-1}Px = P$, e questo significa che $x \in N$.

Ora consideriamo l'azione di $P \times N$ su G. Siano di nuovo $x_1, \ldots, x_k$ i rappresentanti. Possiamo supporre che $e \in Px_1N$. Quindi l'orbita per x_1

coincide con l'orbita per e: ossia $Px_1N = PeN = N$. Dunque $x_1 \in N$, $x_1^{-1}Px_1 = P$, $x_1^{-1}Px_1) \cap N = P$ e

$$|(x_1^{-1}Px_1) \cap N| = |P|. \tag{2.7}$$

Sia invece $i > 1$. Siccome le orbite sono disgiunte, $x_i \notin N$. Per (2.6) questo comporta che $x_i^{-1}Px_1$ non è contenuto in N, quindi $(x_i^{-1}Px_i) \cap N \subsetneq x_i^{-1}Px_i$, dunque

$$|(x_i^{-1}Px_i) \cap N| < |P|.$$

Segue che il numero $|(x_i^{-1}Px_i) \cap N|$ divide p^a, ma è strettamente più piccolo. Abbiamo dimostrato che

$$p \Big| \frac{|P|}{|(x_i^{-1}Px_i) \cap N|} \qquad \text{per ogni } i > 1. \tag{2.8}$$

A questo punto applichiamo la (2.4) all'azione di $P \times N$ e otteniamo

$$|G| = \sum_{i=1}^{k} \frac{|P| \cdot |N|}{|(x_i^{-1}Px_i) \cap N|},$$

$$n_p = \frac{|G|}{|N|} = 1 + \sum_{i=2}^{k} \frac{|P|}{(|x_i^{-1}Px_i) \cap N|}.$$

Per la (2.8) la sommatoria a secondo membro è divisibile per p, cioè $n_p \equiv 1 \mod p$. □

Esercizio 62. *Siano G e G' gruppi e sia $f : G \to G'$ un morfismo. Se $N' \lhd G'$ allora $f^{-1}(N') \lhd G$. Se f è suriettivo e $N \lhd G$, allora $f(N) \lhd G'$. In questo caso l'applicazione $N' \mapsto f^{-1}(N')$ dall'insieme dei sottogruppi normali di G che contengono* $\ker f$ *all'insieme dei sottogruppi normali di G' è biunivoca, con inversa l'applicazione $N \mapsto f(N)$. Se G e G' sono finiti, allora $|f^{-1}(N')| = |N'| \cdot |\ker f|$.*

Lemma 63. *Sia G un p-gruppo di ordine p^a. Allora per ogni $i = 0, \dots, a$ esiste un sottogruppo G_i normale in G di ordine p^i.*

Dimostrazione. Procediamo per induzione su a. Se $a = 0$ siamo a posto. Se $|G| = p^a$ con $a > 0$, allora il centro di G non è banale e contiene un elemento x di ordine p, per la Proposizione 52. Sia $H := \langle x \rangle$. Poniamo $\bar{G} := G/H$. Allora $o(\bar{G}) = p^{a-1}$. Dunque per ipotesi induttiva esistono sottogruppi $\bar{G}_i \lhd \bar{G}$ per $i = 0, \dots, a-1$ tali che $|\bar{G}_i| = p^i$. Indicata con $\pi : G \to \bar{G}$ la proiezione canonica, poniamo $G_i := \pi^{-1}(\bar{G}_{i-1})$ per $i = 1, \dots, a$. Per l'esercizio precendete $G_i \lhd G$ e $|G_i| = |\bar{G}_{i-1}| \cdot |H| = p^i$. □

Corollario 64. *Sia G un gruppo finito. Se $p^a | o(G)$ esiste un sottogruppo di G di ordine p^a.*

Corollario 65 (Teorema di Cauchy)**.** *Se $p | o(G)$, allora G contiene un elemento di ordine p.*

Equazione delle classi. Sia G un gruppo finito e siano $x_1, \dots, x_k$ degli elementi tali che $R := Z(G) \sqcup \{x_1, \dots, x_k\}$ sia un sistema di rappresentanti delle classi di coniugio, ossia ogni elemento di G è coniugato ad un unico elemento di R. Allora

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : Z_G(x_i)]. \tag{2.9}$$

Proposizione 66. *Se G è un p-gruppo, allora $p \,|\, o(Z(G))$. Dunque G ha centro non banale.*

Dimostrazione. Partiamo da (2.9). Siccome $x_i \notin Z(G)$, $Z_G(x_i) \neq G$, dunque $[G : Z_G(x_i)] \neq 1$. D'altronde questo indice è una potenza di p. Dunque p divide $[G : Z_G(x_i)]$ per ogni i. Segue che p divide $|Z(G)|$. □

Esercizio 67. *(a) Sia G un gruppo. Se $G/Z(G)$ è ciclico, allora G è abeliano. (b) Sia G un gruppo e sia $A \subset G$ un sottogruppo abeliano. Supponiamo che la proiezione $\pi : G \to G/Z(G)$ sia tale che $\pi(A) = G/Z(G)$. dimostrare che allora G è abeliano. (c) Dimostrare che (a) è un caso particolare di (b).*

Corollario 68. *Se p è primo e $o(G) = p^2$, allora G è abeliano.*

Dimostrazione. Per la proposizione precedente $Z(G) \neq \{1\}$. Vogliamo dimostrare che $Z(G) = G$. Se così non fosse $Z(G)$ avrebbe ordine p e lo stesso varrebbe per $G/Z(G)$, che pertanto sarebbe un gruppo ciclico. Ma allora G sarebbe abeliano per l'esercizio precedente. □

Definizione 69. *Sia G un gruppo e sia H un sottogruppo. Diciamo che H è un* sottogruppo caratteristico *se per ogni $\alpha \in \operatorname{Aut} G$ vale $\alpha(H) = H$.*

Esercizio 70. *Dimostrare che il centro $Z(G)$ e il sottogruppo dei commutatori $[G, G]$ sono sottogruppi caratteristici.*

Esercizio 71. *Sia V_4 il Vierergruppe o gruppo di Klein, ossia $V_4 = (\mathbb{Z}/2)^2$. Allora tutti i sottogruppi sono normali perché V_4 è abeliano. Tuttavia $\operatorname{Aut} V_4 = \mathrm{Gl}(2, \mathbb{Z}/2)$ che è transitivo sulle rette del piano $(\mathbb{Z}/2)^2$, quindi esiste un automorfismo che manda $\langle (1,0) \rangle$ in $\langle (0,1) \rangle$. Dunque $H = \langle (1,0) \rangle$ è normale ma non caratteristico.*

Lemma 72. *Un p-Sylow di G è normale se e solo è unico (cioè $n_p = 1$) se e solo se è caratteristico.*

Prodotti Il *prodotto diretto* o semplicemente il prodotto di due gruppi G e H è l'insieme $G \times H$ provvisto dell'operazione

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2).$$

Per studiare un gruppo G è molto utile rappresentarlo come prodotto di due suoi sottogruppi. Questi sono più piccoli, quindi è più facile studiarli. Quindi vogliamo capire quando un gruppo G è isomorfo al prodotto di due suoi sottogruppi N e H.

Se A, B sono sottoinsiemi di G, il simbolo AB indica l'insieme di tutti gli elementi $x \in G$ che si possono scrivere nella forma $x = ab$ con $a \in A$ e $b \in B$. Si indica invece con $[A, B]$ il sottogruppo generato dai commutatori $[a, b] = aba^{-1}b^{-1}$ con $a \in A$ e $b \in$b.

Lemma 73. *1. Se N ed H sono sottogruppi di G, allora l'applicazione $f : N \times H \to G$, $f(n, h) = nh$ ha immagine NH.*

2. Se $nh \in NH$, allora $f^{-1}(nh) = \{(nx^{-1}, xh) : x \in N \cap H\}$. Dunque $f^{-1}(nh)$ è in corrispondenza biunivoca con $N \cap H$.

3. Se N ed H sono finiti, allora $|NH| = |N| \cdot |H|/|N \cap H|$.

4. Se $N \lhd G$ e $H \leq G$, allora $NH \leq G$.

5. Se $N, H \lhd G$, allora $NH \lhd G$ e $[N, H] \subset N \cap H$.

6. Se $N, H \lhd G$ e $N \cap H = \{e\}$, allora $NH \cong N \times H$.

Dimostrazione. 1. Ovvio.

2. $f(n_1, h_1) = nh$ sse $n_1 h_1 = nh$ sse $n^{-1} n_1 = h h_1^{-1}$. Basta porre $x := n^{-1} n_1 \in N \cap H$.

3. Discende dalla 2:

$$N \times H = \bigsqcup_{z \in NH} f^{-1}(z)$$
$$|N| \cdot |H| = |N \times H| = \sum_{z \in NH} |f^{-1}(z)| = |NH| \cdot |N \cap H|.$$

4. $n_1 h_1 \cdot n_2 h_2 = n_1 (h_1 n_2 h_1^{-1}) \cdot h_1 h_2$.

5. $x(nh)x^{-1} = (xnx^{-1}) \cdot (xhx^{-1})$.

6. $[n, h] = (nhn^{-1}) \cdot h^{-1} = n \cdot (hn^{-1}h^{-1})$.

□

Se $S_1, \ldots, S_k$ sono sottoinsiemi di un gruppo G indichiamo con $S_1 \cdots S_k$ l'insieme formato da tutti i prodotti $x_1 \cdots x_k$ con $x_i \in S_i$.

Lemma 74. *Siano $N_1, \ldots, N_k$ sottogruppi normali di G. Allora $N_1 \cdots N_k$ è un sottogruppo normale di G. Supponiamo che per ogni i si abbia*

$$N_i \cap (N_1 \cdots \hat{N}_i \cdots N_k) = \{e\}$$

dove $\hat{}$ indica il termine che viene saltato. Allora l'applicazione

$$f : N_1 \times \cdots \times N_k \to N_1 \cdots N_k, \quad f(n_1, \ldots, n_k) := n_1 \cdots n_k$$

è un isomorfismo.

Dimostrazione. Cominciamo dal caso $k = 2$. Il sottoinsieme N_1N_2 è un sottogruppo normale di G per il punto 5 del Lemma 73. Inoltre $[N_1, N_2] \subset N_1 \cap N_2 = \{e\}$, quindi i due sottogruppi commutano e dunque f è un morfismo. f è suriettiva per definizione. L'iniettività discende immediatamente dalla ipotesi sulla intersezione sfruttando il punto 2 del Lemma 73. Per k qualsiasi ragioniamo induttivamente supponendo vera la tesi per $k - 1$ sottogruppi. Dunque $\bar{N} := N_2 \cdots N_k$ è un sottogruppo normale di G. Per ipotesi $N_1 \cap \bar{N} = \{e\}$. Segue di nuovo dal punto 5 del Lemma 73 che $N_1 \cdot \bar{N} = N_1 \cdots N_k$ è un sottogruppo normale di G. Inoltre l'applicazione f fattorizza nel modo seguente

$$N_1 \times N_2 \times \cdots \times N_k \xrightarrow{\mathrm{id}_{N_1} \times g} N_1 \times \bar{N} \xrightarrow{h} N_1\bar{N} = N_1N_2 \cdots N_k$$

$$\text{(arco } f \text{ da } N_1 \times N_2 \times \cdots \times N_k \text{ a } N_1\bar{N}\text{)}$$

dove $g : N_2 \times \cdots \times N_k \to \bar{N}$, $g(n_2, \ldots, n_k) = n_2 \cdots n_k$, $h(n_1, \bar{n}) = n_1\bar{n}$ e dove $\mathrm{id}_{N_1} \times g$ indica l'applicazione $(n_1, n_2, \ldots, n_k) \mapsto (n_1, g(n_2, \ldots, n_k))$. L'applicazione g è un isomorfismo, dunque anche $\mathrm{id}_{N_1} \times g$ lo è. Mentre h è un isomorfismo per il caso $k = 2$. □

Lemma 75. *Se G è un gruppo finito e tutti i sottogruppi di Sylow sono normali, allora G è isomorfo al loro prodotto.*

Dimostrazione. Sia $o(G) = p_1^{a_1} \cdots p_n^{a_n}$ e siano P_i l'unico p_i-Sylow. Cominciamo dimostrando per induzione su k che per ogni $k = 1, \ldots, n$ si ha

$$|P_1 \cdots P_k| = p_1^{a_1} \cdots p_k^{a_k}. \tag{2.10}$$

Se $k = 1$ è ovvio. Supponiamo $k > 1$. Osserviamo che $N := P_1 \cdots P_{k-1}$ è un sottogruppo normale di G, poiché tutti i P_i sono normali. Se $x \in N \cap P_k$ allora $o(x)$ divide $o(N)$ che $o(P_k)$. Ma $o(P_k) = p_k^{a_k}$, mentre $o(N) = p_1^{a_1} \cdots p_{k-1}^{a_{k-1}}$ per ipotesi induttiva. Pertanto $o(x) = 1$ e $N \cap P_k = \{e\}$. Segue quindi dal Lemma 73 che $P_1 \cdots P_k = NP_k$ è un gruppo isomorfo s $N \times P_k$, quindi $|P_1 \cdots P_k| = p_1^{a_1} \cdots p_k^{a_k}$. Questo dimostra la (2.10). Per $k = n$ otteniamo $|P_1 \cdots P_n| = |P_1| \cdots |P_n| = |G|$ dunque $P_1 \cdots P_n = G$ e l'applicazione

$$f : P_1 \times \cdots \times P_n \to G, \quad f(x_1, \ldots, x_n) := x_1 \cdots x_n$$

è biunivoca. D'altro canto, per lo stesso ragionamento fatto sopra

$$(P_1 \cdots P_{n-1}) \cap P_n = \{e\}.$$

Infatti se x sta in questa intersezione il suo ordine divide sia $p^{a_1} \cdots p_{n-1}^{a_{n-1}}$, che $p_n^{a_n}$, quindi $x = e$. Per di più in questa uguaglianza l'ordine dei P_i non conta, quindi con lo stesso ragionamento si ottiene anche $P_i \cap (P_1 \cdots \hat{P}_i \cdots P_n) = \{e\}$. Il Lemma 74 permette di concludere. □

Lemma 76. *Se $o(G) = pq$ con p e q primi tali che $p < q$ e $p \nmid (q-1)$, allora G è ciclico.*

Dimostrazione. $n_p | q$, dunque $n_p = 1$ o $n_p = q$. Nel secondo caso avrei $1 \equiv n_p \equiv q \mod p$, contro l'ipotesi. Dunque $n_p = 1$. D'altro canto $n_q | p$ e $n_q = 1 + kq$. Se $k \neq 0$, $1 + kq > q > p$, dunque $1 + kq \nmid p$. Pertanto $k = 0$ e $n_q = 1$. Dunque se P è il p-Sylow e Q è il q-Sylow, allora $P, Q \lhd G$, $P \cap Q = \{e\}$. Dunque $|PQ| = pq = |G|$. □

77. Consideriamo adesso la seguente situazione: G è un gruppo, $N \lhd G$ e H è un sottogruppo di G. Inoltre $G = NH$ e $N \cap H = \{e\}$. In questo caso l'applicazione $f : N \times H \to G$ è biunivoca. Se $h \in H$, l'automorfismo interno $\mathrm{inn}_h \in \mathrm{Aut}\, G$ preserva H, cioè $\mathrm{inn}_h(N) = N$, dunque la sua restrizione ad N è un automorfismo (non necessariamente interno!) di N, che indichiamo con θ_h:

$$\varepsilon_h : N \to N, \quad \varepsilon_h(n) = hnh^{-1}. \tag{2.11}$$

L'applicazione $\varepsilon : H \to \operatorname{Aut} N$ è un morfismo di gruppi. Osserviamo che se $(n_1, h_1), (n_2, h_2) \in N \times H$, allora

$$\begin{aligned} f(n_1, h_1) \cdot f(n_2, h_2) = n_1 h_1 n_2 h_2 = n_1 \theta_{h_1}(n_2) h_1 h_2 = \\ = f(n_1 \varepsilon_{h_1}(n_2), h_1 h_2). \end{aligned} \tag{2.12}$$

Questo significa che se conosciamo N ed H, con la loro struttura di gruppo e poi conosciamo anche il morfismo ε, allora siamo in grado di calcolare il prodotto di G e dunque possiamo ricostruire la struttura del gruppo G.

Questo ragionamento può anche essere ribaltato.

