

# Algebra I

ANDREA GALLESE

12 GENNAIO 2018

## Indice

|  |           |
|--|-----------|
| <b>G Teoria dei Gruppi</b>                                       | <b>2</b>  |
| G.1 Automorfismi e Azioni . . . . .                              | 2         |
| G.2 Formula delle Classi e Cauchy . . . . .                      | 3         |
| G.3 Gruppi Diedrali $D_n$ . . . . .                              | 5         |
| G.4 Gruppi di Permutazioni $S_n$ . . . . .                       | 6         |
| G.5 Prodotti diretti . . . . .                                   | 8         |
| G.6 Classificazione dei Gruppi di ordine 8 . . . . .             | 9         |
| G.7 Prodotto Semidiretto . . . . .                               | 10        |
| G.7.1 Classificazione dei gruppi di ordine $pq$ . . . . .        | 10        |
| G.8 Teorema di Sylow . . . . .                                   | 11        |
| G.8.1 Classificazione dei gruppi di ordine 12 . . . . .          | 12        |
| G.9 Automorfismi di un gruppo buffo . . . . .                    | 13        |
| G.10 Teorema Fondamentale dei Gruppi Abelianici Finiti . . . . . | 14        |
| G.10.1 Classificazione dei Gruppi di Ordine 30 . . . . .         | 14        |
| G.11 Lemmi vari ed esercizi sparsi . . . . .                     | 15        |
| <b>A Anelli</b>  | <b>16</b> |
| A.1 Prime definizioni . . . . .                                  | 16        |
| A.1.1 Anelli di polinomi . . . . .                               | 16        |
| A.2 Ideali . . . . .   | 17        |
| A.2.1 Prodotto diretto tra anelli . . . . .                      | 18        |
| A.2.2 Estensione e Contrazione di Ideali . . . . .               | 18        |
| A.2.3 Fatti sul radicale . . . . .                               | 19        |
| A.3 Domini . . . . .   | 20        |
| A.3.1 Campo dei quozienti. $\mathbb{Q}(A)$ . . . . .             | 20        |
| A.3.2 Divisibilità. . . . .                                      | 20        |
| A.4 Domini Speciali . . . . .                                    | 21        |
| A.4.1 Dominio Euclideo . . . . .                                 | 21        |
| A.4.2 Dominio a Ideali Principali . . . . .                      | 21        |
| A.4.3 Dominio a Fattorizzazione Unica . . . . .                  | 21        |
| <b>K Teoria dei Campi e di Galois</b>                            | <b>24</b> |
| K.1 Richiami . . . . .   | 24        |
| K.2 Separabilità . . . . .                                       | 26        |
| K.3 Normalità . . . . .  | 27        |
| K.4 Teoria di Galois . . . . .                                   | 28        |
| K.5 Relazioni tra estensioni e gruppi di Galois . . . . .        | 30        |
| K.5.1 Gruppo di Galois di un ciclotomico . . . . .               | 31        |
| K.5.2 Gruppo di Galois di un campo finito . . . . .              | 31        |
| K.6 Esistenza e unicità della chiusura algebrica . . . . .       | 32        |

Per tutto quello che riguarda gli interi di Gauss, rifarsi a **kconrad**.

## G Teoria dei Gruppi

### G.1 Automorfismi e Azioni

**Teorema G.1.** Se  $G$  è un gruppo,  $(\text{Aut}(G), \circ)$  è un gruppo.

**Esempi.**

1.  $\text{Aut}(\mathbb{Z}) \cong \{\pm id\} \cong \mathbb{Z}_2$
2.  $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$
3.  $\text{Aut}(\mathbb{Q}) \cong \mathbb{Q}^\times$
4.  $\text{Aut}(\mathbb{R}) \cong ?$

**Definizione** (automorfismi interni). Chiamiamo

$$\text{Int}(G) = \{\varphi_g \mid g \in G\}$$

l'insieme di tutti gli automorfismi interni, i.e. degli automorfismi di coniugio:

$$\varphi_g(x) = gxg^{-1} \quad \forall x \in G$$

è immediato osservare che  $\text{Int}(G) \triangleleft \text{Aut}(G)$ .

**Lemma G.2** (degli Automorfismi Interni).

$$\text{Int}(G) \cong G/Z(G)$$

*Dimostrazione.* La funzione

$$\Phi: G \rightarrow \text{Int}(G)$$

$$g \mapsto \varphi_g$$

è un omomorfismo con kernel  $Z(G)$ . La tesi segue dal Primo Teorema di Omomorfismo. ♣

*Osservazione.*

$$H \triangleleft G \Leftrightarrow \varphi_g(H) = H \quad \forall \varphi_g \in \text{Int}(G)$$

**Definizione** (Sottogruppo caratteristico). Un sottogruppo  $H < G$  si dice *caratteristico* se è fissato da tutto  $\text{Aut}(G)$ , i.e.

$$\varphi(H) = H \quad \forall \varphi \in \text{Aut}(G)$$

*Osservazione.* Un sottogruppo caratteristico è anche normale, ma non è sempre vero il viceversa:  $\langle(0, 1)\rangle \triangleleft \mathbb{Z}_2 \times \mathbb{Z}_2$ .

**Definizione** (Azione). Si dice azione di un gruppo  $G$  su un insieme  $X$  un omomorfismo  $\varphi$  tale che

$$\begin{aligned} \varphi: G &\rightarrow \mathcal{S}(X) \\ g &\mapsto \varphi_g(x) = g \cdot x. \end{aligned}$$

**Esempio.** Siano  $G = C = \{z \in \mathbb{C} \mid |z| = 1\}$ ,  $X = \mathbb{R}^2$  e sia  $\varphi$  l'azione:

$$\begin{aligned} \varphi: C &\rightarrow \mathcal{S}(\mathbb{R}^2) \\ z &\mapsto \mathcal{R}(O, \arg z) \end{aligned}$$

*Osservazione.* Un'azione induce naturalmente una relazione di equivalenza su  $X$ :  $x \sim y \Leftrightarrow \exists g \in G$  t.c.  $g \cdot x = y$ . Viene quindi spontaneo prendere in considerazione gli elementi della partizione così ottenuta.

**Definizione** (Orbita). Si dice *orbita* di un elemento  $x \in X$  l'insieme di tutti gli elementi che posso essere raggiunti da  $x$  tramite l'azione:

$$\text{Orb}(x) = \{g \cdot x \mid \forall g \in G\}$$

*Osservazione.* Detto  $R$  un insieme di rappresentanti delle varie orbite, visto che queste formano una partizione:

$$X = \bigcup_{x \in R} \text{Orb}(x) \quad \Rightarrow \quad |X| = \sum_{x \in R} |\text{Orb}(x)|$$

**Definizione** (Stabilizzatore). Si dice *stabilizzatore* di un elemento  $x \in X$  l'insieme di tutti gli elementi di  $G$  che agiscono in modo banale su  $x$ :

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

*Osservazione.* Lo stabilizzatore è un sottogruppo

$$\text{Stab}(x) < G$$

ma non è necessariamente normale.

$$Z_{\mathcal{A}_5}(1 \ 2 \ 3) < \mathcal{A}_5$$

**Lemma G.3** (Relazione Orbita-Stabilizzatori).

$$|G| = |\text{Orb}(x)| |\text{Stab}(x)|$$

*Dimostrazione.* La funzione  $f$  così definita

$$\begin{aligned} f: \{g\text{Stab}(x) \mid g \in G\} &\rightarrow \{\text{Orb}(x) \mid x \in X\} \\ g\text{Stab}(x) &\mapsto g \cdot x \end{aligned}$$

è biunivoca, infatti:

$$\begin{aligned} g \cdot x = h \cdot x &\Leftrightarrow \varphi_g(x) = \varphi_h(x) \\ &\Leftrightarrow \varphi_h^{-1} \varphi_g(x) = x \\ &\Leftrightarrow \varphi_{h^{-1}g}(x) = x \\ &\Leftrightarrow h^{-1}g \cdot x = x \\ &\Leftrightarrow h^{-1}g \in \text{Stab}(x) \\ &\Leftrightarrow g \in h\text{Stab}(x) \\ &\Leftrightarrow g\text{Stab}(x) = h\text{Stab}(x) \end{aligned}$$

♣

*Osservazione.* Dall'osservazione precedente

$$|X| = \sum_{x \in R} \frac{|G|}{|\text{Stab}(x)|}$$

**Esempi.**

1.  $[G = C, X = \mathbb{R}^2]$  e l'azione dell'ultimo esempio. Questa ruota ogni punto attorno all'origine, pertanto le orbite sono circonferenze centrate nell'origine e gli stabilizzatori sono tutti banali, tranne quello dell'origine che coincide con  $G$ .
2.  $[G = \mathbb{R}, X = \mathbb{R}^2]$  e l'azione che trasforma  $r \in \mathbb{R}$  nella traslazione orizzontale di lunghezza  $r$ . Le orbite sono le rette parallele alla traslazione e gli stabilizzatori sono tutti banali.
3.  $[G, X = G]$  e l'azione sia la mappa che manda un elemento  $g$  nel coniugio per questo  $\varphi_g(x) = gxg^{-1}$ . L'orbita di un elemento contiene tutti i coniugati di questo ed è detta *classe di coniugio* di  $x$  ( $\mathcal{C}_x$ ). Lo stabilizzatore di  $x$  contiene tutti e soli gli elementi tali che  $xg = gx$ , ovvero il sottogruppo di tutti gli elementi che commutano con  $x$ , è detto *centralizzatore* di  $x$  ( $Z_G(x)$ ).
4.  $[G, X = \{H \mid H < G\}]$  e l'azione di coniugio. Le orbite non sono particolarmente interessanti, mentre lo stabilizzatore di un sottogruppo è detto *Normalizzatore* di  $H$ ,  $N(H)$  ed è il più grande sottogruppo di  $G$  in cui  $H$  è normale.

*Osservazione.*  $H \triangleleft G \Leftrightarrow N(H) = G$

*Osservazione* (euristica). Le azioni più comuni sono quelle naturali: il coniugio, la moltiplicazione a sinistra e, talvolta, la moltiplicazione a destra per l'inverso.

## G.2 Formula delle Classi e Cauchy

**Teorema G.4** (Formula delle Classi). *In ogni gruppo finito*

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

*Dimostrazione.* Osserviamo cosa succede nel caso dell'azione di coniugio di  $G$  in sè (l'esempio 3 di sopra): riprendiamo la partizione di  $X$  in orbite, ma separando quelle banali da quelle non

$$|X| = \sum_{\substack{x \in R \\ \text{Orb}(x) = \{x\}}} 1 + \sum_{\substack{x \in R \\ \text{Orb}(x) \neq \{x\}}} \frac{|G|}{|\text{Stab}(x)|}$$

L'orbita di  $x$  è banale se e solo se  $gxg^{-1} = x$ ,  $\forall g \in G$ , ovvero solo nel caso in cui  $x$  commuta con tutti gli elementi di  $G$  o, meglio, quando vive nel centro di  $G$ . ♣

**Definizione** ( $p$ -gruppo). Dato un primo  $p \in \mathbb{N}$ , si dice  $p$ -gruppo un gruppo finito  $G$  di ordine potenza di  $p$ :  $|G| = p^n$ .