Teorema 78. *Siano N e H gruppi e sia $\theta : H \to \operatorname{Aut} N, h \mapsto \theta_h$ un morfismo. Definiamo su $N \times H$ un prodotto $\bullet_\theta$ mediante la formula*

$$(n_1, h_1) \bullet_\theta (n_2, h_2) := (n_1 \theta_{h_1}(n_2), h_1 h_2). \tag{2.13}$$

Allora $(N \times H, \bullet_\theta)$ è un gruppo. Viene indicato con il simbolo $N \rtimes_\theta H$ e viene chiamato prodotto semidiretto *di N ed H. L'elemento neutro è (e, e) mentre $(n, h)^{-1} = (\theta_{h^{-1}}(n^{-1})$. Inoltre $N \times \{e\}$ è un sottogruppo normale di $N \rtimes_\theta H$ isomorfo a N, mentre $\{e\}$ è un sottogruppo di $N \rtimes_\theta H$ isomorfo ad H e $N \rtimes_\theta H = (N \times \{e\}) \cdot (\{e\} \times H)$. Infine il morfismo ε di (2.11) coincide con θ.*

Dimostrazione. È facile verificare che (e, e) è un inverso bilatero per il prodotto $\bullet_\theta$. Vediamo l'associatività

$$\begin{aligned} (n_1, h_1) \bullet_\theta ((n_2, h_2) \bullet_\theta (n_3, h_3)) = (n_1 \theta_{h_1}(n_2 \theta_{h_2}(n_3)), h_1 h_2 h_3) \\ ((n_1, h_1) \bullet_\theta (n_2, h_2)) \bullet_\theta (n_3, h_3) = (n_1 \theta_{h_1}(n_2) \theta_{h_1 h_2}(n_3), h_1 h_2 h_3). \end{aligned}$$

Questi due termini coincidono perché θ_{h_1} è un automorfismo e θ è un morfismo. È facile verificare che $(\theta_{h^{-1}}(n^{-1})$ è un inverso bilatero di (n, h) per il prodotto $\bullet_\theta$. Abbiamo dimostrato che $G := (N \times H, \bullet_\theta)$ è un gruppo. Consideriamo le mappe

$$\alpha : N \to G, \quad \alpha(n) = (n, e), \qquad \beta : H \to G, \quad \beta(h) = (e, h).$$

È facile verificare che sono entrambe morfismi. Per esempio $\alpha(n) \bullet_\theta \alpha(\bar{n}) = (n, e) \bullet_\theta (\bar{n}, e) = (n \theta_e(\bar{n}), e)$. Siccome θ è un morfismo $\theta_e = \mathrm{id}_N$, dunque $\alpha(n) \bullet_\theta \alpha(\bar{n}) = (n\bar{n}, e) = \alpha(n\bar{n})$. Poniamo $N' := \operatorname{im} \alpha = N \times \{e\}$, $H' := \operatorname{im} \beta = \{e\} \times H$. Segue che N' ed H' sono sottogruppi ed è evidente che $N'H' = N \times H = G$, siccome

$$(n, e) \bullet_\theta (e, h) = (n, h).$$

Infine

$$(n,h)\bullet_\theta(\bar{n},e)\bullet_\theta(n,h)^{-1}=(n\theta_h(\bar{n})n^{-1},e).$$

Questo dimostra che $N'\lhd G$ e anche che $(e,h)\bullet_\theta(\bar{n},e)\bullet_\theta(e,h)^{-1}=(\theta_h(\bar{n}),e)$. Dunque l'isomorfismo ε di (2.11) è

$$\varepsilon_{(e,h)}((n,e))=(e,h)\bullet_\theta(\bar{n},e)\bullet_\theta(e,h)^{-1}=(\theta_h(\bar{n}),e).$$

Quindi identificando N con N' ed H con H' nel modo ovvio, $\varepsilon=\theta$. □

Potremmo chiamare la costruzione sopra prodotto semidiretto *esterno*. La situazione descritta in 77 potremmo invece chiamarla prodotto semidiretto *interno*. Nel teorema sopra abbiamo visto che il prodotto semidiretto esterno può essere visto come un prodotto semidiretto interno. Ora vediamo il viceversa.

Proposizione 79. *Sia G un gruppo, $H\subset G$ un sottogruppo, $N\lhd G$. Definiamo ε come in* (2.11)*. Se $G=NH$ e $H\cap N=\{e\}$, allora $G\cong N\rtimes_\varepsilon H$.*

Dimostrazione. Basta dimostrare che l'applicazione $f:N\times H\to G$ è un isomorfismo di $N\rtimes_\varepsilon H$ su G. Questa applicazione è suriettiva perché $G=NH$ ed è iniettiva perche $N\cap H=\{e\}$ (Lemma 73). Infine f è un morfismo per la (2.12) e per la definizione (2.13) del prodotto $\bullet_\theta$. □

Esercizio 80. *Siano N ed H gruppi e $\theta,\theta':H\to\operatorname{Aut}N$ morfismi. Se esistono $\alpha\in\operatorname{Aut}N$ e $\beta\in\operatorname{Aut}H$ tali che*

$$\theta'_{\beta(h)}=\alpha\circ\theta_h\circ\alpha^{-1},$$

allora l'applicazione

$$F:N\rtimes_\theta H\longrightarrow N\rtimes_{\theta'}H,\quad F(n,h):=(\alpha(n),\beta^{-1}(h))$$

è un isomorfismo $N\rtimes_\theta H\cong N\rtimes_{\theta'}H$.

Gruppi risolubili Sia G un gruppo. Il sottogruppo dei commutatori $[G,G]$ è caratteristico. Se $N\lhd G$, allora G/N è abeliano se e solo se $[G,G]\subset N$.

Una *catena* o *serie normale* in G è una successione di sottogruppi

$$G=G_0\supset G)1\supset\cdots\supset G_i\supset G_{i+1}\supset\cdots$$

tale che $G_{i+1} \lhd G_i$ per ogni i e $G_n = \{1\}$ per qualche n. I gruppi G_i/G_{i+1} si chiamano *fattori* della catena.

Dato G poniamo $D^0G := G$, $D^{i+1}G := [D^iG, D^iG]$. Otteniamo così la *catena dei derivati* di G:

$$G = D^0G \supset D^1G \supset \cdots \supset D^iG \supset \cdots$$

Definizione 81. *Il gruppo G è risolubile se esiste una catena normale con fattori abeliani.*

Esercizio 82. *Sia $f : G \twoheadrightarrow G'$ un epimorfismo di gruppi e siano $N, N' \subset G$ sottogruppi tali che $N \lhd N'$. Allora $f^{-1}(N')/f^{-1}(N) \cong N'/N$.*

Teorema 83. *Sia G un gruppo finito. Le seguenti condizioni sono equivalenti:*

1. *G è risolubile.*
2. *Esiste una catena normale con fattori ciclici di ordine primo.*
3. *$D^nG = \{e\}$ per qualche n (ossia la catena dei derivati è una serie normale).*

Dimostrazione. Chiaramente 2 implica 1. Vediamo il viceversa: sia $G = G_0 \supset \cdots \supset G_n = \{1\}$ una serie normale con G_k/G_{k+1} abeliano. Supponiamo che $G_k/G_{k+1} = A \times B$ con A è B sottogruppi del gruppo abeliano G_k/G_{k+1}. Sia $\pi : G_k \to G_k/G_{k+1}$ la proiezione canonica. Allora ponendo $G'_k := \pi^{-1}(A)$, otteniamo una nuova serie normale

$$G = G_0 \supset \cdots \supset G_k \supset G'_k \supset G_{k+1} \supset \cdots \supset G_n = \{1\}.$$

Questa è un raffinamento della precedente e ha gli stessi fattori, salvo che il fattore G_k/G_{k+1} è sostituto dai due fattori G_k/G'_k e G'_k/G_{k+1}. Per l'Esercizio 82

$$G'_k/G_{k+1} = \pi^{-1}(A)/G_{k+1} \cong A,$$
$$G_k/G'_k = \frac{\pi^{-1}(A \times B)}{\pi^{-1}(A)} \cong \frac{A \times B}{A} \cong B.$$

Per il teorema di classificazione dei gruppi abeliani finiti c'è una scomposizione

$$G_k/G_{k+1} \cong \oplus_{i=1}^{s} \oplus_{j=1}^{t_i} \mathbb{Z}/(p_i^{l_{ij}})$$

con p_i primi. Applicando ripetutamente il ragionamento fatto sopra possiamo raffinare la catena in modo che tutti i fattori siano della forma $\mathbb{Z}/(p^n)$ con p primo. Indichiamo sempre con $\{G_i\}$ la catena raffinata in questo modo. Vogliamo fare un ulteriore raffinamento in modo che tutti i quozienti siano della forma $\mathbb{Z}/p$ per un primo p (che dipende dal fattore). Consideriamo dunque un fattore $G_k/G_{k+1} \cong \mathbb{Z}/(p^n)$. Poniamo

$$G_{k,i} := \pi^{-1}((p^i)/(p^n)), \quad i = 0, 1, \ldots, n.$$

Allora $G_{k,0} = \pi^{-1}(\mathbb{Z}/(p^n)) = G_k$ e $G_{k,i} \rhd G_{k,i+1}$. Sempre per l'Esercizio 82

$$G_{i,k}/G_{k,i+1} \cong \frac{(p^i)/(p^n)}{(p^{i+1})/(p^n)} \cong \frac{(p^i)}{(p^{i+1})} \cong \mathbb{Z}/p.$$

Abbiamo dimostrato che 1 implica 2.
Per convincersi che 3 implica 1 è sufficiente osservare che se $D^nG = \{e\}$ allora la serie derivata è una catena normale e i fattori $D^iG/D^{i+1}G = D^iG/[D^iG, D^iG]$ sono abeliani.
Vediamo che viceversa 1 implica 3. Sia $\{G_i\}_i$ una catena normali con fattori abeliani. Allora $D^iG \subset G_i$. Infatti per $i = 0$ questo è ovvio. Se $D^iG \subset G_i$, allora $D^{i+1}G = [D^iG, D^iG] \subset [G_i, G_i]$. Siccome G_i/G_{i+1} è abeliano, $[G_i, G_i] \subset G_{i+1}$. Dunque $D^{i+1}G \subset G_{i+1}$. Questo dimostra che $D^iG \subset G_i$ per ogni i. Se $G_n = \{e\}$, allora anche $D^nG = \{e\}$. □

Il gruppo moltiplicativo di un campo finito

Lemma 84. *Sia G un gruppo di ordine n. Supponiamo che per ogni d che divide n si abbia $|\{x \in G : x^d = e\}| \leq d$. Allora G è ciclico.*

Dimostrazione. Poniamo $G^d := \{x \in G : x^d = e\}$ e $G_d := \{x \in G : o(x) = d\}$. Sia $d|n$. Se $G_d \neq \varnothing$, fissiamo $x_0 \in G_d$. Allora $\langle x_0 \rangle \subset G^d$ e $|\langle x_0 \rangle| = d$. Dall'ipotesi segue dunque $\langle x_0 \rangle = G^d$. Quindi $G_d \subset G^d$, anzi G_d è l'insieme dei generatori di $\langle x_0 \rangle \cong \mathbb{Z}/d$. Pertanto $|G_d| = \varphi(d)$. Abbiamo dimostrato che per ogni d che divide n o $|G_d| = 0$ oppure $|G_d| = \varphi(d)$. Ma per la formula di Gauss (2.3)

$$n = |G| = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n.$$

Dunque si ha in realtà $|G_d| = \varphi(d)$ per oni d e quindi in particolare $|G_n| = \varphi(n) > 0$, dunque esistono generatori di G. □

Teorema 85. *Sia F un campo e sia $(F^* := F - \{0\}, \cdot)$ il suo gruppo moltiplicativo. Se $G \subset F^*$ è un sottogruppo finito, allora G è ciclico. un gruppo ciclico.*

Dimostrazione. Sia $n := |G|$. Per ogni d che divide n gli elementi $x \in F^*$ tali che $x^d = 1$ sono tutte e sole le radici del polinomio $x^d - 1$ che ha grado d. Dunque questi elementi sono al massimo d. A maggior ragione $|G_d| \leq d$. Il teorema segue dal precedente lemma. □

Capitolo 3

Campi

3.1 Estensioni di campi

Definizione 86. *Dato un anello A consideriamo il morfismo $\varphi : \mathbb{Z} \to A$, $\varphi(m) := m \cdot 1_A$. Il nucleo di φ è un ideale principale. C'è un unico $n \geq 0$ tale che* $\ker \varphi = (n)$. *Diciamo che n è la* caratteristica *dell'anello A.*

Lemma 87. *Sia K un campo di caratteristica n. Se $n = 0$, allora $m \cdot x = 0$ con $m \in \mathbb{Z}$ e $x \in K$ se e solo se $x = 0$ o $m = 0$. Se $n > 0$ allora n è primo, $n \cdot x = 0$ per ogni $x \in K$ e se $m \cdot x = 0$ per un $x \in K$, $x \neq 0$, allora $n|m$.*

L'immagine di $\varphi : \mathbb{Z} \to K$ è contenuta in qualunque sottocampo di K. Il campo da essa generato viene chiamato *campo primo* di K. Se $\operatorname{car} K = 0$, l'immagine $\varphi(\mathbb{Z}) \subset K$ è un anello isomorfo a $\mathbb{Z}$ e il campo primo è isomorfo a $\mathbb{Q}$. Se $\operatorname{car} K = p$, allora $\varphi(Z) \cong Z/(p) \cong \mathbb{Z}/p$ e coincide con il campo primo.

Una *estensione di campi* è un morfismo di anelli $i : F \to E$ dove F ed E sono campi. Siccome i è un morfismo di anelli, $\ker i$ è un ideale di F. Siccome $i(1) = 1$, $\ker i \subsetneq F$. Dunque $\ker i = \{0\}$ e è iniettivo. Tramite i si può identificare F con $i(F) \subset E$. Quindi ci si può spesso ridurre al caso in cui $F \subset E$ è un sottocampo. Salvo indicazione contraria faremo sempre questa identificazione. Se $F \subset E$ è una estensione di campi, scriviamo E/F.

Se E/F è una estensione di campi, E è uno spazio vettoriale su F. Infatti possiamo restringere $(F, +)$ è un gruppo abeliano. Inoltre possiamo restringere il prodotto di E al sottoinsieme $F \times E$ e otteniamo così una applicazione $F \times E \to E$. È immediato verificare che con questa operazione E è uno spazio vettoriale su F. Il grado dell'estensione è il numero

$$[E : F] := \dim_F E.$$

Esercizio 88. *Sia E_1/F e E_2/F due estensioni di F. Consideriamo E_1 ed E_2 come F-spazi vettoriali nel modo appena descritto. Dimostrare che un morfismo di anelli $\sigma : E_1 \to E_2$ è una applicazione F-lineare se e solo se $\sigma_{|F} = \mathrm{id}_F$.*

Ci sono estensioni finite, p.e. $\mathbb{C}/\mathbb{R}$ ha grado 2, ed infinite, per esempio $\mathbb{R}/\mathbb{Q}$.

Se E/K è una estensione di campi, un *campo intermedio* è un campo F tale $K \subset F \subset E$. Se $S \subset E$ è un sottoinsieme qualsiasi, il *sottocampo generato da S*, indicato con $K(S)$, è l'intersezione di tutti i campi intermedi che contengono S:

$$K(S) := \bigcap_{\substack{K \subset F \subset E \\ S \subset F}} F.$$

Data una estensione E/K, e $\alpha \in E$ il sottocampo $K(\alpha)$ è formato da tutte le funzioni razionali valutate in α:

$$K(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} : p, q \in K[x], q(\alpha) \neq 0 \right\}.$$

Lemma 89. *Se E/F ed FK sono estensioni finite, anche E/K lo è e $[E : K] = [E : F] \cdot [F : K]$. Viceversa, se E/K è finita anche E/F e F/K sono finite.*

Se $F \subset E$ ed S è un sottoinsieme di E, allora $F(S)$ è formato da tutti gli elementi di E che posso scrivere nella forma $f(\alpha_1, \ldots, \alpha_n)$, dove $f = p/q \in F(X_1, \ldots, X_n)$ è una funzione razionale definita in $(\alpha_1, \ldots, \alpha_n)$, ossia tale che $q(\alpha_1, \ldots, \alpha_n) \neq 0$.

Sia E/F una estensione. Diciamo che $S \subset E$ è un sistema di *generatori* dell'estensione E/F se $E = F(S)$.

Una estensione E/F è *finitamente generata* se esiste un insieme finito S tale che $E = F(S)$.

Una estensione E/F è *semplice* se è generata da un solo elemento, ossia esiste $\alpha \in E$ tale che $E = F(\alpha)$.

Sia E/F una estensione. L'elemento $\alpha \in E$ è *algebrico* su F se esiste un polinomio $p(x) \in F[X]$ tale che $p(x) \not\equiv 0$ e $p(\alpha) = 0$. Se α non è algebrico, diciamo che è *trascendente* su F. Possiamo riformulare queste definizione usando il morfismo di valutazione in α:

$$\varphi : F[X] \longrightarrow E, \qquad p(x) \mapsto p(\alpha).$$

L'elemento α è trascendente se φ è iniettivo, mentre α è algebrico se $\ker\varphi \neq \{0\}$. In questo caso, si chiama *polinomio minimo* di α su F, indicato con $m_{\alpha,F}$ o m_α, il generatore monico dell'ideale $\ker\varphi$.

Esercizio 90. *Se $\alpha \in E$ è trascendente su F, allora $[E : F] = \infty$.*

Lemma 91. *Se $E = F(\alpha)$ e α è algebrico su F e ha polinomio minimo f, allora la valutazione in α induce un isomorfismo sia di campi che di spazi vettoriali su F*

$$F[X]/(f) \cong F(\alpha), \quad g(x) + (f) \mapsto g(\alpha).$$

Inoltre $[F(\alpha) : F] = \deg f$.

Dimostrazione. Sia φ il morfismo di valutazione in α. Allora $\operatorname{im}\varphi \subset E$ è un dominio di integrità. Dunque $\ker\varphi$ è un ideale primo. Ma $F[X]$ è un dominio a ideali principali, dunque $\ker\varphi$ è automaticamente massimale. Quindi $\operatorname{im}\varphi \cong F[X]/\ker\varphi$ è in realtà un campo. Chiaramente $\alpha = \varphi(X) \in \operatorname{im}\varphi$. Inoltre $F \subset \operatorname{im}\varphi$: se $\lambda \in F$, posso vedere λ come un polinomio costante in $F[X]$ e chiaramente $\varphi(\lambda) = \lambda \in \operatorname{im}\varphi$. Dunque $F(\alpha) \subset \operatorname{im}\varphi$. D'altronde sia K un campo intermedio fra F ed E che contiene α. Allora K contiene anche $p(\alpha)$ per ogni $p(X) \in F[X]$. Dunque $\operatorname{im}\varphi \subset K$. Pertanto $\operatorname{im}\varphi = F(\alpha)$. Dunque $F(\alpha) \cong F[X]/\ker\varphi$. Ma $(f) = \ker\varphi$ per la definizione di polinomio minimo. Sia $\pi : F[X] \to F[X]/(f)$ la proiezione e sia $d := \deg f$. Per concludere basta dimostrare che $\mathscr{B} = \{\pi(1), \pi(X), \ldots, \pi(X^{d-1})\}$ è una base di $F[X]/(f)$ su F. Siano dati scalari $\lambda_i \in F$ tali che

$$\lambda_0\pi(1) + \lambda_1\pi(X) + \cdots + \lambda_{d-1}\pi(X^{d-1}) = 0$$

Sfruttando che π è sia un morfismo di anelli che di spazi vettoriali su F otteniamo allora

$$\begin{aligned} &\pi(\lambda_0 \cdot 1 + \lambda_1 X + \cdots + \lambda_{d-1}X^{d-1}) = 0, \\ \implies &q(X) := \lambda_0 \cdot 1 + \lambda_1 X + \cdots + \lambda_{d-1}X^{d-1} \in \ker\pi. \end{aligned}$$

Ma allora avrei $q \in (f)$ e $\deg q < \deg f$, quindi $q = 0$, ossia $\lambda_i = 0$. Dunque $\mathscr{B}$ è linearmente indipendente. Sia poi $y \in F[X]/(f)$. Allora $y = \pi(h)$ per qualche polinomio $h \in F[X]$. Dividiamo h per f: $h = qf + r$ con $q, r \in F[X]$ e $r = 0$ o $\deg r < d$. Allora $y = \pi(h) = \pi(r)$ che sta certamente nello spazio generato da $\mathscr{B}$. □

Questo lemma dice in particolare che se α è algebrico su F, gli elementi di $F[\alpha]$ si possono scrivere come polinomi in α. Non c'è bisogno di usare le

funzioni razionali. Possiamo ridimostrare questo fatto in modo più diretto, anche se completamente equivalente: sia $y \in p(\alpha) \in F(\alpha)$ e supponiamo $y \neq 0$. Allora $p \notin \ker \varphi$, dunque $f \nmid p$, dunque $(F, p) = 1$ perché f è irriducibile. Sia $1 = qp + hf$ con $q, h \in F[X]$. Allora $1 = q(\alpha)p(\alpha)$. Quindi $1/y$ è ancora della forma $q(\alpha)$. Questo spiega perché le espressioni $p(\alpha)$ con p un polinomio formino un campo.

Corollario 92. *Sia E/F una estensione e sia $\alpha \in E$. Allora α è algebrico su F se e solo se $[F(\alpha) : F] < \infty$.*

Dimostrazione. Se $[F(\alpha) : F] = d$, allora gli elementi $1, \alpha, \ldots, \alpha^d$ sono linearmente dipendenti su F, dunque esistono $a_0, \ldots, a_d \in F$ non tutti nulli e tali che

$$a_0 + a_1\alpha + \cdots + a_d\alpha^d = 0.$$

Questo dimostra che α è algebrico. Un'altra dimostrazione si ottiene sfruttando l'Esercizio 90. Viceversa, se α è algebrico, allora $[F(\alpha) : F] = \deg m_\alpha < \infty$. □

Una estensione E/F è *algebrica* se ogni $\alpha \in E$ è algebrico su F.

Lemma 93. *Sia E/F una estensione. Le tre proprietà seguenti sono equivalenti*

1. *E/F è finita;*
2. *E/F è algebrica e finitamente generata;*
3. *E/F è generata da un numero finito di elementi algebrici.*

Lemma 94. *Consideriamo tre campi $K \subset F \subset E$. Le estensioni E/F ed F/K sono algebriche se e solo se E/K è algebrica.*

Procedimento di Kronecker . *Sia F un campo e sia $f(x) \in F[X]$ un polinomio irriducibile. Allora esiste una estensione algebrica E/F nella quale f ha una radice. Inoltre possiamo supporre che $E = F(\alpha)$ dove α è una radice di f e in tal caso $[E : F] = \deg f$.*

Dimostrazione. Poniamo $E := F[X]/(f)$ e sia $\pi : F[X] \to E$ la proiezione. Siccome f è irriducibile, (f) è massimale, dunque E è un campo. La composizione $F \to F[X] \to F[X]/(f) = E$, dà un morfismo $F \to E$, dunque E/F è una estensione di campi. La proiezione π è un morfismo di anelli. Siccome $F[X]$ è uno spazio vettoriale su F e (f) è un sottospazio, il quoziente E è

anche uno spazio vettoriale su F e la proiezione π è anche F-lineare. Poniamo $\alpha := \pi(X)$. Vogliamo vedere che $f(\alpha) = 0$. Sia $f(X) = \sum_{i=0}^{n} a_i X^i$. Allora

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} a_i \, \pi(X)^i = \sum_{i=0}^{n} a_i \pi(X^i) =$$
$$= \pi\left(\sum_{i=0}^{n} a_i X^i\right) = \pi(f).$$

Nella prima riga $\pi(X)^i = \pi(X^i)$ perché π è un morfismo di anelli; nella seconda invece usiamo che π è F-lineare. Siccome $f \in (f)$, $\pi(f) = 0$. Dunque $\alpha \in E$ è una radice di f. □

Corollario 95. *Sia F un campo e siano $f_1, \ldots, f_n \in F[X]$. Allora esiste una estensione finita E/F in cui ciascuno dei polinomi ha una radice.*

Definizione 96. *Un campo E è* algebricamente chiuso *(e per indicarlo scriviamo $E = \bar{E}$) se ogni polinomio non costante (cioè di grado ≥ 1) ha almeno una radice in E.*

Esercizio 97. *Il campo E è algebricamente chiuso se e solo se ogni polinomio $f(X) \in E[X]$ di grado $n \geq 1$ si spezza in fattori lineari su E, cioè $f(X) = a(x - \lambda_1) \cdots (x - \lambda_h)$ in $E[X]$.*

Definizione 98. *Una* chiusura algebrica *di un campo K è una estensione algebrica L/K con L è algebricamente chiuso.*

Teorema 99. *Per ogni campo K esiste una chiusura algebrica.*

Incominciamo con il seguente lemma che ha interesse indipendente.

Lemma 100. *Se K è un campo e L/K è una estensione con L algebricamente chiuso, allora l'insieme*

$$\bar{K}^L := \{\alpha \in L : \alpha \text{ è algebrico su } K\}$$

è un campo intermedio $K \subset \bar{K}^L \subset L$, è algebricamente chiuso e l'estensione $\bar{K}^L/K$ è algebrica. Dunque $\bar{K}^L/K$ è una chiusura algebrica di K.

Dimostrazione del Teorema 99. Sia $I := \{f \in K[X] : \deg f \geq 1\}$. L'insieme I è infinito. Sia $A := K[X_f : f \in I]$. Se $f \in I$, allora X_f è una variabile dell'anello A. D'altronde $f = f(X)$ è un polinomio nella variabile X. Possiamo sostituite la variabile X_f alla variabile X e otteniamo il polinomio $f(X_f)$.

Se $f(X) = \sum_{i=0}^{n} a_i X^i$, allora $f(X_f) = \sum_{i=0}^{n} a_i X_f^i$. Quindi $f(X_f) \in A$. Sia $\mathfrak{a}$ l'ideale di A generato da tutti gli elementi $f(X_f)$ al variare di f in I. Per prima cosa facciamo vedere che $\mathfrak{a} \neq A$. Ragioniamo per assurdo. Se fosse $\mathfrak{a} = A$, avremmo $1 \in \mathfrak{a}$, dunque esisterebbero $f_1, \ldots, f_n \in I$ e $g_1, \ldots, g_n \in A$ tali che

$$1 = \sum_{i=1}^{n} g_i f_i(X_{f_i}).$$

Per il Corollario 95 una estensione finita K'/K che contiene elementi $\alpha_1, \ldots \alpha_n$ tali che $f_i(\alpha_i) = 0$ per ogni $i = 1, \ldots, n$. A questo punto sia $\sigma : K \to K'$ l'inclusione e consideriamo la valutazione

$$K[X_i : i \in I] \longrightarrow K', \qquad \begin{cases} X_{f_i} \mapsto \alpha_i & i = 1, \ldots, n \\ X_f \mapsto 0 & f \neq f_i \text{ per } i = 1, \ldots, n. \end{cases}$$

Tramite questa valutazione i polinomi g_i assumeranno certi valori $\beta_i \in K'$, mentre i polinomi $f_i(X_{f_i})$ verrano valutati in α_i e dunque si annullerrano. Pertanto otterremmo l'equazione $1 = \sum_i \beta_i \cdot 0 = 0$. Assurdo. Questo dimostra che $1 \notin \mathfrak{a}$ e $\mathfrak{a} \subsetneq A$. Sia quindi $\mathfrak{m}$ un ideale massimale di A contenente $\mathfrak{a}$. Poniamo $L_1 := A/\mathfrak{m}$ e sia $\pi : A \to L_1$ è la proiezione canonica. Allora L_1 è un campo e K abbiamo il morfismo $K \to A \xrightarrow{\pi} L_1$, dunque L_1/K è una estensione. Poniamo $L_0 := K$. L'estensione L_1/L_0 ha la seguente proprietà: ogni polinomio non costante in $L_0[X]$ ha almeno una radice in L_1. Iterando la costruzione otteniamo per ogni $n \in \mathbb{N}$ una estensione L_n/L_{n-1} tale che ogni polinomio non costante in $L_{n-1}[X]$ ha una radice in L_n. Poniamo

$$L := \bigcup_{n=0}^{\infty} L_n.$$

Se fissiamo un numero finito di elementi di L, esiste n tale che L_n contiene tutti gli elementi considerati. Da questo segue che L è un campo. Se $f(X) \in L[X]$, i coefficienti di f appartengono a L_n per un certo n. Dunque $f(X) \in L_n[X]$, per cui $f(X)$ ha una radice in $L_{n+1}[X]$. Questo dimostra che L è algebricamente chiuso. Applicando il Lemma 100 otteniamo una chiusura algebrica di K. (In realtà si può dimostrare facilmente che ciascuna delle estensioni L_{n+1}/L_n è algebrica e da questo discende che anche L/K è algebrica.) □

Ora ci chiediamo se la chiusura algebrica di un campo K è unica. Risulta che è unica a meno di isomorfismo, anche se questo isomorfismo non è canonico. La dimostrazione sfrutta i due teoremi seguenti che serviranno anche

in altri passi decisivi. Per prima cosa introduciamo la seguente notazione: se $\sigma : K \to L$ è un morfismo di campi, e $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, allora f^σ indica il polinomio

$$f^\sigma = \sum_{i=0}^{n} \sigma(a_i) X^i.$$

L'applicazione $f \mapsto f^\sigma$ è un morfismo $K[X] \to L[X]$ che estende σ.

Teorema 101. *Sia $\sigma : K \to L$ un morfismo di campi. Sia $K' = K(\alpha)$ una estensione semplice algebrica e sia f il polinomio minimo di α.*

1. *Se $\sigma' : K' \to L$ è un morfismo che estende σ, allora $\sigma'(\alpha)$ è una radice di f^σ.*

2. *Se $\beta \in L$ è una radice di f^σ, allora esiste uno ed un solo morfismo $\sigma' : K' \to L$ che estende σ e tale che $\sigma'(\alpha) = \beta$.*

3. *Le possibili estensioni di σ a K' sono al più* $\deg f = [K' : K]$.

Dimostrazione. Il punto (1) è semplice: siccome σ' estende σ, $f^\sigma(\sigma'(\alpha)) = f^{\sigma'}(\sigma'(\alpha)) = \sigma'(f(\alpha)) = \sigma'(0) = 0$.
(2) Sappiamo dal Lemma 91 che esiste un isomorfismo $\varphi : K[X](f) \cong K(\alpha)$ tale che $\varphi(X) = \alpha$. Per lo stesso motivo, siccome β è una radice di f^σ, c'è un isomorfismo $\psi : \sigma(K)[X]/(f^\sigma) \cong \sigma(K)(\beta)$. Infine σ induce un isomorfismo

$$\eta : K[X]/(f) \xrightarrow{\cong} \sigma(K)[X]/(f^\sigma), \quad g(X) + (f) \mapsto g^\sigma(X) + (f^\sigma).$$

Ovviamente $\varphi_{|K} = \mathrm{id}_K$ e $\psi_{|\sigma(K)} = \mathrm{id}_{\sigma(K)}$. Se includiamo K in $K[X]/(f)$ mediante l'applicazione $\lambda \mapsto \lambda + (f)$, allora $\eta_{|K} = \sigma$. Allora poniamo $\sigma' := \psi\eta\varphi^{-1}$. Questa mappa è un isomorfismo di $K(\alpha)$ su $\sigma(K)(\beta) \subset L$ e ${\sigma'}_{|K} = \sigma$. Questo dimostra l'esistenza. D'altro canto, K' è generato da K e α come anello. Quindi ogni morfismo da K' in L è determinato dal suo comportamento su K e su α. Se un morfismo estende σ e manda α in β, deve coincidere con quello appena costruito.
(3) Per i due primi punti l'applicazione che associa ad una estensione σ' l'elemento $\sigma'(\alpha$ è una mappa biunivoca dall'insieme delle estensioni nell'insieme delle radici di f^σ in L. □

Teorema 102. *Sia K'/K una estensione algebrica e sia L un campo algebricamente chiuso. Sia $\sigma : K \to L$ un morfismo. Allora esiste sempre un morfismo $\sigma' : K' \to L$ che estende σ. Se K' è algebricamente chiuso e $L/\sigma(K)$ è algebrica, allora ogni estensione è un isomorfismo $K' \cong L$.*

Dimostrazione. Consideriamo l'insieme $\mathfrak{M}$ formato da tutte le coppie (F, τ), dove F è un campo intermerdio $K \subset F \subset K'$ e $\tau : F \to L$ è un morfismo che estende σ. Ł'insieme $\mathfrak{M} \neq \varnothing$ perché $(K, \sigma) \in \mathfrak{M}$. Consideriamo su $\mathfrak{M}$ la seguente relazione:

$$(F, \tau) \leq (F', \tau') \Longleftrightarrow F \subset F' \text{ e } \tau = \tau'_{|F}.$$