**Proprietà.**

1. **Un  $p$ -gruppo  $G$  ha centro non banale.** Tutti i centralizzatori degli elementi di  $R'$  hanno dimensione  $p^k$  per un intero  $0 \leq k < n$ , dunque

$$p \mid \frac{|G|}{|Z_G(x)|} \forall x \in R'$$

pertanto, per la formula delle classi,

$$p \mid |G| - \sum_{x \in R'} \frac{|G|}{|Z_G(x)|} = |Z(G)|$$

che quindi, contenendo  $e$ , deve avere almeno  $p$  elementi.

2. **I gruppi di ordine  $p^2$  sono abeliani.** Il centro di  $G$  avrà, per quanto appena dimostrato, ordine  $p$  o  $p^2$ . Nel secondo caso abbiamo finito. Nel primo

$$|G/Z(G)| = p$$

dunque il quoziente è ciclico. Possiamo appellarci al seguente lemma:

**Lemma G.5.** *Se il quoziente tra un gruppo e il suo centro è ciclico, allora il gruppo è abeliano.*

Presi due elementi qualunque  $x, y \in G$  possiamo esprimerli come  $x = g^h a$  e  $y = g^k b$ , dove  $g$  è il generatore del quoziente e  $a, b \in Z(G)$ . Allora, sfruttando la commutatività degli elementi del centro

$$xy = (g^h a)(g^k b) = g^{h+k} ab = g^{k+h} ba = (g^k b)(g^h a) = yx$$

ricaviamo la commutativa per tutti gli elementi del gruppo.

3. Una possibile dimostrazione del Teorema di Cauchy:

**Teorema G.6** (di Cauchy). *Per ogni fattore primo  $p$  di  $|G|$  esiste un elemento  $g$  di  $G$  di ordine  $p$ .*

*Dimostrazione Classica.* Sia  $|G| = pn$ , procediamo per induzione su  $n$ .

Se  $n = 1$ ,  $G$  è ciclico, quindi ha un generatore di ordine  $p$ .

Supponiamo ora che tutti i gruppi di ordine  $kp \ \forall k < m$  abbiano un elemento di ordine  $p$ . Se  $|G| = pm$  ci sono due casi:

1. Esiste un sottogruppo proprio  $H$  di ordine multiplo di  $p$ , da cui ricadiamo nell'ipotesi induttiva.
2. Nessun sottogruppo di  $G$  ha ordine divisibile per  $p$ , allora

$$p \mid \frac{|G|}{|Z_G(x)|} \forall x \in R'$$

perché i  $Z_G(x) < G$ . Per la formula delle classi

$$p \mid |G| - \sum_{x \in R'} \frac{|G|}{|Z_G(x)|} = |Z(G)|$$

ma abbiamo supposto che i sottogruppi propri non abbiano ordine multiplo di  $p$ , dunque il centro deve coincidere con l'intero gruppo, che risulta pertanto commutativo. ♣

*Dimostrazione Magica.* Sia

$$X = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_p = 1\}$$

questo insieme ha esattamente  $|G|^{p-1}$  elementi, infatti scelti i primi  $p-1$  l'ultimo dev'essere il suo unico inverso. Facciamo agire  $\mathbb{Z}_p$  su  $X$ , in modo da ciclare le  $p$ -uple, e osserviamo che ogni stabilizzatore può essere banale, nel caso di  $p$  elementi ripetuti, o tutto il gruppo. Osserviamo che ci interessa contare il numero di stabilizzatori banali! Detto  $n$  il numero di  $g$  tali che  $g^p = 1$

$$p \mid |G|^{p-1} - n \Rightarrow p \mid n$$

e poiché  $e^p = e$  ci sono almeno  $p-1$  elementi di ordine  $p$ . ♣

**Esercizio.** Classificare i gruppi  $G$  di ordine 6.

**Definizione** (Sottogruppo generato). Sia  $S \subset G$  un sottoinsieme di  $G$ . Chiamiamo  $\langle S \rangle$  il più piccolo sottogruppo contenente  $S$ , sottogruppo generato da  $S$ .

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

**Lemma G.7** (Caratterizzazione dei sottogruppi generati).

$$\langle S \rangle = \{s_1 \cdots s_k \mid k \in \mathbb{N}, s_i \in S \cup S^{-1}\}$$

*Dimostrazione.* È sufficiente osservare che tutti gli elementi di  $S$  devono comparire in tutti i gruppi che contengono  $S$  e che l'insieme proposto è un sottoinsieme chiuso per le operazioni di gruppo, pertanto è un sottogruppo. ♣

**Proprietà.**

1.  $\langle S \rangle$  è abeliano se e solo se tutti gli elementi di  $S$  commutano fra loro.
2.  $\langle S \rangle$  è normale se e solo se ogni elemento di  $S$  rimane in  $\langle S \rangle$  per coniugio.
3.  $\langle S \rangle$  è caratteristico se e solo se ogni elemento di  $S$  viene mandato in  $\langle S \rangle$  da ogni automorfismo di  $G$ .
4.  $G' = \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle$  è detto *Gruppo dei Commutatori* o *Gruppo Derviato* di  $G$ . Questo gruppo gode di alcune proprietà fondamentali

(a)  $G' = \{e\} \Leftrightarrow G$  abeliano.

(b)  $G'$  è caratteristico e pertanto normale in  $G$ .

(c) **Dato**  $H \triangleleft G$ , **il quoziente**  $G/H$  **è abeliano se e solo se**  $G' < H$ .

*Dimostrazione.* La verifica delle proprietà (a) e (b) è banale. Rimane l'ultima (c):

$$\begin{aligned} G/H \text{ abeliano} &\Leftrightarrow xHyH = yHxH && \forall x, y \in G \\ &\Leftrightarrow xyH = yxH && \forall x, y \in G \\ &\Leftrightarrow x^{-1}y^{-1}xy \in H && \forall x, y \in G \\ &\Leftrightarrow g' \in H && \forall g' \in G' \end{aligned}$$



**Definizione.**  $G/G'$  è detto l'abelianizzato di  $G$ , perché è sempre abeliano!

### G.3 Gruppi Diedrali $D_n$

**Definizione** (Gruppo Diedrale). Sia  $D_n$  il gruppo delle isometrie dell' $n$ -agono regolare.

**Teorema G.8** (Caratterizzazione di  $D_n$ ). Si ha

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

*Dimostrazione.* Tutti gli elementi sopra definiti possiamo ridurre a un elemento della forma  $\rho^k$  o  $\sigma\rho^k$  per un qualche  $0 \leq k < n$ . Questo perché così sono fatti i generatori e ogni operazione permessa (composizione e inversione) tra due generatori può immediatamente essere ridotta a questa forma attraverso le cancellazioni imposte. Inoltre possiamo immergere  $D_n$  in un sottogruppo di  $\mathbf{O}_2(\mathbb{R})$  di ordine  $2n$  attraverso un omomorfismo suriettivo:

$$\begin{aligned} \Phi: D_n &\rightarrow \mathbf{O}_2(\mathbb{R}) \\ \sigma &\mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ \rho &\mapsto \begin{pmatrix} \cos \frac{2\pi}{n} & \sin \frac{2\pi}{n} \\ -\sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix} \end{aligned}$$

Pertanto ognuno dei rappresentati sopra individua un'effettiva trasformazione distinta. ♣

*Osservazione.* Conosciamo già un gruppo diedrale:  $D_3 \cong S_3$ .

*Osservazione.* Il sottogruppo  $C_n$  delle rotazioni, generato da  $\rho$ , è ovviamente ciclico e, avendo indice 2, è anche normale in  $D_n$ .

$$\langle \rho \rangle = C_n \triangleleft D_n$$

**Lemma G.9** (Ordine degli elementi di  $D_n$ ). Sappiamo che

- tutte le simmetrie hanno ordine 2.
- ci sono  $\varphi(m)$  rotazioni di ordine  $m$ , per ogni  $m \mid n$ .

*Dimostrazione.* La seconda parte è immediata conseguenza della ciclicità del sottogruppo delle rotazioni. L'ordine delle riflessioni possiamo calcolarlo esplicitamente notando che  $(\sigma\rho^k)(\sigma\rho^k) = (\sigma\rho^k\sigma)\rho^k = \rho^{-k}\rho^k = e$  grazie alla terza proprietà imposta nella caratterizzazione. ♣

**Lemma G.10** (Sottogruppi di  $D_n$ ). I sottogruppi  $H < D_n$  rientrano in una di queste due categorie:

- $H < C_n$ : di cui ne abbiamo esattamente uno per ogni ordine divisore di  $n$ .
- $H = (H \cap C_n) \sqcup \tau(H \cap C_n)$ : di cui ce ne sono  $d$  di ordine  $\frac{2n}{d}$  per ogni  $d \mid n$ .

*Dimostrazione.* Se  $H < C_n$  il risultato viene da Aritmetica. Se  $H \not< C_n$ ,  $H$  contiene almeno una rotazione  $\tau = \sigma\rho^i$ . Consideriamo l'omomorfismo  $f$  che fa commutare il diagramma

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

Restringiamo l'omomorfismo trovato ad  $H$

$$\begin{array}{ccc} D_n & \xrightarrow{\Phi} & \mathbf{O}_2(\mathbb{R}) \\ \uparrow & \searrow f & \downarrow \det \\ H & \dashrightarrow & \mathbb{Z}_2 \end{array}$$

Visto che  $\ker f = C_n \triangleleft D_n$ , il sottogruppo  $H$  viene scomposto in nucleo e laterale

$$H = f^{-1}(0) \sqcup f^{-1}(1) = (H \cap C_n) \sqcup \tau(H \cap C_n)$$

Infine, dato che il nucleo è contenuto nel sottogruppo ciclico  $(H \cap C_n) < C_n$ , possiamo pensarlo come il sottogruppo generato da una potenza della rotazione elementare

$$H \cap C_n = \langle \rho^d : d \mid n \rangle$$

Il suo unico laterale sarà allora composto dagli  $d$  elementi della forma

$$\begin{aligned} \tau(H \cap C_n) &= \{\tau\rho^d, \tau\rho^{2d}, \dots, \tau\rho^{n-d}\} \\ &= \{\sigma\rho^{d+i}, \sigma\rho^{2d+i}, \dots, \sigma\rho^{n-d+i}\} \end{aligned}$$

che è facile convincersi dipendere solamente dalla classe di  $i$  mod  $d$ . ♣

**Esercizi.**

1. Quali sottogruppi di  $D_n$  sono normali?
2. Quali sottogruppi di  $D_n$  sono caratteristici?
3. Quali sono i quozienti di  $D_n$ ?
4. (\*) Chi è  $\text{Aut}(D_n)$ ?

## G.4 Gruppi di Permutazioni $\mathcal{S}_n$

**Definizione** (Gruppi di Permutazioni). Dato un insieme  $X$ , chiamiamo

$$\mathcal{S}(X) = \{f : X \rightarrow X \mid f \text{ è bigettiva}\}$$

con l'operazione di composizione, il gruppo delle permutazioni di  $X$ . Se l'insieme è finito  $|X| = n$ , allora

$$\mathcal{S}(X) \cong \mathcal{S}(\{1, 2, \dots, n\})$$

lo chiamiamo  $\mathcal{S}_n$ .

**Teorema G.11** (Cayley). Possiamo immergere ogni gruppo  $G$  finito in un gruppo di permutazioni, in  $\mathcal{S}(G)$ .