È facile verificare che si tratta di una relazione di ordine. Sia $\mathfrak{C} := \{(F_\alpha, \tau_\alpha)\}_{\alpha \in I}$ una catena in $(\mathfrak{M}, \leq)$, ossia per ogni $\alpha, \beta \in I$ o $(F_\alpha, \tau_\alpha) \leq (F_\beta, \tau_\beta)$ o $(F_\beta, \tau_\beta) \leq (F_\alpha, \tau_\alpha)$. Poniamo

$$F_\infty := \bigcup_{\alpha \in I} F_\alpha$$

e definiamo $\tau_\infty : F_\infty \to L$ imponendo che $\tau_\infty(a) = \tau_\alpha(a)$ se $a \in F_\alpha$. Questa è una buona definizione. Infatti supponiamo che a appartenga anche ad un altro campo F_β. Se $(F_\alpha, \tau_\alpha) \leq (F_\beta, \tau_\beta)$, allora $\tau_\alpha = \tau_{\beta|F_\alpha}$, dunque $\tau_\alpha(a) = \tau_\beta(a)$. Se invece $(F_\beta, \tau_\beta) \leq (F_\alpha, \tau_\alpha)$ si ragiona nello stesso modo. Dunque (F_∞, τ_∞) appartiene ad $\mathfrak{M}$ ed è un maggiorante della catena $\mathfrak{C}$. Abbiamo dimostrato che ogni catena in $\mathfrak{M}$ ha un maggiorante. Per il Lemma di Zorn esiste un elemento massimale (E, τ) di $\mathfrak{M}$. Ora dimostriamo che $E = K'$. Infatti se fosse $E \subsetneq K'$, fissiamo $\alpha \in E - K'$ e consideriamo $F := E(\alpha) \subset K'$. Siccome $\alpha \notin K'$, $E \subsetneq F$. Sia f il polinomio minimo di α su E. Siccome L è algebricamente chiuso, esiste una radice $\beta \in L$ di f^τ. Per il Lemma 101 esiste $\tau' : F \to L$ che estende τ e quindi anche σ. Ma allora (F, τ') sarebbe un elemento di $\mathfrak{M}$ tale che $(E, \tau) \leq (F, \tau')$ e $(E, \tau) \neq (F, \tau')$, contro il fatto che (E, τ) è massimale. Assurdo. Dunque $E = K'$, quindi l'estensione cercata è $(K', \sigma' := \tau)$.
Dimostriamo l'ultima affermazione. Sia $\eta : K' \to L$ una estensione di σ. Allora $\eta(K')$ è un campo isomorfo a K'. Siccome K' è algebricamente chiuso, anche $\eta(K')$ lo è. Siccome $\sigma(K) \subset \eta(K')$, dall'ipotesi che $L/\sigma(K)$ sia una estensione algebrica, segue che anche $L/\eta(K')$ è algebrica. Siccome $\eta(K')$ è algebricamente chiuso, questa estensione è banale, ossia $\eta(K') = L$. Dunque η è un isomorfismo di K' su L. □

Lemma 103. *Se F è un campo finito o numerabile e E/F è una estensione algebrica, allora E è numerabile.*

Dimostrazione. Se F è numerabile, F^n è numerabile e dunque anche $F[X]$, che è unione numerabile si F-spazi vettoriali finito-dimensionali, è numerabile. Ora consideriamo l'applicazione $\varphi : E- \to F[X]$ che associa ad $\alpha \in E-F$

il suo polinomio minimo su F, che indichiamo con m_α. Ovviamente

$$E - F = \bigsqcup_{f \in F[X]} \varphi^{-1}(f).$$

La controimmagine $\varphi^{-1}(f)$ contiene le radici di f in E. Può essere vuota, ma questo non ci disturba. In ogni caso è finita: contiene al massimo $\deg f$ elementi. Dunque $E - F$ è unione numerabile di insiemi finiti. Pertanto è numerabile e il teorema è dimostrato. □

Definizione 104. *Poniamo $\overline{\mathbb{Q}} := \overline{\mathbb{Q}}^{\mathbb{C}}$. Dunque $\overline{\mathbb{Q}}$ è una chiusura algebrica di $\mathbb{Q}$. Gli elementi di $\overline{\mathbb{Q}}$ sono chiamati* numeri algebrici *perché sono algebrici su $\mathbb{Q}$. Gli elementi di $\mathbb{C} - \overline{\mathbb{Q}}$ sono chiamati numeri trascendenti.*

Corollario 105. *$\overline{\mathbb{Q}}$ è numerabile. Esistono numeri trascendenti.*

3.2 Campi di spezzamento

Sia F un campo e sia $f(X) \in F[X]$ un polinomio non costante. Diciamo che f si spezza su una estensione E/F se in $E[X]$ f si scrive come prodotto di fattori lineari:

$$f(X) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

Diciamo che E/F è un *campo di spezzamento* di f su F se f si spezza su E e se f non si spezza su nessun campo intermedio $F \subset E' \subset E$.

È immediato verificare che E è un campo di spezzamento di f se e solo se f si spezza su E ed E è generato dalle radici di f: $E = F(\alpha_1, \ldots, \alpha_n)$. Ovviamente un campo di spezzamento di un polinomio è una estensione finita.

Proposizione 106. *Sia $f(x) \in F[X]$ un polinomio di grado $d \geq 1$. Allora esiste un campo di spezzamento E/F di f con $[E : F] \leq d!$. Se f è irriducibile, allora $d|[E : F]$.*

Dimostrazione. Dimostriamo per induzione su d che l'enunciato vale per qualsiasi campo F. Sia $d = 1$ ed F qualsiasi. Allora $f(X) = X - a$ e $a \in F$, dunque $E = F$ e $[E : F] = 1$, quindi l'enunciato è vero. Sia poi $def f = d > 1$. Sia $f = gh$ con g irriducibile. Per il procedimento di Kronecker esiste una estensione semplice $E_1 = F(\alpha_1)$ dove $g(\alpha_1) = 0$ e $[E_1 : F] = \deg g =: d_1$. Pertanto $g(X) = (X - \alpha_1) \cdot g_1(X)$ in $E_1[X]$. Per induzione esiste un campo di spezzamento E di $g_1 \cdot h$ su E_1 tale che $[E : E_1] \leq (d-1)!$. Siamo

$\alpha_2, \ldots, \alpha_n$ le radici di $g_1 h$. Allora $E = E_1(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$ e $f(X) = (X - \alpha_1) \cdot g_1(X)h(X)$ si spezza su E. Dunque E è un campo di spezzamento di $f(X)$ su F. Infine $[E : F] = [E : E_1] \cdot [E_1 : F] \leq (d-1)!\, d_1 \leq d!$. Supponiamo infine che $f(X)$ sia irriducibile su F. Allora $g = f$ e $d = d_1 = [E_1 : F]$. Dunque $d \mid [E : F]$. □

Esercizio 107. *Sia $\rho = \sqrt[4]{2}$ e $\zeta = e^{2\pi i/3}$. Sia $K = \mathbb{Q}(\rho)$ e $E = (\rho, \zeta)$. Il polinomio minimo di ρ su $\mathbb{Q}$ è $f(X) = X^3 - 2$. Tuttavia K non è il campo di spezzamento di f su $\mathbb{Q}$. Infatti il campo di spezzamento di f su $\mathbb{Q}$ è E e $[E : \mathbb{Q}] = 6$. Infine dimostrare che $E = \mathbb{Q}(i\rho\zeta)$.*

Proposizione 108. *Siano E/F ed E'/F due campi di spezzamento del polinomio $f \in F[X]$. Sia $\overline{E'}$ una chiusura algebrica di E'. Allora per ogni morfismo F-lineare $\eta : E \to \overline{E'}$ si ha $\eta(E) = E'$.*

Dimostrazione. Sia $f(X) = (x - \alpha_1) \cdots (x - \alpha_n)$ lo spezzamento di f su E, e sia $f(X) = (x - \alpha'_1) \cdots (x - \alpha'_n)$ quello su E'. Siccome $\eta_{|F} = \mathrm{id}_F$, si ha $f^\eta = f$, dunque $f(X) = (x - \eta(\alpha_1)) \cdots (x - \eta(\alpha_n))$ è uno spezzamento di f su $\overline{E'}$. Ma $E' \subset \overline{E'}$, quindi abbiamo due spezzamenti di f su $\overline{E'}$ che devono coincidere. Dunque $\{\eta(\alpha_1), \ldots, \eta(\alpha_n)\} = \{\alpha'_1, \ldots, \alpha'_n\}$. Ma allora $E' = F(\alpha'_1, \ldots, \alpha'_n) = \eta(F(\alpha_1, \ldots, \alpha_n)) = \eta(E)$. □

Corollario 109. *Il campo di spezzamento di un polinomio è unico a meno di isomorfismo.*

Dimostrazione. Siano E/F ed E'/F due campi di spezzamento del polinomio $f \in F[X]$. Fissiamo una chiusura algebrica $\overline{E'}$ di E'. Consideriamo il morfismo $\sigma : F \hookrightarrow E' \hookrightarrow \overline{E'}$ ottenuto componendo le inclusioni. Siccome E/F è algebrica e $\overline{E'}$ è algebricamente chiuso, il Teorema 102 assicura che σ si estende a un morfismo $\eta : E \to \overline{E'}$. Per il Lemma precedente $\eta(E) = E'$, dunque η dà un isomorfismo $E \cong E'$. □

Esercizio 110. *Sia E/F una estensione di grado n. Sia $\alpha \in E$. Supponiamo che esistano morfismi F-lineari $\sigma_i : E \to E$ per $i = 1, \ldots, n$, tali che $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ per $i \neq j$ e $\sigma_1 - \mathrm{id}_E$. Allora $E = F(\alpha)$ ed E è il campo di spezzamento di $m_{\alpha,F}$.*

Definizione 111. *Una estensione algebrica E/F è* normale *se ogni polinomio irriducibile a coefficienti in F che ha una radice in E si spezza su E.*

Esercizio 112. *Una estensione algebrica E/F è normale se per ogni $\alpha \in E$ il polinomio minimo $m_{\alpha,F}$ si spezza su E.*

Svolgimento. Sia E/F normale e $\alpha \in E$. Allora $m_{\alpha,F}$ è irriducibile e ha una radice, dunque si spezza. Viceversa, supponiamo che $m_{\alpha,F}$ si spezzi per ogni $\alpha \in E$. Sia $f \in F[X]$ un polinomio irriducibile che ha una radice α in E. Allora $f = c \cdot m_{\alpha,F}$, $c \in F^*$ e $m_{\alpha,F}$ si spezza in $E[X]$. Dunque E/F è normale. □

Teorema 113. *Sia E/F una estensione finita. Le seguenti condizioni sono equivalenti.*

1. *Ogni morfismo F-lineare $E \to \overline{E}$ ha immagine contenuta in E.*
2. *L'estensione E/F è normale.*
3. *E/F è il campo di spezzamento di un polinomio $f \in F[X]$.*

Dimostrazione. $1 \Rightarrow 2$. Sia $f \in F[X]$ e sia $\alpha \in E$ una radice di f. Sia $\beta \in \overline{E}$ un'altra radice di f. Dobbiamo mostrare che $\beta \in E$. Per il Teorema 101 c'è un isomorfismo F-lineare $\sigma : F(\alpha) \to F(\beta)$. Siccome $F(\beta) \subset \overline{E}$ possiamo vedere σ come un morfismo $F(\alpha) \to \overline{E'}$. Visto che E/F è algebrica e $\overline{E'}$ è algebricamente chiuso, possiamo applicare il Teorema 102 e otteniamo che σ si estende ad un morfismo F-lineare $\eta : E \to \overline{E}$. Ma allora $\eta(E) = E$ per la condizione 1. Dunque $F(\beta) \subset \eta(F(\alpha)) \subset \eta(E) = E$. Questo prova che $\beta \in E$, come desiderato.
$2 \Rightarrow 3$. E/F è finita, dunque finitamente generata: $E = F(\alpha_1, \ldots, \alpha_n)$. Sia p_i il polinomio minimo di α_i e $f := p_1 \cdots p_n$. Allora E è il campo di spezzamento di f. Infatti ciascuno dei p_i ha una radice in E e l'estensione E/F è normale. Dunque tutti i p_i si spezzano su E, ossia f si spezza su E. D'altronde E è generato da $\{\alpha_1, \ldots, \alpha_n\}$ che è un sottoinsieme delle radici di f.
$3 \Rightarrow 1$. Se E/F è il campo di spezzamento di un polinomio f, la validità della condizione 1 è assicurata dalla Proposizione 108. □

Esercizio 114. *Sia $K \subset L \subset M$ una catena di campi e sia $\alpha \in M$. Allora $m_{\alpha,L} | m_{\alpha,K}$ in $L[X]$.*

Lemma 115. *Sia $K \subset L \subset M$ una catena di campi. Se M/K è normale, anche M/L lo è.*

Dimostrazione. Per prima cosa osserviamo che se $\alpha \in M$, allora $m_{\alpha,L} | m_{\alpha,K}$ in $L[X]$. Sia ora $f \in L[X]$ irriducibile e sia $f(\alpha) = 0$. Allora $f = c \cdot m_{\alpha,L}$ per una costante $c \in F^*$. Ma allora $f | m_{\alpha,K}$ in $L[X]$. D'altronde $m_{\alpha,K}$ è irriducibile in $K[X]$ e ha una radice in M, dunque si spezza in $K[X]$ e quindi anche in $L[X]$. Siccome f divide $m_{\alpha,K}$ anche f si spezza in $L[X]$. □

3.3 Separabilità

Definizione 116. *Un polinomio a coefficienti in un campo F è* separabile *se non ha radici multiple in nessuna estensione di F.*

Osserviamo che le radici di un polinomio a coefficienti in F stanno sempre in una estensione algebrica di F. Inoltre ogni estensione algebrica di F è contenuta in una chiusura algebrica di F. Infine tutte le chiusure algebriche di F sono isomorfe. Quindi un polinomio a coefficienti in F è separabile se e solo se non ha radici multiple in una chiusura algebrica di F.

Definizione 117. *Sia E/F una estensione algebrica e $\alpha \in E$. Diciamo che α è un* elemento separabile *su F se m_α è un polinomio separabile. Diciamo che E/F è una* estensione separabile *se ogni elemento di E è separabile.*

Lemma 118. *Sia $f(X) \in F[X]$ irriducibile. Se f non è separabile, $f' \equiv 0$.*

Dimostrazione. Le radici multiple di f sono le radici comuni di $f(X)$ e di $f'(X)$. Sia E/F una estensione e sia $\alpha \in E$ una radice multipla. Dunque in $E[X]$ il polinomio $x - \alpha$ divide sia $f(X)$ che $f'(X)$. Indichiamo con $(f, f')_E$ il massimo comun divisore di f e f' in $E[X]$. Dunque $x - \alpha | (f, f')_E$. Ma $(f, f')_E | (f, f')_F$. Quindi anche $(f, f')_F \neq 1$. Ma f è irriducibile. Dunque $(f, f')_F = f$ (a meno di associati). Quindi $f | f'$. Siccome $\deg f' < \deg f$ questo è possibile solo se $f' = 0$. □

Se F è un campo e tutte le estensioni algebriche di E sono separabili, si dice che F è un *campo perfetto.*

Corollario 119. *Se* $\operatorname{car} F = 0$ *ogni polinomio irriducibile a coefficienti in F è separabile e ogni estensione algebrica di F è separabile. Ogni campo di caratteristica 0 è perfetto.*

Teorema 120 (dell'elemento primitivo)**.** *Una estensione E/F finita e separabile è semplice, ossia esiste un elemento $\alpha \in E$ (l'*elemento primitivo*) tale che $E = F(\alpha)$.*

Dimostrazione. Supponiamo inizialmente F finito. Dunque anche E è finito, visto che è uno spazio vettoriale di dimensione finita su F. Ma allora il gruppo moltiplicativo E^* è ciclico, per il Teorema 85. Se $\alpha \in E^*$ è un generatore, allora $E = F(\alpha)$.