*Dimostrazione.* L'azione di moltiplicazione a sinistra è fedele

$$\begin{aligned} \Phi: G &\rightarrow \mathcal{S}(G) \\ g &\mapsto \varphi_g(x) = gx \end{aligned}$$

ovvero, iniettiva. ♣

**Lemma G.12.** Ogni permutazione  $\sigma \in \mathcal{S}_n$  si scrive in modo unico come prodotto di cicli disgiunti.

*Osservazione.* Cicli disgiunti commutano.

*Osservazione.*  $\mathcal{S}_n$  è generato dai suoi cicli.

**Lemma G.13** (delle permutazioni coniugate). Due permutazioni  $\sigma, \tau \in \mathcal{S}_n$  sono coniugate se e solo se hanno lo stesso tipo di decomposizione in cicli.

*Dimostrazione.* E' più che sufficiente osservare che dato un ciclo

$$\sigma = (a_1 \dots a_k)$$

e una permutazione tale che  $\tau : a_i \mapsto b_i$  si ha

$$\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_k)) = (b_1 \dots b_k)$$

♣

*Osservazione.*  $\mathcal{S}_n$  è generato dalle sue trasposizioni.

*Osservazione.* La decomposizione in trasposizioni non è unica. Ma la parità del numeri di trasposizioni lo è:

**Teorema G.14** (delle trasposizioni). La parità del numero di trasposizioni della scomposizione di una qualunque permutazione  $\sigma \in \mathcal{S}_n$  non dipende dalla scomposizione.

*Dimostrazione.* Consideriamo

$$\begin{aligned} \text{sgn} : \mathcal{S}_n &\rightarrow \mathbb{Z}^\times = \{\pm 1\} \\ \sigma &\mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

questo è un omomorfismo di gruppi. Infatti:

1. è ben definito, ovvero  $|\text{sgn}(\sigma)| = 1$ : tutte le differenze che compaiono a denominatore compaiono anche a numeratore, poiché  $\sigma$  è una permutazione, magari con ordine o segno, differente.
2. Si comporta bene con la composizione

$$\begin{aligned} \text{sgn}(\sigma \circ \tau) &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} \\ &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j} \\ &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \prod_{i < j} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \text{sgn}(\sigma) \cdot \text{sgn}(\tau) \end{aligned}$$

Per concludere, osserviamo che tutte le trasposizioni hanno segno negativo. ♣

**Definizione** (Gruppo Alterno). Chiamiamo  $\mathcal{A}_n$  o *gruppo alterno* il sottogruppo delle permutazioni pari

$$\ker(\text{sgn}) = \mathcal{A}_n \triangleleft \mathcal{S}_n$$

*Osservazione.* Ogni sottogruppo  $H < \mathcal{S}_n$  è contenuto interamente in  $\mathcal{A}_n$  o viene spezzato a metà dal gruppo alterno. Questo perché possiamo restringere il determinante al solo  $H$ , che dunque può spezzarsi in nucleo e laterale, o immergersi interamente nel nucleo.

**Lemma G.15** (si spezzamento). La classe di coniugio di  $\sigma$  in  $\mathcal{S}_n$  si spezza in  $\mathcal{A}_n$  se e solo se  $\sigma$  è composto da cicli di lunghezze dispari e distinte.

*Osservazione.*  $\mathcal{A}_n$  è generato dai suoi 3-cicli.

*Osservazione.* Tutti i 3-cicli sono coniugati in  $\mathcal{A}_n$ .

**Teorema G.16.** Il gruppo alterno  $\mathcal{A}_n$  è semplice per  $n \geq 5$ .

*Dimostrazione.* Iniziamo a dimostrare che  $\mathcal{A}_5$  è semplice. Le classi di coniugio di questo gruppo hanno dimensione

$$1, 12, 12, 15, 20$$

Un sottogruppo normale dovrebbe essere unione di un certo numero di queste orbite, ma sommando le loro cardinalità non ottengo mai divisori di 60. Allo stesso modo,  $\mathcal{A}_6$  è semplice: le sue classi coniugio hanno dimensione

$$1, 40, 40, 45, 72, 72, 90$$

Dimostriamo ora la tesi per  $n \geq 7$ . Supponiamo che esista un sottogruppo normale

$$\{e\} \neq N \triangleleft \mathcal{A}_n$$

e mostriamo che contiene un 3-ciclo. Non essendo banale, prendiamo una permutazione non identica  $\sigma$ , che possiamo supporre, senza perdita di generalità, non fissare l'1:

$$\sigma(1) \neq 1$$

e  $\tau = (i \ j \ k)$  una permutazione di tre indici diversi da 1 tali che  $\sigma(1) \in \{i, j, k\}$ . Nell'operare questa scelta, abbiamo bisogno che il gruppo contenga almeno 4 elementi! Inoltre

$$\tau\sigma\tau^{-1}(1) = \tau(\sigma(1)) \neq \sigma(1)$$

dunque  $\tau\sigma\tau^{-1} \neq \sigma$  e siamo sicuri che la permutazione

$$\phi = \tau\sigma\tau^{-1}\sigma^{-1}$$

non sia l'identità. Inoltre questa è sia il prodotto tra un coniugato di un elemento nel nostro sottogruppo normale per il suo inverso

$$\phi = (\tau\sigma\tau^{-1})\sigma^{-1} \in N$$

che prodotto di un 3-ciclo e di un suo coniugato

$$\phi = \tau(\sigma\tau^{-1}\sigma^{-1})$$

quindi permuta al più 6 numeri. Aggiungiamo, se necessario, numeri a caso fino ad averne esattamente 6 e chiamiamo  $H$  il sottogruppo di  $\mathcal{A}_n$  che li permuta. Abbiamo mostrato che

$$\phi \in N \cap H$$

dunque l'intersezione è non vuota, ma essendo  $H \cong A_6$  semplice, questo, non potendosi spezzare, vive interamente nell'intersezione:

$$H < N$$

$A_6$  contiene tutti i 3-cicli di cui abbiamo bisogno! ♣

**Teorema G.17** (del ribelle). *Per ogni  $n \geq 3$  i gruppi di permutazioni sono i propri automorfismi*

$$\text{Aut}(\mathcal{S}_n) \cong \mathcal{S}_n$$

ma non per  $\mathcal{S}_6$ , che è un ribelle.

*Dimostrazione.* Per cominciare, osserviamo che

$$\text{Int}(\mathcal{S}_n) \cong \mathcal{S}_n / Z(\mathcal{S}_n) \cong \mathcal{S}_n$$

dunque  $\mathcal{S}_n \triangleleft \text{Aut}(\mathcal{S}_n)$ , pertanto ci basta dimostrare che tutti gli automorfismi sono interni. Sfruttiamo il fatto che gli automorfismi mandano classi di coniugio in classi di coniugio e che preservano l'ordine degli elementi per mostrare che

- Ogni automorfismo rispetta la classe delle trasposizioni. Guardiamo come sono fatte le classi di coniugio degli elementi di ordine 2. Sia  $C_k$  la classe delle permutazioni composte da  $k$  trasposizioni disgiunte, abbiamo che

$$|C_k| = \frac{1}{2^k \cdot k!} \cdot \frac{n!}{(n-2k)!}$$

Imporre  $|C_1| = |C_k|$ , equivale a risolvere

$$2^{k-1} = \frac{(n-2)!}{(n-k)!} \binom{n-k}{k}$$

- Per  $\boxed{k=2}$  abbiamo

$$4 = (n-2)(n-3)$$

che non ha soluzione, perché i due fattori a destra sono interi consecutivi, quindi uno di loro sarà dispari.

- Per  $\boxed{k=3}$  abbiamo

$$4 = (n-2) \binom{n-3}{3}$$

che ammette  $n=6$  come unica soluzione (il caso famigerato!), visto che  $n-2 \mid 4$  limita la ricerca delle soluzioni ai soli  $n=3, 4, 6$ .

- Infine, per  $\boxed{k>3}$  notiamo che il fattore

$$\frac{(n-2)!}{(n-k)!}$$

contiene almeno un primo dispari.

Pertanto ogni automorfismo rispetta  $C_1$ , perché le altre classi sono troppo grandi.

- Osserviamo che, preso  $\varphi \in \text{Aut}(\mathcal{S}_n)$ , si ha

$$\varphi(1, i) = (a_1, a_i)$$

con tutti gli  $a_i$  distinti.

- Dunque  $\varphi$  coincide, in realtà, con il coniugio per la permutazione

$$\sigma : i \mapsto a_i$$



## Esercizi.

1. Quanti  $k$ -cicli ci sono in  $\mathcal{S}_n$ ?
2. Come conto gli elementi con una composizione fissata in un  $\mathcal{S}_n$  dato? Per esempio, come calcolo le permutazioni del tipo  $3+3+2+2+2$  in  $\mathcal{S}_{10}$ ?
3. L'ordine di  $\sigma$  è il minimo comune multiplo delle lunghezze dei suoi  $k$ -cicli.
4. Notiamo che il centralizzatore di  $\sigma$  coincide con lo stabilizzatore dell'azione di coniugio di  $\mathcal{S}_n$  in se. Dunque

$$|Z(\sigma)| = \frac{n!}{|C(\sigma)|}$$

5. Data una permutazione  $\sigma$  trovare  $|N(\langle \sigma \rangle)|$ .

Osserviamo che

$$N(\langle \sigma \rangle) = \{\tau \mid \tau \sigma \tau^{-1} = \sigma^k\}$$

dunque il normalizzatore contiene il centralizzatore di  $\sigma$  e, visto che il coniugio preserva la scomposizione in cicli, che possiamo prendere solo i  $k$  coprime coll'ordine di  $\sigma$ . Inoltre prese due permutazioni  $\tau_1, \tau_2 \in N(\langle \sigma \rangle)$  che generano lo stesso  $\sigma^k$ , abbiamo che

$$\tau_1 \sigma \tau_1^{-1} = \tau_2 \sigma \tau_2^{-1} \Leftrightarrow (\tau_2^{-1} \tau_1) \sigma (\tau_2^{-1} \tau_1)^{-1} = \sigma$$

Dunque  $\tau_2^{-1} \tau_1 \in Z(\sigma)$ , ovvero  $\tau_1 \in \tau_2 Z(\sigma)$ . Pertanto il normalizzatore dev'essere composto da tutti i laterali del centralizzatore indotti da permutazioni che mi danno  $\sigma^k$  dello stesso tipo di  $\sigma$ . Ovvero

$$N(\langle \sigma \rangle) = \bigcup_{(i, \text{ord}(\sigma))=1} \tau_i Z(\sigma)$$

e pertanto

$$|N(\langle \sigma \rangle)| = |Z(\sigma)| \cdot \phi(\text{ord}(\sigma))$$

## G.5 Prodotti diretti

**Teorema G.18** (di Struttura). *Sia  $G$  un gruppo e  $H, K < G$  due sottogruppi. Se*

1.  $H \triangleleft G$  e  $K \triangleleft G$
2.  $HK = G$
3.  $H \cap K = \{e\}$

allora

$$G \cong H \times K$$

*Dimostrazione.* Mostriamo innanzitutto che  $hkh^{-1}k^{-1}$  appartiene ad entrambi i sottogruppi, infatti:

$$H \ni h(kh^{-1}k^{-1}) = h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1} \in K$$

dunque, per la seconda ipotesi,

$$hkh^{-1}k^{-1} = e$$

quindi gli elementi di un sottogruppo commutano con quelli dell'altro  $hk = kh$ .