Supponiamo ora F infinito e cominciamo dal caso in cui $E = F(\alpha, \beta)$. Vogliamo mostrare che esiste γ tale che $E = F(\gamma)$. Lo cerchiamo nella forma

$\gamma = \alpha + t\beta$, per qualche $t \in F$. Poniamo $F_t := F(\alpha + t\beta)$. Se $\beta \in F_t$, allora anche $\alpha \in F_t$, dunque $F_t = E$ e siamo a posto. Poniamo

$$g := m_{\beta,F}.$$

Ora ragioniamo per assurdo: supponendo che $\beta \notin F_t$ per ogni t, dimostreremo che g non è separabile. Questo contrasta con l'ipotesi che l'estensione sia E/F sia separabile e dunque è assurdo. In questo modo dimostreremo che esiste almeno un $t \in F$ tale che $\beta \in F_t$, dunque $E = F_t$ come desiderato.

Supponiamo quindi $\beta \notin F_t$ per ogni $t \in F$. Poniamo

$$p_t = m_{\beta,F_t}.$$

Siccome $\beta \notin F_t$, $\deg p_t \geq 2$. Inoltre $F \subset F_t \subset E$, quindi $p_t \mid g$ in $F_t[X]$. Fissiamo un campo di spezzamento K di g su E. Allora $p_t \mid g$ anche in $K[X]$. Siccome g ha un numero finito di divisori, c'è (almeno) un sottoinsieme infinito $A \subset F$ tale che p_t è costante per $t \in A$. Indichiamo con p questo polinomio costante, ossia $p_t = p$ per ogni $t \in A$. Chiaramente $d := \deg p \geq 2$. Ora dimostriamo che in $K[X]$ si ha la fattorizzazione

$$p(X) = (X - \beta)^d. \tag{3.1}$$

Siccome p si spezza in $K[X]$, basta dimostrare che β è la sua unica radice in K. Sia dunque $\beta' \in K$ una radice di $p(X)$. Vogliamo mostrare che $\beta' = \beta$. Poniamo

$$f := m_{\alpha,F},$$

e consideriamo il polinomio

$$h_t(X) := f(\alpha + t(\beta - X)) = f(\alpha + t\beta - tX) \in F_t[X].$$

Allora $h_t(\beta) = f(\alpha) = 0$. Dunque $p_t | h_t$ in $F_t[X]$. Pertanto $p | h_t$ in $K[X]$ per ogni $t \in A$. Siccome $p(\beta') = 0$ otteniamo

$$h_t(\beta') = f(\alpha + t(\beta - \beta')) = 0 \quad \text{ per ogni } t \in A.$$

Abbiamo dimostrato che per ogni $t \in A$ l'elemento $\alpha + t(\beta' - \beta)$ è una radice di f. Siccome $f \not\equiv 0$, ci sono solo un numero finito di radici di f. Quindi l'applicazione $K \to K$, $t \mapsto \alpha + t(\beta' - \beta)$ manda l'insieme A, che è infinito, in un insieme finito. In particolare non è iniettiva. Quindi $\beta' = \beta$. ossia β è l'unica radice di p. È così provata la (3.1). Visto che $p | g$ in $K[X]$, segue che g ha una radice multipla in $K[X]$. Quindi g non è separabile, contro

l'ipotesi. Assurdo. Abbiamo dimostrato che se $F(\alpha, \beta)/F$ è separabile, esiste l'elemento primitivo.

Ora veniamo al caso generale, sempre con F infinito. Siccome E/F è finita, $E = F(\alpha_1, \ldots, \alpha_n)$. Se $n = 1$ non c'è niente da dimostrare. Il caso $n = 2$ l'abbiamo appena trattato. Se $n > 2$ procediamo per induzione. Sia $E = F(\alpha_1, \ldots, \alpha_n)$ con $n > 2$. Allora $E = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ e per ipotesi induttiva $F(\alpha_1, \ldots, \alpha_{n-1}) = F(\gamma)$. Dunque $E = F(\gamma)(\alpha_n) = F(\gamma, \alpha_n)$. Riapplicando il caso $n = 2$ otteniamo il risultato. □

Esercizio 121. *1. Sia L un campo, siano $f, g \in L[X]$ e supponiamo $f|g$. Dimostrare che se g è separabile anche f lo è.*

2. Data una catena di campo $K \subset L \subset M$. Dimostrare che se M/K è separabile, anche M/L e L/K lo sono.

3.4 Teoria di Galois

Teorema 122. *Sia E/F una estensione finita e separabile. Allora esistono esattamente $[E : F]$ morfismi F-lineari da E a $\overline{F}$.*

Dimostrazione. Per il Teorema dell'elemento primitivo, possiamo supporre $E = F(\alpha)$. Sia $f = m_\alpha$ e sia $n := \deg f = [E : F]$. Ovviamente f si spezza su $\overline{F}$:

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

e le radici sono tutte distinte perché f è separabile. Per ogni j, si ha $f = m_{\alpha_j, F}$. Quindi c'è un isomorfismo F-lineare $\tau_j : F[X]/(f) \cong F(\alpha_j) \subset \overline{F}$ che manda $X + (f)$ in α_j. Per lo stesso motivo, c'è un isomorfismo F-lineare $\tau : F[X]/(f) \cong F(\alpha)$, che manda α in $X + (f)$. Quindi $\sigma_j := \tau_j \circ \tau^{-1}$ è un isomorfismo F-lineare da $E = F(\alpha)$ a $F(\alpha_j) \subset \overline{F}$ che manda α in α_j. Ed è l'unico morfismo con questa proprietà, perché un morfismo F-lineare è determinato univocamente dal valore che assume su α. Infine ogni possibile morfismo F-lineare da E in $\overline{F}$ manda α in una radice di f, ossia in uno degli elementi α_j e quindi coincide con σ_j. □

Definizione 123. *Se E/F è una estensione finita,* $\mathrm{Gal}(E/F)$ *è l'insieme degli automorfismi di campo F-lineari di E. Questo insieme è ovviamente un gruppo ed è chiamato* gruppo di Galois *dell'estensione E/F.*

Definizione 124. *Una estensione finita E/F è* di Galois *se è normale e separabile.*

Proposizione 125. *Se E/F è finita e normale, allora* $\mathrm{Gal}(E/F)$ *coincide con l'insieme dei morfismi F-lineari $E \to \overline{E}$. Se E/F è di Galois, allora* $|\mathrm{Gal}(E/F)| = [E : F]$.

Dimostrazione. Sia $\sigma : E \to \overline{E}$ un morfismo F-lineare. Siccome E/F è normale e finita, per il Teorema 113, $\sigma(E) \subset E$. Ma $[\sigma(E) : F] = [E : F]$, dunque $\sigma(E) = E$. Quindi $\sigma \in \mathrm{Gal}(E/F)$. Se E/F è anche separabile, il risultato discende dal Teorema 122. □

Definizione 126. *Se $f(X) \in F[X]$, il gruppo di Galois di f, indicato con* $\mathrm{Gal}(f)$ *è il gruppo di Galois del campo di spezzamento di f.*

Esercizio 127. *Sia p primo e $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$. Allora f è irriducibile. Allora $E/\mathbb{Q}$ è normale e separabile e* $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/p$.

Lemma 128. *Se E/F è una estensione, $\alpha \in E$, $f \in F[X]$, $f(\alpha) = 0$ e $\sigma \in \mathrm{Gal}(E/F)$, allora $\sigma(\alpha)$ è una radice di f.*

Dimostrazione. Basta osservare che $\sigma(f(\alpha)) = f^\sigma(\sigma(\alpha)) = f(\sigma(\alpha)) = 0$. □

Lemma 129. *Se $E = F(\alpha_1, \ldots, \alpha_n)$ e $d_i = \deg m_{\alpha_i}$, allora*

$$|\mathrm{Gal}(E/F)| \leq d_1 \cdots d_n.$$

Dimostrazione. Sia $\sigma \in \mathrm{Gal}(E/F)$. Siccome $\alpha_1, \ldots, \alpha_n$ generano E su F, σ è determinato dai valori $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. Applicando il Lemma 128 ad α_i con $f = m_{\alpha_i}$ otteniamo che $\sigma(\alpha_i)$ è una radice di m_{α_i}. Siccome m_{α_i} ha al più d_i radici in E, ho al più d_i possibilità per $\sigma(\alpha_i)$. □

Lemma 130. *Se $f \in F[X]$ e sia E il campo di spezzamento di f su E. Sia $X := \{\alpha_1, \ldots, \alpha_n\}$ l'insieme delle radici di f in E. Allora R è invariante per l'azione di* $\mathrm{Gal}(E/F)$ *su E. Inoltre c'è un morfismo di gruppi iniettivo* $\mathrm{Gal}(E/F) \hookrightarrow S_n$.

Dimostrazione. Sia $\sigma \in \mathrm{Gal}(E/F)$. Se $\alpha \in R$ allora $f(\alpha) = 0$, e anche $f(\sigma(\alpha)) = 0$ per il Lemma 128. Quindi $\sigma(\alpha) \in R$, ossia R è invariante. Dunque l'azione di $\mathrm{Gal}(E/F)$ su E si restringe ad una azione su R cioè a un morfismo $\mathrm{Gal}(E/F) \to S_R \cong S_n$. Questo morfismo è iniettivo perché E è il campo di spezzamento di f, dunque $E = F(R)$ e quindi l'azione di σ su R determina σ. □

Proposizione 131. *1. Per una estensione semplice $E = F(\alpha)/F$, l'ordine del gruppo di Galois* $|\mathrm{Gal}(E/F)|$ *coincide con il numero delle radici di $m_{\alpha,F}$ in E.*

2. *Una estensione finita E/F è di Galois se e solo se* $|\operatorname{Gal}(E/F)| = [E : F]$.

Dimostrazione. (1) Sia $R \subset E$ l'insieme delle radici di $f := m_\alpha$. Allora consideriamo l'applicazione

$$\varphi : \operatorname{Gal}(E/F) \to R, \qquad \sigma \mapsto \sigma(\alpha).$$

Siccome σ è F-lineare, è determinato dal suo comportamento su α, che genera E su F. Dunque φ è iniettiva. Tramite il solito ragionamento (il metodo di Kronecker) vediamo che è suriettiva. Infatti sia $\beta \in R$. Allora f è il polinomio minimo anche di β. Ragioniamo come nel Teorema 122: abbiamo $F(\alpha) \cong F[X]/(f) \cong F(\beta)$, quindi c'è un isomorfismo $\sigma : E = F(\alpha) \to F(\beta) \subset E$. Resta da dimostrare che $F(\beta) = E$ e per farlo ragionaniamo sul grado: dalle inclusioni $F \subset F(\beta) \subset E$ ricaviamo

$$[E : F] = [E : F(\beta)] \cdot [F(\beta) : F]. \tag{3.2}$$

Siccome σ dà un isomorfismo fra le estensioni $F(\alpha)/F$ e $F(\beta)/\beta$, queste hanno lo stesso grado: $[E : F] = [F(\beta) : F]$. Dall'equazione (3.2) segue allora che $[E : F(\beta)] = 1$, ossia $F(\beta) = E$, come desiderato. Dunque $\sigma(E) = E$, per cui $\sigma \in \operatorname{Gal}(E/F)$. Questo dimostra (1). La parte "solo se" in (2) è già nota dalla Proposizione 125. La parte "se": posso supporre $E = F(\alpha)$ e $f = m_\alpha$. Sia $n = [E : F]$. Allora $\deg f = n$ e f ha n radici. Dunque f si spezza su E, per cui E è il campo di spezzamento di f. Inoltre le radici sono tutte distinte, quindi f è separabile, α è separabile e E/F è separabile. □

Si noti che nella dimostrazione della prima parte abbiamo dato un metodo pratico per scrivere tutti gli elementi di una estensione semplice! Infatti se $E = F(\alpha)$, siano $\alpha_1 = \alpha, \ldots, \alpha_r$ le radici di m_α in E. Allora $\operatorname{Gal}(F(\alpha)/F) = \{\sigma_1, \ldots, \sigma_r\}$ dove σ_i è l'isomorfismo che manda α in α_i.

Definizione 132. *Sia E/F una estensione finita e sia G un sottogruppo di* $\operatorname{Gal}(E/F)$. *Allora $E^G := \{\alpha \in E : \gamma(\alpha) = \alpha,$ per ogni $\gamma \in G\}$ è un sottocampo di E e si chiama il* campo fissato *da G.*

Proposizione 133. *Sia E/F una estensione finita. Per ogni sottogruppo $G \subset \operatorname{Gal}(E/F)$, l'estensione E/E^G è di Galois,* $\operatorname{Gal}(E/E^G) = G$ *e* $[E : E^G] = |G|$

Dimostrazione. Incominciamo dimostrando la separabilità di E/E^G (automatica se $\operatorname{car} F = 0$). Sia $\alpha \in E$ un elemento qualsiasi e sia $G \cdot \alpha = \{\alpha_1 = \alpha, \dots, \alpha_r\}$. Poniamo

$$q(X) := (X - \alpha_1) \cdots (X - \alpha_r).$$

Allora

$$q^\gamma(X) = \prod_{i=1}^{r} (X - \gamma(\alpha_i)).$$

Siccome γ agisce sull'orbita $G \cdot \alpha$ permutando gli elementi, i fattori di $q^\gamma(X)$ sono gli stessi di $q(X)$, cambia solo l'ordine. Quindi $q^\gamma(X) = q(X)$ per ogni $\gamma \in G$. Pertanto $q(X) \in E^G[X]$. Inoltre $q(X)$ è separabile per costruzione, visto che ha r radici distinte. Siccome $q(\alpha) = 0$, il polinomio minimo m_{α,E^G} divide $q(X)$, dunque anche m_{α,E^G} è separabile. Dunque α è separabile su E^G. Siccome α è un arbitrario elemento di E, abbiamo dimostrato che l'estensione E/E^G è separabile. Siccome è finita, è anche semplice, quindi $E = E^G(\alpha_0)$ per un certo $\alpha_0 \in E$ fissato. Sia $q_0 \in E^G[X]$ il polinomio costruito come sopra sfruttando l'orbita $G \cdot \alpha_0$. Allora q_0 si spezza su E. Siccome E è generato da α_0 e contiene tutte le radici di q_0, il campo generato su F da queste radici coincide con E. Dunque E/E^G è il campo di spezzamento di q_0, quindi E/E^G è normale. Abbiamo dimostrato che E/E^G è di Galois. Ora dimostriamo che $\operatorname{Gal}(E/E^G) = G$. Una inclusione è immediata: se $\gamma \in G$, γ è un automorfismo di E che fissa ogni elemento di E^G, per definizione di E^G, dunque

$$G \subset \operatorname{Gal}(E/E^G). \tag{3.3}$$

Segue ovviamente che $|G| \leq |\operatorname{Gal}(E/E^G)|$. Dal fatto che $E = E^G(\alpha_0)$ e dal Lemma 129 segue che

$$\begin{aligned} |\operatorname{Gal}(E/E^G)| &\leq \deg m_{\alpha_0,E^G} \leq \deg q_0 = |G \cdot \alpha_0| \\ &\leq |G|. \end{aligned}$$

Quindi $|\operatorname{Gal}(E/E^G)| = |G|$. Ma allora l'inclusione (3.3) deve essere una ugualianza. Infine, per la Proposizione 131 $[E : E^G] = |\operatorname{Gal}(E/E^G)|$, quindi $[E : E^G] = |G|$. □

Teorema 134. *Sia E/F una estensione finita. Allora le seguenti condizioni sono equivalenti:*

1. *E/F è di Galois;*
2. *$|\mathrm{Gal}(E/F)| = [E : F]$;*
3. *$E^{\mathrm{Gal}(E/F)} = F$.*

Dimostrazione. (1) $\Longrightarrow$ (2). Questo lo sappiamo già dall Proposizione 125.
(2) $\Longrightarrow$ (3). Siccome $F \subset E^{\mathrm{Gal}(E/F)} \subset E$, si ha

$$[E : F] = [E : E^{\mathrm{Gal}(E/F)}] \cdot [E^{\mathrm{Gal}(E/F)} : F].$$

Ma per la Proposizione precedente applicata a $G = \mathrm{Gal}(E/F)$

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

Segue che $[E^{\mathrm{Gal}(E/F)} : F] = 1$, cioè $F = E^{\mathrm{Gal}(E/F)}$.
(3) $\Longrightarrow$ (1). Per la Proposizione precedente, $E/F = E/E^{\mathrm{Gal}(E/F)}$ è di Galois. □

Lemma 135. *Se $K \subset L \subset M$ sono estensioni finite e M/K è di Galois, allora anche M/L è di Galois.*

Vedi Lemma 115 e Esercizio 121.