Consideriamo ora l'isomorfismo

$$\begin{aligned} \Phi: H \times K &\rightarrow G \\ (h, g) &\mapsto hg \end{aligned}$$

e verifichiamo che

1. è ben definito.
2. è un omomorfismo: infatti

$$\Phi(hh', kk') = hh'kk' = hkh'k' = \Phi(h, k)\Phi(h', k')$$

3. è suriettivo; ed è, sostanzialmente, l'ipotesi 2.
4. è iniettivo per l'ipotesi 3; infatti

$$\ker \Phi = \{(h, k) \mid hk = e\} = \{(e, e)\}$$

perché se  $h$  e  $k$  sono inversi, vivono nello stesso gruppo, dunque nell'intersezione, che non ci lascia molta libertà di scelta.



*Osservazione.* Nel prodotto diretto i fattori commutano.

**Proprietà di  $G = H \times K$ .**

1.  $Z(G) = Z(H) \times Z(K)$ .
2.  $\text{Int}(G) \cong \text{Int}(H) \times \text{Int}(K)$ .
3.  $\text{Aut}(H) \times \text{Aut}(K) < \text{Aut}(G)$ .

**Teorema G.19** (degli automorfismi prodotto). *Si ha*

$$\text{Aut}(H) \times \text{Aut}(K) < \text{Aut}(H \times K)$$

*e sono isomorfi se e solo se  $H$  e  $K$  sono caratteristici.*

*Dimostrazione.* Consideriamo la mappa

$$\begin{aligned} \Phi: \text{Aut}(H) \times \text{Aut}(K) &\rightarrow \text{Aut}(H \times K) \\ (f, g) &\mapsto \varphi_{fg}: (h, k) \mapsto (f(h), g(k)) \end{aligned}$$

e verifichiamo che

- è bene definita, ovvero  $\varphi$  è un automorfismo. Immediata conseguenza del fatto che  $f$  e  $g$  sono a loro volta automorfismi.

- è un omomorfismo.

$$\begin{aligned} \Phi(ff', gg') &= (f(f'(h)), g(g'(k))) \\ &= (\varphi_{fg} \circ \varphi_{f'g'})(h, k) \\ &= \Phi(f, g)\Phi(f', g') \end{aligned}$$

- è iniettiva.

$$\ker \Phi = \{(id, id)\}$$

perché restringendo l'identità non possiamo certo sperare di permutare qualcosa.

- è suriettiva se e solo se  $H \times \{e_K\}$  e  $\{e_H\} \times K$  sono caratteristici in  $H \times K$ .

⇒. Se  $\Phi$  è suriettivo, allora tutti gli automorfismi di  $H \times K$  sono della forma di cui sopra e pertanto  $\varphi_{fg}$  agisce sugli elementi di  $H$  come  $\varphi_{fg|H} = f \in \text{Aut}(H)$ .

⇐. Viceversa, supponiamo  $H$  e  $K$  caratteristici, preso un automorfismo  $\varphi \in \text{Aut}(H \times K)$  consideriamo le sue restrizioni ai due sottogruppi caratteristici.

$$f = \Pi_H(\varphi|_{H \times \{e_K\}}) \quad g = \Pi_K(\varphi|_{\{e_H\} \times K})$$

Notiamo che  $f \in \text{Aut}(H)$ .

- $f$  è iniettiva. Se  $f(h) = f(h')$  allora

$$\Pi_H(\varphi(h, e_K)) = \Pi_H(\varphi(h', e_K))$$

poiché  $H \times \{e_K\}$  è caratteristico

$$\varphi(h, e_K) = (a, e_K) \quad \varphi(h', e_K) = (b, e_K)$$

ma necessariamente  $a = f(h)$  e  $b = f(h')$ , pertanto

$$\varphi(a, e_K) = (f(h), e_K) = (f(h'), e_K) = \varphi(b, e_K)$$

e, visto che  $\varphi$  è iniettivo,  $h = h'$ .

- $f$  è suriettiva. Fissiamo un qualunque  $h \in H$ . Essendo  $H \times \{e_K\}$  caratteristico, necessariamente la controimmagine di  $(h, e_K)$  è un suo elemento

$$\varphi^{-1}(h, e_K) = (h', e_K)$$

dunque

$$f(h') = \Pi_H(\varphi(h', e_K)) = \Pi_H(h, e_K) = h$$

Infine osserviamo che  $\Phi(f, g) = \varphi$ . Infatti

$$\begin{aligned} \varphi_{fg}(h, k) &= (f(h), g(k)) \\ &= (\Pi_H(\varphi(h, e_K)), \Pi_K(\varphi(e_H, k))) \\ &= (\Pi_H(\varphi(h, k)), \Pi_K(\varphi(h, k))) \\ &= \varphi(h, k) \end{aligned}$$

dove la terza uguaglianza segue da

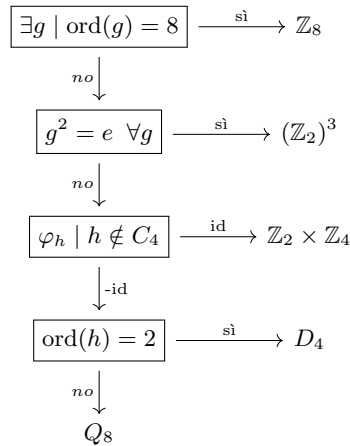
$$\begin{aligned} \Pi_H(\varphi(h, e_K)) &= \Pi_H(\varphi(h, e_K)) \Pi_H(\varphi(e_H, k)) \\ &= \Pi_H(\varphi(h, e_K)\varphi(e_H, k)) \\ &= \Pi_H(\varphi(h, k)) \end{aligned}$$



**Esercizio.** Trovare  $\text{Aut}(\mathbb{Z}_{20} \times \mathbb{Z}_2)$ .



## G.6 Classificazione dei Gruppi di ordine 8



Prendiamo un gruppo  $G$  di ordine 8.

- Se esiste un elemento di ordine 8 il gruppo è ciclico e pertanto isomorfo a  $\mathbb{Z}_8$ .
- Se  $G$  ha solo elementi di ordine 2, allora è isomorfo a  $(\mathbb{Z}_2)^3$ . Mostriamo un risultato appena più generale.

**Teorema G.20** (dei gruppi solipsisti). *Se  $|G|$  ha solo elementi di ordine due ed è finito, allora  $G \cong (\mathbb{Z}_2)^n$ .*

*Dimostrazione.* Osserviamo che

$$a^2b^2 = e = (ab)^2 = abab$$

e, moltiplicando per  $a$  a sinistra e per  $b$  a destra, otteniamo

$$ab = ba \text{ per ogni } a, b \in G$$

Pertanto  $G$  è abeliano. Possiamo ora procedere per induzione sulla dimensione di  $G$ . Se  $|G| = 2$  il risultato è chiaro. Supponiamo ora che sia vero per tutti i gruppi di ordine  $< 2^n$  e supponiamo  $2^n \leq |G| < 2^{n+1}$ . Quando prendiamo un insieme minimale di  $h < n$  generatori  $\langle g_1, \dots, g_h \rangle$  di un sottogruppo di  $H < G$ , questo sarà isomorfo a  $(\mathbb{Z}_2)^h$  per ipotesi induttiva. Prendiamo un elemento  $g \notin H$ , abbiamo che  $H$  e  $\langle g \rangle \cong \mathbb{Z}_2$  sono sottoinsiemi normali e con intersezione banale, pertanto il sottoinsieme

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

per il teorema di struttura G.18. Così facendo possiamo continuare ad aggiungere elementi fino alla saturazione. ♣

Se  $G$  non ha elementi di ordine 8 e non hanno tutti ordine 2, allora esiste un  $g \in G$  di ordine 4 e sia  $C_4 = \langle g \rangle$ . Sia  $h \notin C_4$

e consideriamo l'azione di coniugio di  $h$  su  $C_4$

$$\begin{aligned}
 \varphi_g: C_4 &\rightarrow C_4 \\
 x &\mapsto h x h^{-1}
 \end{aligned}$$

ben definita perché  $C_4$ , avendo indice 2, è normale in  $G$ . Poiché  $\text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$ , abbiamo solo due possibilità:

$$\varphi_g = id^{\pm 1}$$

- $[\varphi_g = id, \text{ord}(h) = 2]$ . Dunque gli elementi di  $C_4$  commutano con  $h$ , l'intersezione tra  $C_4$  e  $\langle h \rangle$  è banale e il loro prodotto genera  $G$  per ragioni di cardinalità, pertanto

$$G \cong \langle h \rangle \times C_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

- $[\varphi_g = id, \text{ord}(h) = 4]$ . Possiamo considerare  $h^2$  e ricondurci al caso precedente.
- $[\varphi_g = id^{-1}, \text{ord}(h) = 2]$ . Abbiamo che  $hgh = g^{-1}$ , quindi per la nostra caratterizzazione dei gruppi diedrali

$$G \cong D_4$$

- $[\varphi_g = id^{-1}, \text{ord}(h) = 4]$ . Anche  $\text{ord}(gh) = 4$ . Infatti

$$e = ghgh = ghgh^{-1}hh = hh \neq e$$

Dunque abbiamo trovato l'ordine di tutti gli elementi, possiamo costruire un'isomorfismo esplicito con  $Q_8$ .

**Definizione** (Quaternioni). Sia  $Q_8$  l'insieme  $\{\pm 1, \pm i, \pm j, \pm k\}$  con l'operazione che soddisfa

$$i^2 = j^2 = k^2 = ijk = -1$$

## G.7 Prodotto Semidiretto

**Definizione** (Prodotto semidiretto). Siano  $H, K$  due gruppi e  $\varphi : K \rightarrow \text{Aut}(H)$  un'omomorfismo. Si dice prodotto semidiretto

$$H \rtimes_{\varphi} K$$

l'insieme dato dal prodotto cartesiano, dotato dell'operazione

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

*Osservazione.* Il prodotto semidiretto è un gruppo.

*Osservazione.* Il prodotto diretto è un prodotto semidiretto in cui  $\varphi$  manda tutti gli elementi di  $K$  nell'identità su  $H$ .

*Osservazione.* Sia  $\bar{H} = H \times e_K$ . Si ha

$$\ker \Pi_K = \bar{H} \triangleleft H \rtimes_{\varphi} K$$

qualunque sia l'omomorfismo  $\varphi$ . Infatti  $\bar{H}$  è il nucleo dell'omomorfismo di proiezione su  $K$ .