Lemma 136. *Se E/F è di Galois e $\alpha \in E$ e*

$$\mathrm{Gal}(E/F) \cdot \alpha = \{\alpha_1 = \alpha, \ldots, \alpha_r\},$$

allora

$$m_{\alpha,F}(X) = (X - \alpha_1) \cdots (X - \alpha_r).$$

Dimostrazione. Poniamo per semplicità $G := \mathrm{Gal}(E/F)$ e $f(X) = (X - \alpha_1) \cdots (X - \alpha_r)$. Ragionando come nella dimostrazione della Proposizione 133 si vede $f^\gamma = f$ per ogni $\gamma \in G$, dunque f ha coefficienti in $E^G = F$. Siccome $f \in F[X]$ e $f(\alpha) = 0$, $m_\alpha | f$. Se facciamo vedere che i due polinomi hanno lo stesso grado essi coincideranno. Quindi basta dimostrare che $\deg f = \deg m_\alpha = [F(\alpha) : F]$. Sappiamo che $\deg f = r = |G \cdot \alpha| = |G|/|G_\alpha|$, dove G_α è lo stabilizzatore di α in G. Gli elementi di G fissano tutti F puntualmente per definizione. Dunque G_α contiene tutti gli automorfismi di E che fissano puntualmente $F \cup \{\alpha\}$. Pertanto $G_\alpha = \mathrm{Gal}(E/F(\alpha))$. Siccome $E/F(\alpha)$ è di Galois per il Lemma precedente, $|G_\alpha| = [E : F(\alpha)]$. Quindi

$$r = \frac{|G|}{|G_\alpha|} = \frac{[E : F]}{[E : F(\alpha)]} = [F(\alpha) : F].$$

Questo conclude la dimostrazione. □

Veniamo alla corrispondenza di Galois.

Fissiamo una estensione finita E/F. Sia $\mathscr{F}$ l'insieme di tutti i campi intermedi:

$$\mathscr{F} := \{\text{campi } K \text{ tali che } F \subset K \subset E\}.$$

Sia invece $\mathscr{G}$ l'insieme di tutti i sottogruppi di $\mathrm{Gal}(E/F)$. La *corrispondenza di Galois* consiste nelle due funzioni seguenti

$$\sigma : \mathscr{F} \longrightarrow \mathscr{G}, \qquad \sigma(K) := \mathrm{Gal}(E/K),$$
$$\tau : \mathscr{G} \longrightarrow \mathscr{F}, \qquad \tau(G) := E^G.$$

Proposizione 137. *1. Per ogni $K \in \mathscr{F}$ si ha $K \subset \tau\sigma(K) = E^{\mathrm{Gal}(E/K)}$.*

2. Per ogni $G \in \mathscr{G}$ si ha $G = \sigma\tau(G)$. Ossia

$$\sigma\tau = \mathrm{id}_{\mathscr{G}}\,.$$

Dimostrazione. Se $\lambda \in K$ e $\gamma \in \mathrm{Gal}(E/K)$, allora $\gamma(\lambda) = \lambda$ per definizione di $\mathrm{Gal}(E/K)$. Questo dimostra (1). Invece (2) equivale al fatto che $\mathrm{Gal}(E/E^G) = G$, dimostrato nella Proposizione 133. □

Morale: σ è sempre suriettiva e τ è sempre iniettiva.

Esempio $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. In questo esempio σ non è iniettiva e τ non è suriettiva. Il problema è che ci sono pochi automorfismi!

Teorema 138 (fondamentale della teoria di Galois - I parte)**.** *Sia E/F una estensione finita. Allora la corrispondenza di Galois è biunivoca, ossia σ e τ sono biunivoche e sono l'una l'inversa dell'altra se e solo se E/F è di Galois.*

Dimostrazione. Sia E/F di Galois. Basta dimostrare che $\tau\sigma = \mathrm{id}_{\mathscr{F}}$, ossia che per ogni $K \in \mathscr{F}$ si ha $K = E^{\mathrm{Gal}(E/K)}$. Infatti E/K è di Galois per il Lemma 135. Dunque $E^{\mathrm{Gal}(E/K)} = K$ per il Teorema 134. Viceversa, supponiamo σ e τ biunivoche. Allora sono l'una l'inversa dell'altra e in particolare $\tau\sigma = \mathrm{id}_{\mathscr{F}}$. Applicando questa identità a F troviamo $F = \tau\sigma(F) = E^{\mathrm{Gal}(E/F)}$. Di nuovo per il Teorema 134 concludiamo che E/F è di Galois. □

Proposizione 139. *Sia E/F una estensione finita e separabile. Allora esiste una estensione K/E tale che K/F sia di Galois.*

Dimostrazione. Dimostrazione solo nel caso $\operatorname{car} F = 0$. Sia $E = F(\alpha)$ e sia $\overline{E}$ una chiusura algebrica. Sia $f = m_\alpha$. Il polinomio f si spezza su $\overline{E}$: $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$. Possiamo supporre $\alpha = \alpha_1$. Poniamo $K = E(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$. Allora K è il campo di spezzamento di f, dunque K/F è normale e di Galois. E ovviamente $F \subset E \subset K$. □

Domanda: data una estensione di Galois E/F e dato un campo intermedio $F \subset K \subset E$, quando è che K/F è di Galois? Prima di rispondere vediamo il Lemma seguente, che è una generalizzazione della Proposizione 108. La dimostrazione è identica.

Lemma 140. *Sia $\sigma : F \to F'$ un isomorfismo di campi. Sia $f \in F[X]$ e sia E un campo di spezzamento di f. Sia poi E' un campo di spezzamento di f^σ. Allora esiste un morfismo $\bar{\sigma} : E \to E'$ che estende σ.*

Dimostrazione. Sia $\overline{E'}$ una chiusura algebrica di E'. Allora $F' \subset E' \subset \overline{E'}$, dunque posso considerare σ come un morfismo $\sigma : F \to \overline{E'}$. Ora E/F è algebrica e $\overline{E'}$ è algebricamente chiuso. Dunque σ si estende a $\bar{\sigma} : E \to \overline{E'}$ (Teorema 102). Sia ora $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ in E e $f^\sigma(X) = (X - \beta_1) \cdots (X - \beta_n)$ in E'. Allora ho anche $f^\sigma(X) = (X - \bar{\sigma}(\alpha_1)) \cdots (X - \bar{\sigma}(\alpha_n))$ in $\overline{E'}$. Dunque a meno di permutazioni $\beta_j = \bar{\sigma}(\alpha_j)$ e $E' = F(\beta_1, \ldots, \beta_n) = \bar{\sigma}(F(\alpha_1, \ldots, \alpha_n)) = \bar{\sigma}(E)$. Quindi ρ è suriettiva e la dimostrazione è conclusa. □

Teorema 141 (fondamentale della teoria di Galois - II parte)**.** *Sia E/F una estensione di Galois e sia $K \in \mathscr{F}$. Allora K/F è di Galois se e solo se $\operatorname{Gal}(E/K) \lhd \operatorname{Gal}(E/F)$. In tal caso*

$$\operatorname{Gal}(K/F) \cong \frac{\operatorname{Gal}(E/F)}{\operatorname{Gal}(E/K)}.$$

Dimostrazione. K/F è sempre separabile. Quindi dobbiamo dimostrare che K/F è normale se e solo se $\operatorname{Gal}(E/K)$ è normale in $\operatorname{Gal}(E/F)$. (Infatti è per questo motivo che le estensioni normali si chiamano normali.) Cominciamo assumendo $\operatorname{Gal}(E/K) \lhd \operatorname{Gal}(E/F)$ e dimostriamo che allora K/F è normale. Quindi sia $f \in F[X]$ irriducibile e sia $\alpha \in K$ una radice di f. Dobbiamo mostrare che f si spezza su K. Possiamo supporre f monico, quindi $f = m_{\alpha,F}$. Di sicuro f si spezza su E, perché E/F è normale:

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_r),$$

dove $\operatorname{Gal}(E/F) \cdot \alpha = \{\alpha_1 = \alpha, \ldots, \alpha_r\}$, vedi Lemma 136. Dobbiamo mostrare che le radici α_i giacciono in K. Sappiamo che $K = \tau\sigma(K) = E^{\operatorname{Gal}(E/K)}$,

perché E/F è di Galois. Dunque è sufficiente provare che $\gamma(\alpha_i) = \alpha_i$ per ogni $\gamma \in \mathrm{Gal}(E/K)$. Supponiamo che $\alpha_i = \varphi(\alpha)$ per $\varphi \in \mathrm{Gal}(E/F)$ e sia $\gamma \in \mathrm{Gal}(E/K)$. Siccome $\mathrm{Gal}(E/K)$ è normale, $\gamma' := \varphi^{-1}\gamma\varphi \in \mathrm{Gal}(E/K)$. Dunque

$$\gamma(\alpha_i) = \gamma\varphi(\alpha) = \varphi\gamma'(\alpha) = \varphi(\alpha) = \alpha_i.$$

Quindi ogni γ in $\mathrm{Gal}(E/K)$ fissa α_i, come desiderato. Quindi $\alpha_i \in K$ e f si spezza su K. Questo dimostra che K/F è normale e quindi di Galois.

Viceversa, supponiamo che K/F sia normale. Siccome $K \subset E$ è algebrica, posso identificare $\overline{E} = \overline{K}$. Se $\gamma \in \mathrm{Gal}(E/F)$, allora $\gamma_{|K}$ è un morfismo F-lineare $\gamma : K \to E \subset \overline{K}$. Ma allora per il Teorema 113 $\gamma_{|K}(K) \subset K$. Ragionando sul grado delle estensioni otteniamo $\gamma_{|K}(K) = K$. Dunque $\gamma_{|K} \in \mathrm{Gal}(E/K)$. Consideriamo il morfismo

$$\rho : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F), \qquad \rho(\gamma) := \gamma_{|K}.$$

$\ker\rho = \mathrm{Gal}(E/K)$. Infine vogliamo vedere che ρ è suriettiva. Questo dipende dal seguente Lemma. □

3.5 Equazioni polinomiali

Consideriamo l'equazione di secondo grado $x^2 + bx + c = 0$ con i coefficienti b, c che giacciono in un certo campo F. La soluzione è data dalla formula

$$x = \frac{-b \pm \sqrt{\Delta}}{2}$$

dove $\Delta = b^2 - 4c$. Quindi se E/F è una estensione che contiene un elemento α tale che $\alpha^2 = \Delta$, allora le soluzioni sono

$$x_1 = \frac{-b + \alpha}{2}, \qquad x_2 = \frac{-b - \alpha}{2}.$$

Diciamo che l'equazione è risolubile per radicali, perché per esprimere le soluzioni in termini dei coefficienti abbiamo usato solo le usuali operazioni di campo e l'estrazione di radici.

Vogliamo esprimere questo concetto in modo più astratto.

Definizione 142. *Una estensione finita E'/F è una* estensione radicale *se esiste una catena*

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \ldots, \alpha_r) = E'$$

tale che per ogni $i = 1, \ldots, r$ esiste $m_i \in \mathbb{Z}$, $m_i > 0$ tale che $\alpha_i^{m_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$.

Definizione 143. *Una equazione polinomiale $f(X) = 0$ con $f \in F[X]$ è* risolubile per radicali *se il campo di spezzamento di $f(X)$ su F è contenuto in E', dove E'/F è una estensione radicale.*

Nel caso sopra l'estensione radicale è $E' = F(\alpha)$ dove $\alpha^2 = \Delta \in F$, mentre il campo di spezzamento di $f(X) = X^2 + bX + c$ è $F(x_1, x_2) \subset E'$ (in realtà in questo caso $F(x_1, x_2) = E'$).

Consideriamo un altro esempio: il polinomio biquadratico $f(X) = x^4 + 6x^2 - 8$. Qui $f(X) \in \mathbb{Q}[X]$, dunque $F = \mathbb{Q}$. Se $g(Y) = Y^2 + 6Y - 8$, allora $f(X) = g(X^2)$. Le soluzioni di $g(Y) = 0$ sono

$$y_1 = -3 - \sqrt{17}, \qquad y_2 = -3 + \sqrt{17}.$$

Quindi le soluzioni di $f(X) = 0$ sono

$$x_1 = i\sqrt{3 + \sqrt{17}}, \quad x_2 = -i\sqrt{3 + \sqrt{17}}$$
$$x_3 = \sqrt{\sqrt{17} - 3} \quad x_4 = -\sqrt{\sqrt{17} - 3}.$$

Quindi il campo di spezzamento $F(x_1, x_2, x_3, x_4)$ di $f(X)$ è contenuto in $E' = \mathbb{Q}(\sqrt{3 + \sqrt{17}}, \sqrt{\sqrt{17} - 3})$. E l'estensione E'/F è radicale, come possiamo verificare considerando la catena

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{17}) \subset \mathbb{Q}(\sqrt{17}, \sqrt{3 + \sqrt{17}}) \subset$$
$$\subset \mathbb{Q}(\sqrt{17}, \sqrt{3 + \sqrt{17}}, \sqrt{\sqrt{17} - 3}) = E'.$$

Il fatto è che non tutte le equazioni polinomiali si possono risolvere in termini di radicali.

Definizione 144. *Sia F un campo di caratteristica 0 e sia $f(X) \in F[X]$ un polinomio. Sia E il campo di spezzamento di f su F. Il* gruppo di Galois *di f è* $\mathrm{Gal}(E/F)$*. Il gruppo di Galois di f viene indicato con* $\mathrm{Gal}(f)$ *e viene chiamato anche* gruppo di Galois dell'equazione $f(X) = 0$.

Teorema 145. *In caratteristica 0 ogni estensione radicale è contenuta in una estensione radicale e di Galois.*

Teorema 146. *In caratteristica 0 una estensione di Galois E/F è contenuta in una estensione radicale e di Galois (se e) solo se* $\mathrm{Gal}(E/F)$ *è un gruppo risolubile.*

Teorema 147 (Galois)**.** *Sia F un campo di caratteristica nulla. E sia $f(X) \in F[X]$. Allora l'equazione $f(X) = 0$ si può risolvere per radicali (se e) solo se il suo gruppo di Galois è un gruppo risolubile.*

Negli ultimi due teoremi non dimostreremo la parte fra parentesi. Dimostriamo per prima cosa il Teorema di Galois a partire dai Teoremi 145 e 146.

Dimostrazione. Sia E il campo di spezzamento di f. Per ipotesi $E \subset E'$ dove E'/F è radicale. Per il Teorema 145 possiamo supporre che E'/F sia di Galois. Ma allora - per il Teorema 146 - $\mathrm{Gal}(E/F)$ è risolubile. □

Ora restano da dimostrare i Teoremi 145 e 146. Incominciamo con alcune osservazioni sulle estensioni radicali.

Lemma 148. *1. Sia $K \subset L \subset M$ una catena di campi. Se L/K e M/K sono radicali, anche M/K lo è.*

2. Se K'/K è radicale e v è un elemento di una estensione di K', allora anche $K'(v)/K(v)$ è radicale.

3. Se K'/K è radicale e $v_1, \dots v_n$ sono elementi di una estensione di K', allora anche $K'(v_1, \dots, v_n)/K(v_1, \dots, v_n)$ è radicale.

4. Sia $\overline{F}$ una chiusura algebrica di F e siano K ed L sottocampi di $\overline{F}$. Supponiamo che le estensioni K/F e L/F siano radicali e che $L = F(b_1, \dots, b_k)$. Allora $K(b_1, \dots, b_k)/F$ è radicale.

Dimostrazione. (1) Sia $L = K(u_1, \dots, u_s)$ con $u_i^{m_i} \in K(u_1, \dots, u_{i-1})$ e sia $M = L(v_1, \dots, v_t)$ con $v_j^{n_j} \in L(v_1, \dots, v_{j-1})$. Allora ovviamente $L(v_1, \dots, v_{j-1}) = K(u_1, \dots, u_s, v_1, \dots, v_{j-1})$. Dunque basta considerare la catena

$$K \subset K(u_1) \subset \cdots \subset K(u_1, \dots, u_s) = L \subset K(u_1, \dots, u_s, v_1) = L(v_1) \subset \cdots$$
$$\cdots \subset K(u_1, \dots, u_s, v_1, \dots, v_t) = L(v_1, \dots, v_t) = M.$$

(2) Sia $K' = K(u_1, \dots, u_s)$ con $u_i^{m_i} \in K(u_1, \dots, u_{i-1})$. Allora $K'(v) = K(v, u_1, \dots, u_s)$ e ovviamente $u_i^{m_i} \in K(v, u_1, \dots, u_{i-1})$.
(3) segue da (2) iterando.
(4) Poniamo $M := K(b_1, \dots, b_k)$ e consideriamo la catena

$$F \subset K \subset M$$

Siccome K/F è radicale, basta dimostrare che anche M/K è radicale e poi applicare il punto (3). Siccome K/F è finita, $K = F(a_1, \dots, a_m)$. Siccome

L/F è radicale, per il punto (3) anche $L(a_1, \ldots, a_m)/F(a_1, \ldots, a_m)$ è radicale. Ma $L(a_1, \ldots, a_m) = F(b_1, \ldots, b_k, a_1, \ldots, a_m) = F(a_1, \ldots, a_m, b_1, \ldots, b_k) = K(b_1, \ldots, b_k) = M$ e $F(a_1, \ldots, a_m) = K$. Dunque abbiamo dimostrato che M/K è radicale, come desiderato. □

Lemma 149. *Sia $n \in \mathbb{Z}$, $n > 0$. Sia K un campo di carattestica nulla che contiene tutte le n radici n-esime dell'unità. Sia K'/K una estensione finita. Supponiamo che $K' = K(v)$ per $v \in K' - K$ e che $v^n \in K$ per $n \in \mathbb{Z}$. Allora*

1. *K'/K è di Galois;*
2. *$\mathrm{Gal}(K'/K)$ è abeliano.*

Dimostrazione. (1) Sia $\zeta \in K$ una radice n-esima primitiva dell'unità. Poniamo $\gamma := v^m \in K$. Allora il polinomio $q(X) := X^n - \gamma$ è in $K[X]$. Gli elementi $\zeta^i v$ sono radici di q e sono tutti distinti perché $v \neq 0$. Allora q si spezza su K'. Inoltre $K' = K(v)$ per ipotesi, dunque K' è il campo di spezzamento di q su K. In particolare K'/K è di Galois.
(2) Fissiamo una radice n-esima primitiva dell'unità ζ. Dato $\sigma \in \mathrm{Gal}(K'/K)$ consideriamo il quoziente $\sigma(v)/v$. Si vede subito che questo elemento è una radice dell'unità, dunque esiste un unico $[i]_n \in \mathbb{Z}/n$ tale che

$$\frac{\sigma(v)}{v} = \zeta^i.$$

Definiamo $\varphi : \mathrm{Gal}(K'/K) \to \mathbb{Z}/n$ imponendo $\varphi(\sigma) := [i]_n$. Verifichiamo che φ è un morfismo: $\varphi(\sigma) = [i]_n$, $\varphi(\tau) = [j]_n$, allora

$$\sigma(v) = \zeta^i v, \qquad \tau(v) = \zeta^j v$$
$$\sigma\tau(v) = \sigma(\zeta^j v) = \zeta^j \sigma(v) = \zeta^{i+j} v.$$

(Abbiamo usato che σ è K-lineare e $\zeta^j \in K$.) Dunque $\varphi(\sigma\tau) = \varphi(\sigma) + \varphi(\tau)$. Infine φ è iniettivo: se $sig(v) = v$ allora $\sigma = \mathrm{id}_{K'}$ perché $K' = K(v)$. Dunque $\mathrm{Gal}(K'/K)$ è isomorfo a un sottogruppo di $\mathbb{Z}/n$. Quindi è abeliano. □

Sia F un campo di caratteristica nulla e si $n \in \mathbb{Z}$, $n > 0$. Sia E il campo di spezzamento di $f(X) := X^n - 1$ su F. E/F è normale dunque di Galois. Sia R l'insieme delle radici di f in E. La derivata $f' = nX^{n-1}$ non ha radici in comune con f, dunque f è un polinomio separabile. Quindi $|R| = n$. Siccome R è un sottogruppo del gruppo moltiplicativo F^*, R è

ciclico, dunque isomorfo a $\mathbb{Z}/n$. Gli elementi di R si chiamano *radici n-esime dell'unità*. Una radice n-esima dell'unità $\zeta \in R$ è detta *primitiva* se ζ è un generatore del gruppo R. Se ζ è primitiva, $E = F(\zeta)$. Una volta fissata una radice primitiva ζ, otteniamo un isomorfismo

$$\varphi : \mathbb{Z}/n \longrightarrow R, \qquad \varphi([i]_n) = \zeta^i.$$

Tramite questo isomorfismo gli elementi di $(\mathbb{Z}/n)^* = \{[a]_n \in \mathbb{Z}/n : (a, n) = 1\}$ corrispondono alle radici primitive. Dunque il numero delle radici n-esimi primitive dell'unità è $\varphi(n)$. Ricordiamo che $(\mathbb{Z}/n)^*$ è un gruppo - ovviamente abeliano - rispetto al prodotto.

Teorema 150. $\mathrm{Gal}(E/F)$ *è un gruppo abeliano.*

Dimostrazione. Definiamo un'applicazione

$$\psi : \mathrm{Gal}(E/F) \longrightarrow (\mathbb{Z}/n)^*, \qquad \psi(\sigma) := \varphi^{-1}(\sigma(\zeta)).$$

Osserviamo che se ζ è primitiva, anche $\sigma(\zeta)$ lo è perché $\sigma_{|R}$ è un automorfismo del gruppo R. Dunque $\psi(\sigma)$ appartiene effettivamente a $(\mathbb{Z}/n)^*$. Inoltre

$$\psi(\sigma) = [a]_n \iff \sigma(\zeta) = \zeta^a.$$

Sia $\psi(\sigma) = [a]_n$ e $\psi(\tau) = [b]_n$, ossia $\sigma(\zeta) = \zeta^a$, $\psi(\tau) = \zeta^b$. Allora

$$\psi(\sigma\tau) = \varphi^{-1}(\sigma(\tau(\zeta))) = \varphi^{-1}\sigma(\zeta^b) = \varphi^{-1}((\sigma(\zeta)^b) = \varphi^{-1}(\zeta^{ab}) = \\ = [ab]_n = [a]_n \cdot [b]_n = \psi(\sigma)\psi(\tau).$$

Dunque ψ è un morfismo di gruppi. Visto che $E = F(\zeta)$, se $\sigma(\zeta) = \zeta$, allora $\sigma = \mathrm{id}_E$, ossia $\ker \psi = \{\mathrm{id}_E\}$. Dunque ψ è un morfismo iniettivo. Quindi $\mathrm{Gal}(E/F)$ è isomorfo a un sottogruppo di $(\mathbb{Z}/n)^*$, per cui è abeliano. □

Lemma 151. *Sia F un campo di caratteristica 0 e sia $f \in F[X]$ un polinomio irriducibile. Allora* $\mathrm{Gal}(f)$ *agisce transitivamente sulle radici di f.*

Dimostrazione. Siano $\alpha_1, \ldots, \alpha_r$ le radici di f nel suo campo di spezzamento E. Allora $f = m_{\alpha_j}$ per ogni j. Dunque per ogni i, j c'è un isomorfismo F-lineare

$$\sigma : F(\alpha_i) \cong F[X]/(f) \cong F(\alpha_j).$$

Sia $\bar{E}$ una chiusura algebrica di E. Allora posso considerare σ come un morfismo $\sigma : F(\alpha_i) \to \overline{E}$. Posso quindi estenderlo a un morfismo $\bar{\sigma} : E \to \overline{E}$ (Teorem 102). Per normalità (Teorema 113) $\bar{\sigma}(E) \subset E$, anzi $\bar{\sigma}(E) = E$ per grado. Dunque $\bar{\sigma} \in \mathrm{Gal}(E/F)$ scambia due radici qualsiasi. □

Possiamo finalmente passare alla dimostrazione dei due teoremi rimasti.

Dimostrazione del Teorema 145. Sia E/F una estensione radicale. Allora $E = F(\alpha)$. Sia $p = m_\alpha$. Sia E' il campo di spezzamento di p. Allora $E \subset E'$ e E'/F è di Galois. Basta dimostrare che anche E'/F è radicale. Siano $\alpha_1 = \alpha, \ldots, \alpha_n\}$ le radici di p in E'. Allora per ogni j c'è un isomorfismo F-lineare $F(\alpha_j) \cong F(\alpha_1) = E$. Dunque tutte le estensioni $F(\alpha_j)/F$ sono radicali. Consideriamo la catena

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \ldots, \alpha_n) = E'.$$

Vogliamo provare che tutti i passi intermedi sono estensioni radicali. Il punto (1) del Lemma 148 assicurerà che allora anche E'/F è radicale e ciò concluderà la dimostrazione.

La prima estensione, cioè $F \subset F(\alpha_1) = E$ è radicale per ipotesi. Passiamo alla estensione successiva. Sappiamo $F \subset F(\alpha_2)$ è radicale. Per il punto (2) del Lemma 148 anche $F(\alpha_1) \subset F(\alpha_1, \alpha_2)$ è radicale. Quindi passiamo al passo successivo. All'i-esimo passo dobbiamo dimostrare che è radicale l'estensione $F(\alpha_1, \ldots, \alpha_{i-1}) \subset F(\alpha_1, \ldots, \alpha_i)$. Ma sappiamo che $F \subset F(\alpha_i)$ è radicale. Dunque basta applicare il punto (3) del Lemma 148. □

Dimostrazione del Teorema 146. Sia E/F una estensione di Galois e sia E'/F una estensione radicale tale che $E \subset E'$. Per il Teorema 145 possiamo supporre che E'/F oltre che radicale sia anche di Galois. Dunque $E' = F(u_1, \ldots, u_r)$ e $u_i^{m_i} \in F(u_1, \ldots, u_{i-1})$ per $i = 1, \ldots, r$. Inoltre E' sarà il campo di spezzamento di un polinomio $h(X) \in F[X]$. Sia ora $n := m_1 \cdots m_r$ e sia E'' il campo di spezzamento di $X^n - 1$ su F. Infine sia L il campo di spezzamento del polinomio $(X^n - 1)h(X)$. Siano $\alpha_1, \ldots, \alpha_r$ le radici di $X^n - 1$ in L e siano $\beta_1, \ldots, \beta_s$ le radici di h in L. Allora $L = F(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$. Inoltre $F(\alpha_1, \ldots, \alpha_r)$ è un campo di spezzamento di $X^n - 1$ su F, quindi per l'unicità del campo di spezzamento (Corollario 109) $E'' \cong F(\alpha_1, \ldots, \alpha_r)$. Per lo stesso motivo $E' \cong F(\beta_1, \ldots, \beta_s)$. Dunque a meno di passare ad estensioni isomorfe - che non ci dà fastidio - possiamo supporre che

$$E' = F(\beta_1, \ldots, \beta_s), \qquad E'' = F(\alpha_1, \ldots, \alpha_r),$$

e dunque $E', E'' \subset L$. Ora facciamo un altro po' di giochetti per scrivere L in un altro modo: Inoltre

$$L = F(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s) = F(\beta_1, \ldots, \beta_s)(\alpha_1, \ldots, \alpha_r) = \\ = E'(\alpha_1, \ldots, \alpha_r).$$

Ma $E' = F(u_1, \ldots, u_r)$, dunque

$$L = F(u_1, \ldots, u_r)(\alpha_1, \ldots, \alpha_r) = F(\alpha_1, \ldots, \alpha_r)(u_1, \ldots, u_r) = \\ = E''(u_1, \ldots, u_r).$$

L'estensione L/F è di Galois perché L è un campo di spezzamento. Consideriamo la catena

$$F \subset E'' \subset E''(u_1) \subset \cdots \subset E''(u_1, \ldots, u_r) = L.$$

Ciascuno di questi campi è un campo intermedio fra F ed L. Consideriamo la corrispondente successione di sottogruppi. Siccome la corrispondenza di Galois inverte le inclusioni otteniamo

$$G_1 \supset G_0 \supset G_1 \supset \cdots \supset G_r = \{e\},$$

dove

$$G_{-1} = \mathrm{Gal}(L/F), \qquad G_i = \mathrm{Gal}(L/E''(u_1, \ldots, u_i)).$$

Vogliamo dimostrare i due fatti seguenti:

1. $G_{i+1} \lhd G_i$ per $i = -1, \ldots, r-1$.
2. G_{i+1}/G_i è abeliano per $i = -1, \ldots, r-1$.

Da queste due proprietà segue che G_{-1} è un gruppo risolubile. Per il Teorema fondamentale - parte II - visto che L/F è di Galois, la (1) è equivalente al fatto che l'estensione E''/F e tutte le estensioni $E''(u_1, \ldots, u_{i+1})/E''(u_1, \ldots, u_i)$ per $i = 0, \ldots, r-1$ sono di Galois. Infatti E''/F è un campo di spezzamento, dunque è di Galois. Poniamo $K := E''(u_1, \ldots, u_i)$. Allora $E''(u_1, \ldots, u_{i+1}) = K(u_{i+1})$ e $u_{i+1}^{m_{i+1}} \in K$. Inoltre K contiene E'', quindi contiene tutte le radici n-esime dell'unità e quindi anche tutte le radici m_{i+1}-esime dell'unità, visto che $m_{i+1} | n$. Possiamo dunque applicare il Lemma 149 e otteniamo che $K(u_{i+1})/K$ è effettivamente di Galois. Il punto (1) è dimostrato. Sempre per il Teorema fondamentale - parte II - e grazie al fatto che L/F è di Galois - otteniamo che

$$\frac{G_{i+1}}{G_i} = \frac{\mathrm{Gal}(L/E''(u_1, \ldots, u_{i+1}))}{\mathrm{Gal}(L/E''(u_1, \ldots, u_i))} \\ \cong \mathrm{Gal}(E''(u_1, \ldots, u_{i+1}))/E''(u_1, \ldots, u_i)) = \mathrm{Gal}(K(u_{i+1})/K).$$

Di nuovo il Lemma 149 garantische che questo gruppo è abeliano.

È così dimostrato che $\mathrm{Gal}(L/F)$ è risolubile.

Infine, dalla II parte del Teorema fondamentale, applicato questa volta al campo intermedio E fra F ed L, e ricordando che E/F è di Galois, abbiamo

$$\mathrm{Gal}(E/F) \cong \frac{\mathrm{Gal}(L/F)}{\mathrm{Gal}(L/E)}.$$

Dunque c'è un morfismo suriettivo da $\mathrm{Gal}(L/F)$ a $\mathrm{Gal}(E/F)$. Siccome $\mathrm{Gal}(L/F)$ è risolubile, anche $\mathrm{Gal}(E/F)$ è risolubile. Questo conclude la dimostrazione. □

3.6 Campi ciclotomici

Fissiamo $n \in \mathbb{Z}$, $n > 0$. Sia E il campo di spezzamento del polinomio $p(X) = X^n - 1$ su $\mathbb{Q}$. L'estensione $E/\mathbb{Q}$ è di Galois. Possiamo vedere E dentro il campo dei numeri complessi. Sia R_n l'insieme delle radici di p. Gli elementi di R_n si chiamano *radici n-esime dell'unità*. Il polinomio $p(X)$ è separabile, perché la sua derivata $p'(X) = nX^{n-1}$ si annulla solo in $X = 0$ che ovviamente non è soluzione di $p(X) = 0$. Dunque p e p' non hanno radici in comune, ossia p non ha radici multiple, ossia p è separabile. Quindi $|R_n| = n$. Siccome R_n è un sottogruppo finito del moltiplicativo E^*, R_n è un gruppo ciclico. I suoi generatori si chiamano *radici primitive n-esime dell'unità*. Indicheremo con P_n l'insieme delle radici primitive n-esimi dell'unità. Dunque

$$P_n = \{\zeta \in \mathbb{C} : \zeta^k = 1 \Leftrightarrow n|k\}.$$

Un elemento di P_n è $\zeta_n := e^{2\pi i/n}$. Se $\zeta \in P_n$, allora ζ genera R come gruppo ed E come campo. Pertanto si usa generalmente la notazione

$$E = \mathbb{Q}(\zeta_n).$$

Il campo $\mathbb{Q}(\zeta_n)$ viene chiamato *n-esimo campo ciclotomico*.

Se fissiamo $\zeta \in P_n$, l'applicazione

$$\varphi : \mathbb{Z}/n \longrightarrow R_n, \quad \varphi([i]_n) = \zeta^i$$

è un isomorfismo e $\varphi((\mathbb{Z}/n)^*) = P_n$. Quindi $|P_n| = |(\mathbb{Z}/n)^*| = \varphi(n)$. Poniamo

$$\Phi_n(X) := \prod_{\zeta \in P_n} (X - \zeta).$$

Φ_n è l'*n-esimo polinomio ciclotomico*.