*Osservazione.* Inoltre  $\bar{K}$  se e solo se il prodotto è diretto.

$$\bar{K} \triangleleft H \rtimes_{\varphi} K \Leftrightarrow \rtimes = \times$$

**Teorema G.21** (di decomposizione). Siano  $G$  un gruppo e  $H, K < G$  sottogruppi. Se

1.  $H \triangleleft G$
2.  $HK = G$
3.  $H \cap K = \{e\}$

allora

$$G \cong H \rtimes_{\varphi} K$$

dove  $\varphi$  manda  $k$  nella corrispondente azione di coniugio

$$\begin{aligned} \varphi : K &\rightarrow \text{Aut}(H) \\ k &\mapsto \varphi_k : h \mapsto hkh^{-1} \end{aligned}$$

*Dimostrazione.* Consideriamo la mappa

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

questo

- è un omomorfismo, perché

$$\begin{aligned} \Phi((h, k)(h', k')) &= \Phi(h\varphi_k(h'), kk') \\ &= \Phi(hkh'h'^{-1}, kk') \\ &= hkh'h'^{-1}kk' \\ &= hkh'h' \\ &= \Phi(h, k)\Phi(h', k') \end{aligned}$$

- è iniettivo e suriettivo per le ipotesi, rispettivamente, 2 e 3, come nella decomposizione in prodotto diretto.

dunque  $\Phi$  è un isomorfismo come desiderato. ♣

**Esempi.**

1.  $\mathcal{S}_n \cong A_n \rtimes_{\varphi} \langle (1\ 2) \rangle$ , con  $\varphi$  di coniugio.
2.  $D_n \cong \langle \rho \rangle \rtimes_{\varphi} \langle \sigma \rangle$ , con  $\varphi$  di coniugio.

### G.7.1 Classificazione dei gruppi di ordine $pq$

Se  $p = q$ , allora  $|G| = p^2$ , quindi  $G$  è abeliano. Allora necessariamente

$$G \cong \mathbb{Z}_{p^2} \quad \text{oppure} \quad G \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

Se  $p < q$ , allora ho due elementi  $x, y$  di ordine, rispettivamente,  $p$  e  $q$ , che generano relativi gruppi ciclici. Il più grande dei quali sarà normale perché ha indice  $p$  (vedi G.25):

$$\mathbb{Z}_p < G \quad \text{e} \quad \mathbb{Z}_q \triangleleft G$$

Osserviamo inoltre che i due sottogruppi hanno intersezione banale e pertanto  $\mathbb{Z}_p\mathbb{Z}_q = G$  per ragioni di cardinalità. Quindi

$$G \cong \mathbb{Z}_q \rtimes_{\varphi} \mathbb{Z}_p$$

dove

$$\begin{aligned} \varphi : \mathbb{Z}_p &\rightarrow \text{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_q^{\times} \cong \mathbf{GL}_1(\mathbb{F}_q) \\ 1 &\mapsto \varphi_1 : x \mapsto kx \end{aligned}$$

**Achtung!** Siamo passati in notazione additiva, perché i gruppi in questione sono abeliani e ciclici. A questo punto è molto comodo pensare a  $\mathbb{Z}_q$  come spazio vettoriale unidimensionale e al suo gruppo di automorfismi come l'insieme delle "matrici" invertibili che vi agisce sopra, ovvero l'insieme degli elementi invertibili di  $\mathbb{F}_p$ . Abbiamo definito l'omomorfismo solo per il generatore di  $\mathbb{Z}_p$ , perché possiamo ottenere gli altri da

$$y \mapsto \varphi_y : x \mapsto k^y x$$

ed è molto semplice convincersene: stiamo componendo applicazioni lineari, dunque moltiplicando fra loro le corrispondenti matrici. Non tutte le scelte di  $k \in \mathbb{Z}_q^{\times}$  sono accettabili però, per esempio se

$$p \nmid q-1 = |\mathbb{Z}_q^{\times}|$$

l'unico omomorfismo  $\varphi$  possibile è quello banale che ci induce

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q$$

Se invece  $p \mid q-1$  possiamo scegliere  $k$  come un qualunque generatore del solo sottogruppo di ordine  $p$  di  $\mathbb{Z}_q^{\times} \cong \mathbb{Z}_{q-1}$ . Fissiamo un generatore  $g$ , allora tutte le possibili azioni saranno della forma

$$\begin{aligned} \psi^m : \mathbb{Z}_p &\rightarrow \text{Aut}(\mathbb{Z}_q) \\ 1 &\mapsto \psi_1^m : x \mapsto g^m x \end{aligned}$$

al variare di  $m$  in  $\{1, \dots, p-1\}$ . Osserviamo dunque che

$$\psi_1^m(x) = g^m(x) = \psi_1^1(x)$$

e possiamo dunque costruire la funzione

$$\begin{aligned} \Phi : \mathbb{Z}_q \rtimes_{\psi^m} \mathbb{Z}_p &\rightarrow \mathbb{Z}_q \rtimes_{\psi_1} \mathbb{Z}_p \\ (x, y) &\mapsto (x, my) \end{aligned}$$

e verificare che è un isomorfismo:

- è un omomorfismo

$$\begin{aligned} \Phi(x, y)\Phi(x', y') &= (x, my)(x', my') \\ &= (x + \psi_{my}^1(x'), my + my') \\ &= (x + \psi_y^m(x'), my + my') \\ &= \Phi(x + \psi_y^m(x'), y + y') \end{aligned}$$

- è iniettivo: se  $\Phi(h, k) = (e, e)$ , allora  $h = e$  e, poiché  $k^m$  è un automorfismo di  $\mathbb{Z}_p$ ,  $k = e$ .

pertanto, in questo caso, esiste un unico gruppo di ordine  $pq$  non abeliano.

$$G \cong \mathbb{Z}_q \rtimes \mathbb{Z}_p$$

## G.8 Teorema di Sylow

**Definizione.** Chiamiamo  $p$ -syLOW ogni  $p$ -sottogruppo di ordine massimo. Ovvero  $H < G$ , dove  $|G| = p^m n$  con  $(m, n) = 1$  e  $|H| = p^m$ .

**Teorema G.22** (di Sylow). *Sia  $G$  un gruppo finito di ordine  $|G| = p^n m$ , dove  $p$  è primo e  $m$  è un intero a lui coprimo:  $(p, m) = 1$ . Allora sappiamo che:*

- ∃. Per ogni  $0 \leq \alpha \leq n$ , esiste un sottogruppo  $H < G$  di ordine  $|H| = p^\alpha$ .
- ⊆. Ogni  $p$ -sottogruppo è incluso in un  $p$ -syLOW.
- $\varphi_g$ . Due qualsiasi  $p$ -syLOW sono coniugati.
- $n_p$ . Il numero  $n_p$  di  $p$ -syLOW è congruo a 1 mod  $p$ .

*Dimostrazione.* Dimostriamo i punti nello stesso ordine

- ∃. Fissiamo  $0 \leq \alpha \leq n$ . Sia  $\mathcal{M}_\alpha$  l'insieme di tutti i sottoinsiemi di  $G$  di cardinalità  $p^\alpha$

$$\mathcal{M}_\alpha = \{M < G \mid |M| = p^\alpha\}$$

possiamo allora calcolarci

$$|\mathcal{M}_\alpha| = \binom{p^n m}{p^\alpha} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i}$$

e in particolare

$$v_p(|\mathcal{M}_\alpha|) = n - \alpha$$

Consideriamo ora l'azione di  $G$  su  $\mathcal{M}_\alpha$  per moltiplicazione a sinistra

$$\begin{aligned} \Psi: G &\rightarrow \mathcal{S}(\mathcal{M}_\alpha) \\ g &\mapsto \psi_g: M \mapsto gM \end{aligned}$$

Cerchiamo il sottoinsieme richiesto tra gli stabilizzatori di  $\Psi$ . Dato il solito partizionamento in orbite

$$|\mathcal{M}_\alpha| = \sum |\text{Orb}(M_i)|,$$

scopriamo che non tutte le orbite posso essere divisibili per potenze di  $p$  troppo grandi, in particolare

$$\exists i \text{ tale che } p^{n-\alpha+1} \nmid |\text{Orb}(M_i)|.$$

Il corrispondente stabilizzatore avrà pertanto cardinalità divisibile per  $p^\alpha$ ; se fissiamo un elemento  $x \in M_i$  e consideriamo la funzione iniettiva

$$\begin{aligned} f: \text{Stab}(M_i) &\rightarrow M_i \\ g &\mapsto gx \end{aligned}$$

scopriamo che lo stabilizzatore non può avere una cardinalità maggiore dell'insieme che stabilizza

$$p^\alpha \mid |\text{Stab}(M_i)| \leq |M_i| = p^\alpha$$

ed è dunque il sottogruppo che cercavamo.

- ⊆. Sia  $H < G$  un  $p$ -sottogruppo  $|H| = p^\alpha$  e  $S$  un  $p$ -syLOW. Consideriamo l'azione di  $H$  sull'insieme  $X$  delle classi laterali di  $S$  per moltiplicazione a sinistra

$$\begin{aligned} F: H &\rightarrow \mathcal{S}(X) \\ h &\mapsto \psi_h: gS \mapsto hgS \end{aligned}$$

Per la decomposizione in orbite

$$m = [G : S] = |X| = \sum \frac{|H|}{|\text{Stab}(gS)|} = \sum \frac{p^\alpha}{p^{e_i}}$$

ma, non potendo  $p$  dividere  $m$ , esiste un laterale  $\bar{g}S$  stabilizzato da tutto  $H$ . Ovvero

$$h\bar{g}S = \bar{g}S \Leftrightarrow h \in \bar{g}S\bar{g}^{-1} \forall h \in H$$

Dunque  $H \in \bar{g}S\bar{g}^{-1}$ , che è il  $p$ -syLOW cercato.

$\varphi_g$ . Siano  $A, B$   $p$ -syLOW. Per il punto precedente

$$\exists g \in G \text{ tale che } A < gBg^{-1}$$

dunque  $A$  e  $B$ , avendo la stessa cardinalità, coincidono.

$n_p$ . Consideriamo l'azione di coniugio di un  $p$ -syLOW  $S$  sull'insieme  $Y$  dei suoi coniugati

$$\begin{aligned} \Phi: S &\rightarrow \mathcal{S}(Y) \\ g &\mapsto \varphi_g: H \mapsto gHg^{-1} \end{aligned}$$

Mostriamo che l'orbita di  $S$  è l'unica banale. Infatti se  $H \in Y$  ha orbita banale significa che è stabilizzato da  $S$ , dunque che i due commutano e pertanto il loro prodotto è un sottogruppo di  $G$ .

$$|HS| = \frac{|H||S|}{|H \cap S|} = \frac{p^{2n}}{|H \cap S|} \mid p^n m$$

Necessariamente  $|H \cap S| = p^n$  e dunque  $H = S$ . Per una formula ancora mai usata

$$n_p = |Y| = \text{Orb}(S) + \sum_{H \neq S} \frac{|S|}{|\text{Stab}(H)|} \equiv 1 \pmod{p}$$

Per concludere è sufficiente osservare che se

$$\text{Stab}(H) \leq S$$

allora l'orbita corrispondente ha cardinalità divisibile per  $p$ .