Lemma 152. *1. Φ_n è monico di grado $\varphi(n)$.*

2.

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

3. $\Phi_n(X) \in \mathbb{Z}[X]$.

Dimostrazione. (1) è evidente.
(2) Nel campo E il polinomio $p(X)$ si spezza in fattori lineari:

$$p(x) = \prod_{\zeta \in R_n} (X - \zeta).$$

D'altro canto R_n è un gruppo ciclico di ordine n, dunque

$$R_n = \bigsqcup_{d|n} R_{n,d}.$$

dove $R_{n,d} := \{\zeta \in R_n : o(\zeta) = d\}$. Ma in realtà $R_{n,d} = P_d$. Quindi

$$p(x) = \prod_{\zeta \in R_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in P_d} (X - \zeta) = \prod_{d|n} \Phi_d.$$

(3) Procediamo per induzione. $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Supponiamo $\Phi_d(X) \in \mathbb{Z}[X]$ per $d < n$. Da (2) segue che

$$X^n - 1 = \prod_{\substack{d|n \\ d<n}} \Phi_d(X) \cdot \Phi_n(X).$$

Ma $X^n - 1 \in \mathbb{Z}[X]$, quindi dal lemma di Gauss segue che $\Phi_n(X) \in \mathbb{Z}[X]$. □

Prima di procedere dobbiamo introdurre un oggetto fondamentale negli anelli di caratteristica p.

Sia A un anello (commutativo) di caratteristica p. Il *morfismo di Frobenius* è la seguente applicazione:

$$F : A \longrightarrow A, \qquad F(x) := x^p.$$

Lemma 153. *Se A ha caratteristica p, allora F è un morfismo di anelli.*

Dimostrazione. Chiaramente $F(xy) = F(x) \cdot F(y)$ perché A è commutativo. La cosa interessante è che $F(x+y) = F(x) + F(y)$. Infatti per il binomio di Newton

$$F(x+y) = F(x) + F(y) + \sum_{0<k<p} \binom{p}{k} x^k y^{p-k}.$$

Se $0 < k < p$, allora

$$s := \binom{p}{k} = \frac{p!}{k!)p-k)!}, \qquad k!s = \frac{p!}{(p-k)!}.$$

Siccome $k > 0$, p divide il secondo membro dell'equazione a destra. Siccome $k < p$, p non divide $k!$. Dunque $p|s$. Ma allora

$$\sum_{0<k<p} \binom{p}{k} x^k y^{p-k} = 0$$

in A. □

Ci interessa il morfismo di Frobenius nel caso $A = \mathbf{F}_p = \mathbb{Z}/p$ (il campo con p elementi) e nel caso $A = \mathbf{F}_p[X]$. Se $a \in \mathbf{F}_p$, allora $a^p = a$ (piccolo Teorema di Fermat). Quindi su $\mathbf{F}_p$ il morfismo di Frobenius è l'identità.

Lemma 154. *Sia $f(X) \in \mathbf{F}_p[X]$. Allora $f(X^p) = (f(X))^p$.*

Dimostrazione. Sia $F : \mathbf{F}_p[X] \to \mathbf{F}_p[X]$ il morfismo di Frobenius. Dobbiamo dimostrare che $F(f(X)) = f(X^p)$. Sia $f(X) = \sum_{i=0}^n a_i X^i$. Sfruttando il fatto che F è un morfismo di anelli otteniamo

$$F(f) = F\left(\sum_{i=0}^n a_i X^i\right) = \sum_{i=0}^n F(a_i) F(X^i).$$

Siccome $a_i \in \mathbf{F}_p$, $F(a_i) = a_i$. Dunque

$$F(f) = \sum_{i=0}^n a_i X^{pi} = f(X^p),$$

come desiderato. □

Teorema 155 (Gauss)**.** *$\Phi_n(X)$ è irriducibile.*

Dimostrazione. Per prima cosa vogliamo dimostrare che

$$\text{se } \zeta \in P_n,\ p \text{ è un primo e } p \nmid n, \text{ allora } m_{\zeta,\mathbb{Q}}(\zeta^p) = 0. \qquad (*)$$

Scriviamo per semplicità $f := m_{\zeta,\mathbb{Q}}$ e supponiamo per assurdo che $f(\zeta^p) \neq 0$. Siccome $\zeta^p \in R_n$, $p(\zeta^p) = 0$, dunque

$$X^n - 1 = p(X) = f(x)g(X) \qquad (3.4)$$

per un certo polinomio $g(X) \in \mathbb{Z}[X]$ (lemma di Gauss!). Se $f(\zeta^p) \neq 0$, allora $g(\zeta^p) = 0$. Quindi il polinomio $g(X^p)$ si annulla in $X = \zeta$, dunque $f|g(X^p)$ ossia esiste $h(X)$ tale che $g(X^p) = f(X)h(X)$ e $h(X) \in \mathbb{Z}[X]$ (lemma di Gauss!). Riduciamo modulo p: $\bar{g}(X^p) = \bar{f}(X)\bar{h}(X)$. Sfruttando il Lemma precedente otteniamo $\bar{g}(X^p) = (\bar{g}(X))^p$, dunque

$$(\bar{g}(X))^p = \bar{f}(X)\bar{h}(X).$$

Fissiamo una chiusura algebrica $\overline{\mathbf{F}}_p$ e sia $\alpha \in \overline{\mathbf{F}}_p$ una radice di $\bar{f}$. Allora anche $\bar{g}(\alpha) = 0$ per la relazione sopra. Dunque per (3.4) α è una radice doppia del polinomio $\bar{p}(X)$. Quindi è una radice comune a $\bar{p}$ e $\bar{p}'$. Ma $\bar{p}' = nX^{n-1}$ si annulla solo per $X = 0$, perché $p \nmid n$. Mentre $p(0) = -1 \neq 0$. Assurdo! Abbiamo dimostrato $(*)$.
Ora iteriamo: per $(*)$ se $\zeta \in P_n$, p è primo e $p \nmid n$, allora $m_\zeta(\zeta^p) = 0$. Dunque $m_{\zeta^p} = m_\zeta$. Di nuovo per $(*)$ abbiamo $0 = m_{\zeta^p}((\zeta^p)^p)) = m_\zeta(\zeta^{p^2})$. Dunque $m_\zeta = m_{\zeta^{p^2}}$. Iterando ulteriormente troviamo

$$\zeta \in P_n,\ p \text{ primo}, p \nmid n \Longrightarrow m_\zeta(\zeta^{p^a}) = 0 \text{ e } m_\zeta = m_{\zeta^{p^a}} \text{ per ogni } a. \qquad (**)$$

Sia ora q un altro primo che non divide n e $b \in \mathbb{Z}, b > 0$. Poniamo $\xi := \zeta^{p^a}$. Dunque $\xi \in P_n$ perché $(p^a, n) + 1$. Per $(**)$ $m_\zeta = m_\xi$. Quindi

$$m_\zeta(\zeta^{p^a q^b}) = m_\xi(\xi^{q^b}).$$

Applicando di nuovo $(**)$ a ξ, q e b otteniamo che $m_\xi(\xi^{q^b}) = 0$ e dunque che

$$m_\zeta = m_{\zeta^{p^a q^b}}, \qquad m_\zeta(\zeta^{p^a q^b}) = 0.$$

Se invece di p e q abbiamo $p_1, \ldots, p_s$, primi che non dividono n, iterando in modo simile otteniamo finalmente che $m_\zeta(\zeta^{p_1^{a_1} \cdots p_s^{a_s}}) = 0$. Ma se k è un intero positivo primo con n allora k è della forma $k = p_1^{a_1} \cdots p_s^{a_s}$. Quindi abbiamo dimostrato che fissata $\zeta \in P_n$, se $(k, n) = 1$, allora $m_\zeta(\zeta^k) = 0$. Dunque m_ζ si annulla su ogni elemento di P_n. Quindi $\Phi_n | m_\zeta$. Viceversa, siccome $\Phi_n \in \mathbb{Q}[X]$ e $\varphi_n(\zeta) = 0$, allora $m_\zeta | \Phi_n$. Otteniamo che $\Phi_n = m_\zeta$ (sono entrambi monici) e quindi Φ_n è irriducibile.

□

Corollario 156. *L'estensione $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è di Galois, di grado $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$ e $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^*$.*

Dimostrazione. La prima affermazione discende dal fatto che $\mathbb{Q}(\zeta_n)$ è il campo di spezzamento del polinomio $X^n - 1$. La seconda discende dal fatto che il polinomio minimo di ζ_n su $\mathbb{Q}$ è Φ_n che ha grado $\varphi(n)$. Per verificare la terza affermazione fissiamo una qualsiasi radice primitiva ζ e consideriamo l'applicazione

$$\psi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n)^*,$$

definita in questo modo: dato $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, sia $\sigma(\zeta) = \zeta^i$. Allora poniamo

$$\psi(\sigma) := [i]_n.$$

Siccome ζ è primitiva e σ è un automorfismo, anche $\sigma(\zeta)$ è primitiva, dunque $(i, n) = 1$. L'applicazione ψ è un morfismo di gruppi, perché se $\psi(\sigma) = [i]_n$ e $\psi(\tau) = [j]_n$, allora $\tau(\zeta) = \zeta^j$, dunque

$$\sigma\tau(\zeta) = \sigma(\zeta^j) = (\sigma(\zeta))^j = (\zeta^i)^j = \zeta^{ij}.$$

Dunque $\psi(\sigma\tau) = [ij]_n = \psi(\sigma)\psi(\tau)$. Inoltre ψ è iniettiva: se $\sigma \in \ker\psi$, allora $\sigma(\zeta) = \zeta$, dunque $\sigma = \mathrm{id}_{\mathbb{Q}(\zeta_n)}$. Siccome $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è di Galois, $|\operatorname{Gal}\mathbb{Q}(\zeta_n)/\mathbb{Q}| = \varphi(n) = |(\mathbb{Z}/n)^*|$. Dunque ψ è un isomorfismo.

□

3.7 Discriminante

Sia $f \in F[X]$ un polinomio. Fissiamo un campo di spezzamento E di f e siano $\alpha_1, \ldots, \alpha_n$ le radici di f. Poniamo

$$\delta = \prod_{i<j}(\alpha_i - \alpha_j), \qquad \Delta := \delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

δ è definito a meno del segno ed appartiene a E. Invece Δ è ben definito e appartiene a F. Si chiama *discriminante* di f. Si dimostra che $\mathrm{Gal}(f) \subset A_n$ se e solo se Δ è un quadrato in F se e solo se $\delta \in F$ e δ è ben definito (anche col segno).

Nel caso di un polinomio cubico f questo significa che $\mathrm{Gal}(f) = \mathbb{Z}/3$ se Δ è un quadrato in F e $\mathrm{Gal}(f) = S_3$ se Δ non è un quadrato in F.

Questo è di qualche utilità solo se è possibile calcolare Δ senza conoscere le radici. Infatti per una cubica senza termine quadratico $f = X^3 + aX + b$ si ha

$$\Delta = -4a^3 - 27b^3.$$

3.8 Polinomi non risolubili per radicali

Lemma 157. *1. Le permutazioni* (12) *e* $(12\dots n)$ *generano* S_n.

2. Se p *è primo, un* p*-ciclo e una trasposizione qualsiasi generano* S_p.

Dimostrazione. (1) Poniamo $\tau = (1,2), \sigma = (1,2,3,\dots,n)$. Allora $\sigma^a \tau \sigma^{-a} = (a, a+1)$. Inoltre

$$(2,3)(1,2)(2,3) = (1,3)$$
$$(3,4)(1,3)(3,4) = (1,4)$$

ecc. Dunque coniugando troviamo tutte le trasposizioni del tipo $(1, 1+s)$. Coniugando un opportuno elemento di $\langle\sigma\rangle$ troviamo $(a, a+s)$, ossia tutte le trasposizioni, che generano S_n.
(2) Sia σ un p-ciclo e sia τ una trasposizione. A meno di rinumerare gli elementi (che corrisponde a coniugare con una elemento di S_p), possiamo supporre $\tau = (1,2)$. Il gruppo $\langle\sigma\rangle$ agisce transitivamente su $\{1,2,\dots,p\}$. Dunque esiste i tale che $\sigma^i(1) = 2$. Siccome p è primo, σ^i ha ordine p, dunque è un p-ciclo: $\sigma^i = (1,2,\varphi_3,\dots,\varphi_p)$. Poniamo $\varphi_1 = 1, \varphi_2 = 2$. Coniugando con φ ci riportiamo alla situazione $\tau = (1,2), \sigma = (1,2,3,\dots,p)$. A questo punto l'enunciato segue dal punto (1). □

Se n non è primo il punto (2) in generale è falso. Per esempio sia $n = 4$, $\sigma = (1324)$ e $\tau = (12)$. Allora $\tau\sigma\tau = (1423) = \sigma^3$. Quindi $\langle\sigma,\tau\rangle$ è un sottogruppo isomorfo a D_4.

Lemma 158. *Sia* p *un numero primo e sia* $G \subset S_p$ *un sottogruppo* transitivo*, cioè che agisce transitivamente su* $\{1,\dots,p\}$*. Allora* G *contiene un* p*-ciclo.*

Dimostrazione. Se $X = \{1,\dots,p\}$, allora X è una G-orbita: $X = G \cdot x$. Dunque

$$|X| = |G \cdot x| = \frac{|G|}{|G_x|} \Longrightarrow o(G) = |X| \cdot |G_x| = p \cdot |G_x|.$$

Dunque $p|o(G)$. Invece $p^2 \nmid o(G)$. Altrimenti da $G \subset S_p$, seguirebbe $p^2|o(S_p) = p!$, da cui $p|(p-1)!$ che è assurdo, visto che p è primo. Sia dunque $H \subset G$ un p-Sylow. Quindi $o(H) = p$. Quindi H è ciclico, generato da $\sigma \in H$ e $o(\sigma) = p$, dunque σ è un p-ciclo. □

Ricordiamo senza dimostrazione i seguenti fatti.

Proposizione 159.

$$[A_n, A_n] = \begin{cases} 1 & \text{se } n = 2, 3 \\ V_4 & \text{se } n = 4 \\ A_n & \text{se } n \geq 5. \end{cases}$$

(Qui V_4 indica il sottogruppo $B_4 \cup \{1\}$.) In particolare A_n è risolubile se e solo se $n \leq 4$. Inoltre $[S_n, S_n] = A_n$ per $n \geq 2$.

Corollario 160. *S_n non è risolubile se $n \geq 5$.*

Teorema 161. *Sia $f \in \mathbb{Q}[X]$ un polinomio irriducibile di grado p con $p \geq 5$ primo. Se f ha esattamente $p-2$ radici reali, allora* $\mathrm{Gal}(f) = S_p$ *ed f non è risolubile per radicali*

Dimostrazione. Sia E il campo di spezzamento di f su $\mathbb{Q}$. Siccome f è irriducibile, f è separabile, dunque ha p radici distinte. E si ottiene da $\mathbb{Q}$ aggiungendo le p radici di f. Siccome f è irriducibile, $G := \mathrm{Gal}(f)$ è transitivo sulle radici. Dunque $G \subset S_p$ è transitivo. Per il Lemma 158 G contiene un p-ciclo. Inoltre $\mathrm{Gal}(f)$ contiene il coniugio che fissa tutte le radici reali e scambia le due uniche radici complesse. Dunque il coniugio agisce come una trasposizione sulle p radici di f. Per il Lemma 157 $G = S_p$. Siccome S_p non è risolubile, f non è risolubile per radicali. □

Esercizio 162. *Il polinomio $f = X^5 - 4X + 2$ non è risolubile per radicali.*

Svolgimento. Basta fare lo studio di funzione di $f(x)$ e vedere che ha esattamente 3 zeri.

$$f' = 5x^4 - 4 = 5(x^2 + \sqrt{4/5})(x - \sqrt[4]{4/5})(x + \sqrt[4]{4/5}),$$
$$f' > 0 \iff x < -\sqrt[4]{4/5} \text{ oppure } x > \sqrt[4]{4/5},$$
$$f(-\sqrt[4]{4/5}) > 0, \qquad f(\sqrt[4]{4/5}) < 0.$$

Quindi f ha esattamente uno zero per $x < -\sqrt[4]{4/5}$, esattamente uno zero fra $-\sqrt[4]{4/5}$ e $\sqrt[4]{4/5}$, esattamente uno zero per $x > \sqrt[4]{4/5}$. In totale 3 zeri. □