*Osservazione.*  $n_p$  è l'indice del normalizzatore di un  $p$ -syLOW in  $G$ . Infatti, estendendo l'azione di coniugio a tutto il gruppo

$$n_p = |\text{Orb}(P)| = \frac{|G|}{|\text{Stab}(P)|} = \frac{|G|}{|N(P)|} = [G : N(P)]$$

**Teorema G.23.** *Ogni gruppo  $G$  abeliano finito è prodotto diretto dei suoi  $p$ -syLOW.*

*Dimostrazione.* Usiamo la nozione additiva e sia  $G = p^n m$  come al solito. Per ogni divisore  $d$  dell'ordine del gruppo sia

$$G_d = \ker \psi_d = \{g \in G \mid dg = 0\}$$

Ci è sufficiente mostrare che

$$G \cong G_{p^n} \times G_m$$

Osserviamo innanzitutto che  $G_{p^n}$  è un  $p$ -syLOW. Dev'essere un  $p$ -gruppo perché se  $|G_{p^n}|$  fosse divisibile per un primo  $q$ , allora per il Teorema di Cauchy G.6 conterrebbe almeno un elemento di ordine  $q$ , contro la sua definizione. A questo punto, dovendo contenere l'unico  $p$ -syLOW di  $G$  (il coniugio è banale negli abeliani) non può che esserlo. Verifichiamo che

1. I due sottogruppi sono normali in  $G$ , perché è abeliano.

- La loro intersezione è banale, perché tutti gli elementi del  $p$ -syllow hanno ordine divisibile per un primo che non divide l'ordine  $m$  dell'altro sottogruppo.
- La loro somma è  $G$ . Infatti per Bezout esistono interi  $a, b$  tali che

$$ap^n + bm = 1$$

che moltiplicato per un qualunque elemento di  $g \in G$  diventa

$$a(gp^n) + b(gm) = g$$

Osserviamo che  $gp^n \in G_m$ , poiché

$$m(gp^n) = (mp^n)g = |G|g = 0$$

Analogamente  $gm \in G_{p^n}$  e pertanto la somma dei due sottogruppi contiene  $G$ .



### Esercizi.

- Chi è il 2-sylow di  $S_4$ ?
- Chi sono i gruppi di ordine 12?

### G.8.1 Classificazione dei gruppi di ordine 12

Quanti possono essere i  $p$ -syllow? I 3-sylow sono necessariamente di ordine 3, pertanto ciclici, e possono essere  $n_3 = 1$  o 4. I 2-sylow sono di ordine 4, quindi isomorfi a  $\mathbb{Z}_2 \times \mathbb{Z}_2$  o  $\mathbb{Z}_4$ , e sono  $n_2 = 1$  o 3. Se  $P_3$  non è normale, allora ne ho 4 copie con intersezione banale e rimane spazio solo per un  $P_2$ , che sarà normale.

Quindi almeno uno tra un 2-sylow e un 3-sylow sarà normale. Inoltre devono avere intersezione banale e il loro prodotto ha necessariamente cardinalità 12. Quindi  $G$  è un prodotto semidiretto tra un sylow e l'altro. Analizziamo le varie possibilità

►  $\mathbb{Z}_4 \rtimes_{\varphi} \mathbb{Z}_3$ . Abbiamo

$$\varphi : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$$

che è necessariamente banale. Otteniamo

$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$$

►  $\mathbb{Z}_2 \times \mathbb{Z}_2 \rtimes_{\varphi} \mathbb{Z}_3$ . Abbiamo

$$\varphi : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$$

la cui immagine dev'essere un sottogruppo di  $A_3$ . Otteniamo l'automorfismo banale, da cui

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

e quelli associati a  $\sigma = (1\ 2\ 3)$  e  $\sigma^2 = (1\ 3\ 2)$ , che vogliamo mostrare indurre lo stesso prodotto. Infatti, scelto un  $\varphi$  non banale, possiamo far agire  $G$  sull'insieme dei suoi 3-sylow per coniugio: sia

$$\Phi : G \rightarrow S(\text{3-sylow di } G) \cong S_3$$

$$g \mapsto \varphi_g : H \mapsto gHg^{-1}$$

Osserviamo che  $N(P_3) = P_3$ , per la formula delle classi. Allora

$$\ker \Phi = \bigcap \text{Stab}(H) = \bigcap N(H) = \bigcap H = \{e\}$$

dunque  $\Phi$  è iniettivo e mappa  $G$  in un sottogruppo di ordine 12 di  $S_4$ . Ma l'unico sottogruppo di questa dimensione è  $A_4$ , quindi entrambi i gruppi generati dal prodotto non diretto sono isomorfi a questo sottogruppo.

$$G \cong A_4$$

►  $\mathbb{Z}_3 \rtimes_{\varphi} \mathbb{Z}_4$ . Abbiamo

$$\varphi : \mathbb{Z}_4 \rightarrow \text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$$

che può essere solo  $\pm id$ . Il caso banale ci restituisce un prodotto diretto, già considerato, l'altro è un gruppo buffo

$$G \cong \mathbb{Z}_3 \rtimes_{-id} \mathbb{Z}_4$$

►  $\mathbb{Z}_3 \rtimes_{\varphi} \mathbb{Z}_2 \times \mathbb{Z}_2$ . Abbiamo

$$\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$$

e abbiamo, oltre all'omomorfismo banale, 3 modi di proiettare  $\mathbb{Z}_2 \times \mathbb{Z}_2$  su un suo fattore. A meno di isomorfismi di  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ,  $\mathbb{Z}_3$  commuta con uno dei fattori e agisce con  $-id$  sull'altro quindi

$$G \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \rtimes_{-id} \mathbb{Z}_2 \cong D_6$$

## G.9 Automorfismi di un gruppo buffo

Vogliamo scoprire chi è  $\text{Aut}(Q_8 \times D_4)$ . Per far questo, possiamo scomporre un qualunque automorfismo  $\varphi$  nelle sue restrizioni ai due termini del prodotto e proiettarli sulle due componenti. Il seguente diagramma magico è molto esplicativo

$$\begin{array}{ccccc} Q_8 & & & & Q_8 \\ & \searrow & & \nearrow & \\ & G & \xrightarrow{\varphi} & G & \\ & \nearrow & & \searrow & \\ D_4 & & & & D_4 \end{array}$$

Dunque possiamo scomporre l'automorfismo nei quattro omomorfismi

$$\varphi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

dove

$$\begin{array}{ll} \alpha : Q_8 \rightarrow Q_8 & \beta : D_4 \rightarrow Q_8 \\ \gamma : Q_8 \rightarrow D_4 & \delta : D_4 \rightarrow D_4 \end{array}$$

Iniziamo ad analizzare i possibili omomorfismi.

$\beta$ . Consideriamo le possibili immagini per dimensione, tra i sottogruppi dei quaternioni:

$\{e\}$ . [✓] Ovviamente abbiamo un omomorfismo banale.

$\mathbb{Z}_2$ . [✓] Il nucleo dev'essere un sottogruppo di indice 2 e il diedrale ne ha tre:  $\langle \rho \rangle, \langle \rho^2, \sigma \rangle, \langle \rho^2, \sigma \rho \rangle$ .

$\mathbb{Z}_4$ . L'unico sottogruppo di indice 4 del diedrale è  $\langle \rho \rangle \cong \mathbb{Z}_4$  ed è il nucleo di un omomorfismo che uccide i termini di ordine 4.

$Q_8$ . Non è possibile, sarebbe un isomorfismo!

Tutti questi omomorfismi preservano necessariamente i centralizzatori, perché l'unico sottogruppo dei quaternioni di ordine 2 è il centro. Dunque sembrano accettabili tutti gli omomorfismi

$$\boxed{\beta : D_4 \rightarrow Z(Q_8)}$$

$\gamma$ . Consideriamo le possibili immagini, per dimensione:

$\{e\}$ . [✓] Ovviamente abbiamo un omomorfismo banale.

$\mathbb{Z}_2$ . [✓] Il nucleo dev'essere un sottogruppo di indice 2 e i quaternioni ne hanno tre:  $\langle i \rangle, \langle j \rangle, \langle k \rangle$ .

$\mathbb{Z}_4$ . L'unico sottogruppo di indice 4 dei quaternioni è  $\{\pm 1\}$  ed è il nucleo di un omomorfismo che uccide i termini di ordine 4.

$\mathbb{Z}_2 \times \mathbb{Z}_2$ . Possiamo mandare i quaternioni in  $(\mathbb{Z}_2)^3$  usando i tre omomorfismi con immagine  $\mathbb{Z}_2$ , questo omomorfismo non sarà suriettivo, altrimenti sarebbe un isomorfismo, e ha almeno 4 elementi nell'immagine, visto che gli omomorfismi di sopra sono distinti. Quindi, permutando le componenti opportunamente, otteniamo 6 omomorfismi.

$D_4$ . Non è possibile, sarebbe un isomorfismo!

possiamo però escludere alcuni omomorfismi osservando che l'automorfismo  $\varphi$  deve preservare i centralizzatori. Infatti osservando il magico diagramma

$$\begin{array}{ccc} Q_8 \hookrightarrow Q_8 \times D_4 & \rightarrow & Q_8 \times D_4 \\ i \mapsto (i, e) & \mapsto & (\alpha(i), \gamma(i)) \end{array}$$

scopriamo che  $Z(i, e) \cong \mathbb{Z}_4 \times D_4$ . Possiamo ora cercare di capire cosa dovrebbe essere  $Z(\alpha(i)) \times Z(\gamma(i))$ , per esempio elencando i possibili prodotti di sottogruppi di ordine 32

$Q_8 \times (\mathbb{Z}_2)^2$ . Che però ha solo 25 elementi di ordine 2.

$Q_8 \times \mathbb{Z}_4$ . Che ha sol 11 elementi di ordine 2.

$\mathbb{Z}_4 \times (\mathbb{Z}_2)^2$ . Che però è abeliano.

$\mathbb{Z}_4 \times \mathbb{Z}_4$ . Che è abeliano.

$\mathbb{Z}_4 \times D_4$ . [✓] Che sicuramente è il gruppo che cerchiamo.

quindi necessariamente il centralizzatore di  $Z(\gamma(i)) \cong D_4$  e pertanto  $\gamma(i)$  è un elemento del centro di  $D_4$ , che ha solo due elementi. Quindi gli omomorfismi  $\gamma$  accettabili sono solo quello banale e i tre che hanno immagine in  $\mathbb{Z}_2$ . Dunque sembrano accettabili tutti gli omomorfismi

$$\boxed{\gamma : Q_8 \rightarrow Z(D_4)}$$

$\alpha$ . Dev'essere un isomorfismo. Se non fosse un'isomorfismo l'immagine non potrebbe avere dimensione 4, perché come già visto i sottogruppi di indice adatto eliminano gli elementi di ordine 4, e non potrebbe avere dimensione più piccola, perché altrimenti il primo termine dell'immagine di  $\varphi$  apparterrebbe sempre al centro di  $G$ .

$\delta$ . Analogamente dev'essere un isomorfismo.

Mostriamo ora che le condizioni trovate sono sufficienti. Ci basta mostrare che  $\varphi$ , costruito con le componenti sopra trovate, è iniettivo. Supponiamo di aver trovato  $(x, y) \in G$  tale che

$$\varphi(x, y) = (\alpha(x)\beta(y), \gamma(x)\delta(y)) = (e, e)$$

Visto che  $\beta(y)$  e  $\gamma(x)$  stanno nei centri dei rispettivi insiemi, anche  $\alpha(x)$  e  $\delta(y)$ , che sono i loro inversi, vi staranno. Ma  $\alpha$  e  $\delta$  sono isomorfismi, pertanto anche  $x, y$  staranno nei centri dei loro rispettivi gruppi! Ma  $\beta$  e  $\gamma$  contengono i centri nei loro nuclei, quindi si annullano, così come i rispettivi isomorfismi. Così  $x, y$  sono necessariamente l'elemento neutro del proprio gruppo e  $\ker \varphi = \{(e, e)\}$ .

Conosciamo già  $\text{Aut}(D_4)$ , cerchiamo, per concludere, di capire chi sia  $\text{Aut}(Q_8)$ .

Ogni automorfismo  $\alpha$  di  $Q_8$  deve mandare  $\alpha(-x) = -\alpha(x)$ , quindi le coppie

$$(i, -i) \quad (j, -j) \quad (k, -k)$$

non vengono scisse, ma solo permutate fra loro. Possiamo quindi far agire  $\text{Aut}(Q_8)$  sull'insieme di queste tre coppie, costruendo così un'omomorfismo

$$\xi : \text{Aut}(Q_8) \rightarrow \mathcal{S}_3$$

Il nucleo di  $\xi$  è costituito dagli automorfismi che non scambiano nessuna coppia, dunque quello identico e i tre che cambiano segni a due delle coppie, ed è dunque isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

Se consideriamo ora gli isomorfismi

$$S : \begin{cases} i \mapsto j \\ j \mapsto i \\ k \mapsto k \end{cases} \quad T : \begin{cases} i \mapsto j \\ j \mapsto k \\ k \mapsto i \end{cases}$$

questi generano un sottogruppo "disgiunto" da  $\mathbb{Z}_2 \times \mathbb{Z}_2$  isomorfo a  $\mathcal{S}_3$ , quindi

$$\boxed{\text{Aut}(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \rtimes_{\phi} \mathcal{S}_3}$$

Per una certa azione  $\phi$  che rende il gruppo  $\mathcal{S}_4$  (per ragioni magiche non dimostrate).

## G.10 Teorema Fondamentale dei Gruppi Abeliani Finiti

**Teorema G.24** (di Struttura dei Gruppi Abeliani Finiti).  
*Se  $G$  è un gruppo abeliano finito allora si decompone in modo unico come prodotto diretto di gruppi ciclici*

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

con  $n_1 \mid \cdots \mid n_s$ .

*Dimostrazione.* Avendo già dimostrato che ogni gruppo abeliano finito si decompone nel prodotto dei suoi  $p$ -syloew ci è sufficiente dimostrare la tesi per i  $p$ -gruppi. Dato gruppo abeliano  $G$  di ordine  $p^n$ , ci basta mostrare che possiamo scriverlo come prodotto diretto del generato da un suo elemento di ordine massimo  $g$  e un altro sottogruppo  $K$

$$G \cong \langle g \rangle \times K$$

così da poter procedere per induzione.

Mostriamo questo risultato intermedio per induzione sull'ordine del  $p$ -gruppo  $G$ . Se  $|G| = p$  allora il gruppo è ciclico ed è generato da  $g$ . Supponiamo ora la tesi vera per ogni  $k$  con  $1 \leq k < n$  e prendiamo  $g$  un elemento di ordine massimo, diciamo  $p^m$ . Prendiamo ora un elemento  $h \in G$  che non stia nel sottogruppo  $\langle g \rangle$  e in modo che abbia ordine minimo possibile, se non esiste abbiamo  $G = \langle g \rangle$  e abbiamo finito.

Vogliamo ora mostrare che

$$\langle g \rangle \cap \langle h \rangle = \{e\}$$

L'ordine di  $h^p$  è ovviamente minore di quello di  $h$ , dunque  $h^p \in \langle g \rangle$ , ovvero esiste un intero  $r \in \mathbb{Z}$  tale che

$$h^p = g^r$$

L'ordine di  $g^r$  è al più  $p^{m-1}$ :

$$(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = e$$

pertanto non è un generatore di  $\langle g \rangle$ , dunque per un qualche intero  $s$  abbiamo

$$h^p = g^r = g^{ps}$$

e succede che

$$(g^{-s}h)^p = g^{-sp}h^p = e$$

esiste un elemento (ovvero  $g^{-s}h$ ) di ordine  $p$  che non appartiene a  $\langle g \rangle$ ! Quindi anche l'ordine di  $h$  è  $p$  e i due sottogruppi devono essere disgiunti.

Osserviamo ora che, detto  $H = \langle h \rangle$ , l'ordine di  $gH$  in  $G/H$  è lo stesso di  $g$  in  $G$ , in particolare è ancora massimo. Se fosse più piccolo, sarebbe al più  $p^{m-1}$  e

$$H = (gH)^{p^{m-1}} = g^{p^{m-1}}H$$

e pertanto  $g^{p^{m-1}} \in H$ , assurdo. Per l'ipotesi induttiva e il teorema di corrispondenza

$$G/H \cong \langle gH \rangle \times K/H$$

per un certo sottogruppo  $H < K < G$ . Mostriamo che  $K$  è il sottogruppo che cercavamo

►  $\langle g \rangle \cap K = \{e\}$ . Infatti se  $b$  stesse nell'intersezione,  $bH$  apparterebbe all'intersezione  $\langle gH \rangle \cap K/H$  che è  $H$ , dunque  $b \in H$ .

►  $G = \langle g \rangle K$ . Per ragioni di cardinalità.

L'unicità è noiosa e poco interessante e, pertanto, lasciata al lettore.



### G.10.1 Classificazione dei Gruppi di Ordine 30

Tiriamo a caso qualche gruppo di quest'ordine

$$\boxed{\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5} \quad \boxed{D_{15}} \quad \boxed{D_5 \times \mathbb{Z}_3} \quad \boxed{D_3 \times \mathbb{Z}_5}$$

questi sono distinti perché il primo è l'unico abeliano e i centri di dei seguenti sono rispettivamente  $\{e\}$ ,  $\mathbb{Z}_3$ ,  $\mathbb{Z}_5$ . Sappiamo che

$$n_5 \equiv 1 \pmod{5} \quad \text{e} \quad n_5 \mid 6$$

per il Teorema di Sylow G.22 e perché  $n_5 \mid |G|$  in quanto cardinalità dell'orbita dell'azione di coniugio, rispettivamente. E, analogamente

$$n_3 \equiv 1 \pmod{3} \quad \text{e} \quad n_3 \mid 10$$

Allora, se  $P_5$  non è normale, ci sono sei 5-syloew, quindi 24 elementi di ordine 5. Tra i pochi elementi che rimangono non ci stanno sicuramente dieci 3-syloew e pertanto  $P_3$  è normale. Dunque almeno uno tra  $P_5$  e  $P_3$  è normale. Allora  $P_3$  e  $P_5$  commutano (perché uno dei due è contenuto nel normalizzatore dell'altro), dunque

$$P_3 P_5 < G$$

e avendo indice 2 è normale, nonché ciclico.

Abbiamo allora che

$$G \cong \mathbb{Z}_{15} \rtimes_{\varphi} \mathbb{Z}_2$$

per una qualche azione di coniugio

$$\begin{aligned} \varphi: \mathbb{Z}_2 &\rightarrow \text{Aut}(\mathbb{Z}_{15}) \cong \mathbb{Z}_5^{\times} \times \mathbb{Z}_3^{\times} \\ y &\mapsto \varphi_y: x \mapsto xy^{-1} = x^a \end{aligned}$$

sapendo che  $\varphi_y^2(x) = x^{a^2} = x$ , dobbiamo avere che

$$a^2 \equiv 1 \pmod{15}$$

e risolvendo il sistema di diofantee troviamo

$$a \equiv \pm 1, \pm 4 \pmod{15}$$

e ognuna di queste azioni induce un prodotto semidiretto isomorfo a uno dei gruppi trovati all'inizio. In particolare  $a = 1$  è l'automorfismo identico, che induce il prodotto diretto, che restituisce il gruppo abeliano, mentre  $a = -1$  sappiamo già essere l'omomorfismo che genera il gruppo diedrale. Per  $a = 4$  troviamo l'automorfismo che fissa  $\mathbb{Z}_3$ , per  $a = -4$  quello che fissa  $\mathbb{Z}_5$ , in entrambi i casi uno dei fattori a sinistra del prodotto semidiretto commuta anche col fattore di destra, siamo così autorizzati a raccoglierlo all'esterno per ottenere, rispettivamente,  $D_5 \times \mathbb{Z}_3$  e  $D_3 \times \mathbb{Z}_5$ .

## G.11 Lemmi vari ed esercizi sparsi

**Lemma G.25** (del piccolo indice primo). *Siano  $G$  un gruppo finito e  $H$  un sottogruppo che ha come indice il più piccolo primo  $p$  che divide  $G$ , allora  $H \triangleleft G$ .*

*Dimostrazione.* Consideriamo l'azione di  $G$  sull'insieme  $X$  dei laterali di  $H$  per moltiplicazione a sinistra

$$\begin{aligned}\Phi: G &\rightarrow \mathcal{S}_p \\ g &\mapsto \Pi_g: xH \mapsto gxH\end{aligned}$$

Osserviamo che

$$\begin{aligned}g \in \text{Stab}(xH) &\Leftrightarrow gxH = xH \\ &\Leftrightarrow x^{-1}gx \in H \\ &\Leftrightarrow g \in xHx^{-1}\end{aligned}$$

dunque  $\text{Stab}(xH) = xHx^{-1}$  è il sottogruppo coniugato di  $H$  rispetto ad  $x$ . Possiamo ora riscrivere il nucleo come

$$\ker \Phi = \bigcap_{x \in G} xHx^{-1} < H$$

e osservare che, per il Primo Teorema di Omomorfismo

$$\Phi': G/\ker \Phi \rightarrow \mathcal{S}_p$$

è iniettivo e pertanto

$$\left| G/\ker \Phi \right| \mid |\mathcal{S}_p| = p!$$

ma  $p$  era il più piccolo primo a dividere  $|G|$ , quindi non potendo  $\ker \Phi$  coincidere con tutto il gruppo, dovrà essere proprio  $H$ . Il che conclude la dimostrazione. ♣

**Lemma G.26.** *Sia  $G$  un gruppo di ordine  $2^k d$ , dove  $d$  è dispari. Allora esiste un sottogruppo di indice 2.*

*Dimostrazione.* Il Teorema di Cayley ci fornisce l'immersione seguente, per moltiplicazione sinistra

$$\begin{aligned}\Phi: G &\hookrightarrow \mathcal{S}_{2d} \\ g &\mapsto \varphi_g: x \mapsto gx\end{aligned}$$

Dato un elemento  $g$ , conosciamo la decomposizione in cicli di  $\varphi_g$ , questa dev'essere prodotto di cicli del tipo

$$(x \ gx \ \dots \ g^{m-1}x)$$

al variare di  $x$  in un opportuno sistema di rappresentanti e dove  $m$  è l'ordine di  $g$ . Per il Teorema di Cauchy esiste un elemento di ordine 2, che avrà dunque come immagine il prodotto di  $d$   $2^k$ -cicli, perché nessun elemento è fissato dalla moltiplicazione sinistra. Pertanto  $G \not\triangleleft \mathcal{A}_{2d}$  e quindi

$$[G : G \cap \mathcal{A}_{2d}] = 2$$

♣

**Lemma G.27.** *Sia  $G$  un gruppo semplice e finito. Se esiste un sottogruppo  $H < G$  di indice  $n$ , allora esiste un'immersione di  $G$  in  $\mathcal{A}_n$ .*

*Dimostrazione.* Facendo agire  $G$  per moltiplicazione sinistra sull'insieme degli  $n$  laterali di  $H$  otteniamo un omomorfismo

$$\Phi: G \rightarrow \mathcal{A}_n$$

il cui nucleo dev'essere però banale, per non contraddire la normalità di  $G$ . Ovviamente l'omomorfismo non è banale, dunque  $\Phi$  è un'immersione. ♣

*Osservazione.* Sia  $G$  un gruppo abeliano. Sia

$$\begin{aligned}\psi_n: G &\rightarrow G \\ x &\mapsto x^n\end{aligned}$$

preso un qualunque automorfismo  $\varphi \in \text{Aut}(G)$  il seguente diagramma è commutativo

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

quindi  $\ker \psi_n$  e  $\psi_n(G)$  sono caratteristici in  $G$ .

### Esercizi.

1. Trova  $\text{Aut}(\mathbb{Z} \times \mathbb{Z}_n)$ .
2. Trova  $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4)$ .
3. Trova  $\text{Aut}(Q_8 \times D_4)$ .
4. Sia  $G$  un gruppo abeliano finito. Se  $H \triangleleft G$  è ciclico e lo è anche il loro quoziente, allora anche  $G$  è ciclico.
5. Dati

$$H \triangleleft K \triangleleft G$$

quali inclusioni devono essere caratteristiche per far sì che  $H$  sia normale o caratteristico in  $G$ ?

6. Sia  $G$  un gruppo finito. Se esiste un sottogruppo  $H < G$  di indice  $n$ , allora esiste un sottogruppo normale  $N \triangleleft G$  di indice divisore di  $n!$ .
7. Un gruppo di ordine 112 non è semplice.
8. Un gruppo di ordine 144 non è semplice.
9. Quanti sono i  $p$ -sylow di  $\mathbf{GL}_n(\mathbb{F}_p)$ ?
10. Dato un gruppo di ordine  $|G| = p^3$ 
  - (a) dimostrare che  $|Z(G)| = p$ .
  - (b) dimostrare che  $G' = Z(G)$ .
  - (c) contare il numero di classi di coniugio.
11. In un  $p$ -gruppo, il centro di uno stabilizzatore di un elemento non nel centro è più grande del centro di tutto il gruppo.
12.  $\mathbb{Z}_n^\times$  è ciclico se e solo se  $n = 2, 4, p^n, 2p^n$ .

## A Anelli

### A.1 Prime definizioni

Per “Anello” si intende un anello commutativo con identità.

**Definizione** (Divisori di 0). Un elemento di un anello  $x \in A$  si dice *divisore di zero* quando

$$\exists y \in A \quad \text{tale che} \quad yx = 0$$

Un anello  $A$  si dice *dominio d'integrità* quando l'unico divisore di zero è lo 0 stesso

$$\mathcal{D} := \{\text{divisori di zero}\} = \{0\}$$

**Definizione** (Nilpotenza). Un elemento di un anello  $x \in A$  si dice *nilpotente* quando

$$\exists n \in \mathbb{N} \quad \text{tale che} \quad x^n = 0$$

Un anello  $A$  si dice *ridotto* quando l'unico elemento nilpotente è 0

$$\mathcal{N} := \{\text{nilpotenti}\} = \{0\}$$

**Lemma A.1** (Prime proprietà). *Valgono:*

1.  $A^\times$  è un gruppo moltiplicativo.
2.  $A^\times \cap \mathcal{D} = \emptyset$ .
3. Se  $A$  è finito  $A = A^\times \sqcup \mathcal{D}$ .

*Osservazione.* Un dominio d'integrità finito è un campo.

#### A.1.1 Anelli di polinomi

Dato un anello  $A$ , consideriamo il corrispondente anello dei polinomi a coefficienti in  $A$ :

$$A[x] = \{a_0 + \dots + nx^n \mid a_k \in A\}$$

**Quali sono gli elementi nilpotenti di  $A[x]$  ?**

Prendiamo un polinomio nilpotente

$$f = a_0 + \dots + a_n x^n$$

e osserviamo che il termine di grado maggiore in  $f^k$  è  $a_n^k x^{nk}$ . Quindi, affinché  $f$  sia nilpotente,  $a_n$  dev'essere nilpotente in  $A$  e pertanto  $a_n x^n$  sarà nilpotente in  $A[x]$ . Osserviamo che *la somma di elementi nilpotenti è nilpotente*:

$$a^n = 0, b^m = 0 \quad \Rightarrow \quad (a+b)^{n+m} = 0$$

per concludere che anche  $f - a_n x^n$  sarà nilpotente, e quindi, iterando

$$f \in \mathcal{N}(A[x]) \quad \Leftrightarrow \quad a_0, \dots, a_n \in \mathcal{N}(A)$$

La freccia inversa è banale: elevando il polinomio a una potenza sufficientemente alta, otteniamo prodotti di potenze dei coefficienti tali che in ogni prodotto compare almeno un coefficiente con potenza maggiore del suo indice di nilpotenza.

**Quali sono gli elementi invertibili di  $A[x]$  ?**

Procediamo come prima, prendendo un polinomio invertibile

$$f = a_0 + \dots + a_n x^n$$

e il suo inverso

$$g = b_0 + \dots + b_m x^m \quad \text{tale che} \quad fg = 1$$

e osserviamo le relazioni tra i coefficienti di  $fg$  e quelli dei fattori:

$$\begin{aligned} 1 &= a_0 b_0 \\ 0 &= a_0 b_1 + a_1 b_0 \\ &\vdots \\ 0 &= a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m \\ 0 &= a_n b_{m-1} + a_{n-1} b_m \\ 0 &= a_n b_m \end{aligned}$$

Innanzitutto,  $a_0$  e  $b_0$  sono invertibili. Moltiplicando la penultima relazione per  $a_n$  otteniamo

$$0 = a_n^2 b_{m-1} + a_n a_{n-1} b_m = a_n^2 b_{m-1}$$

moltiplicando la terzultima per  $a_n^2$

$$0 = a_n^3 b_{m-2}$$

e iterando

$$0 = a_n^{m+1} b_0$$

ma  $b_0$  è invertibile, quindi non può essere un divisore di zero, pertanto  $a_n^{m+1} = 0$ . Procedendo come prima

$$f \in A[x]^\times \quad \Leftrightarrow \quad a_0 \in A^\times \text{ e } f - a_0 \in \mathcal{N}(A[x])$$

Per la freccia inversa scriviamo

$$f = a_0 + g \quad \text{con } a_0 \in A^\times \text{ e } g \in \mathcal{N}(A[x])$$

e consideriamo i polinomi

$$h_m(x) = a_0^{2m} - a_0^{2m-1}g + a_0^{2m-2}g^2 + \dots + g^{2m}$$

che moltiplicati per  $f$  restituiscono

$$f h_m = a_0^{2m+1} + g^{2m+1}$$

scelto  $m$  maggiore dell'indice di nilpotenza di  $g$ , abbiamo che

$$a_0^{-(2m+1)} f h_m = 1$$

**Quali sono i divisori di zero in  $A[x]$  ?**

Prendiamo un polinomio divisore di zero

$$f = a_0 + \dots + a_n x^n$$

e un polinomio

$$g = b_0 + \dots + b_m x^m \quad \text{tale che} \quad fg = 0$$

di grado minimo possibile. Consideriamo, al variare di  $0 \leq k \leq n$ , i prodotti  $a_k q$ . Se questi non sono tutti nulli, consideriamo il più grande  $k$  tale che

$$a_k q \neq 0$$

Allora

$$0 = fg = (a_0 + \dots + a_k x^k)(b_0 + \dots + b_m x^m)$$

osserviamo che i coefficienti del termine di grado massimo è

$$a_k b_m = 0$$

e quindi

$$p \cdot (a_k q) = 0$$

ma  $\deg a_k q < \deg q$ , quindi dobbiamo avere necessariamente che  $a_k q = 0 \forall k$ , quindi che  $a_k b_0 = 0 \forall k$ , ossia

$$f \in \mathcal{D}(A[x]) \quad \Leftrightarrow \quad \exists b \neq 0 \in A \mid ba_k = 0 \quad \forall k$$



## A.2 Ideali

**Definizione** (ideale). Chiamiamo *ideale* un sottogruppo additivo  $I \subseteq A$  che assorbe per moltiplicazione.

*Osservazione.* Abbiamo una bella caratterizzazione degli ideali propri

$$I \subsetneq A \Leftrightarrow I \cap A^\times = \emptyset \Leftrightarrow 1 \notin I$$

(è quasi completamente ovvia guardando la contronominale)

*Osservazione.* Un campo  $\mathbb{K}$  ha solo ideali banali.

**Definizione** (Omomorfismo). Una funzione tra due anelli  $A$  e  $B$  è detta omomorfismo di anelli se

1. è omomorfismo dei rispettivi gruppi additivi.
2.  $f(ab) = f(a)f(b)$
3.  $f(1_A) = f(1_B)$

**Teorema A.2** (di omomorfismo). *Dato un omomorfismo di anelli  $f$  e un ideale  $I \subseteq \ker f$ , esiste ed è unico l'omomorfismo  $\bar{f}$  che fa commutare il seguente diagramma*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow \bar{f} & \\ A/I & & \end{array}$$

*Dimostrazione.* Come per l'analogo teorema sui gruppi, consideriamo la mappa

$$\begin{aligned} \bar{f}: A/I &\rightarrow B \\ a + I &\mapsto f(a) \end{aligned}$$

e verifichiamo che è ben definita e un omomorfismo. ♣

*Osservazione.* Gli ideali sono tutti e soli i nuclei di omomorfismi.

**Lemma A.3.** *Dato un omomorfismo  $f: A \rightarrow B$*

- ▶ *La controimmagine  $f^{-1}(J)$  di un ideale  $J \subseteq B$  è un ideale di  $A$ .*
- ▶ *L'immagine  $f(I)$  di un ideale  $I \subseteq A$  è un ideale di  $B$ , se  $f$  è suriettiva.*

*Dimostrazione.* Preso  $J \subseteq B$ , osserviamo che la sua controimmagine  $f^{-1}(J)$  assorbe per prodotto

$$f(af^{-1}(J)) = f(a)f(J) = J \Rightarrow af^{-1}(J) = f^{-1}(J)$$

ed è additivamente chiusa

$$f(i+j) = f(i) + f(j) \in J \quad \forall i, j \in f^{-1}(J)$$

Assumendo  $f$  suriettiva, per ogni  $b \in B$  peschiamo un elemento  $a$  della controimmagine, allora

$$f(aI) = f(a)f(I) = af(I) = f(I)$$

e la chiusura additiva è analoga. ♣

**Teorema A.4** (di corrispondenza). *Ogni proiezione*

$$\Pi: A \rightarrow A/I$$

*induce una relazione biunivoca tra gli ideali del quoziente e gli ideali di  $A$  che contengono  $I$*

$$\{\text{ideali di } A/I\} \leftrightarrow \{\text{ideali di } A \text{ che contengono } I\}$$

*che preserva:*

- ▶ *l'ordinamento indotto dall'inclusione.*
- ▶ *l'indice.*
- ▶ *primalità e massimalità.*

*Dimostrazione.* La controimmagine di un ideale del quoziente, per il lemma precedente (A.3), è ancora un ideale. Inoltre, essendo un ideale, contiene lo 0, dunque la sua controimmagine contiene  $\ker f = I$ . Osserviamo ora che, essendo la proiezione una mappa suriettiva, l'immagine di ogni ideale è ancora un ideale! Pertanto è sufficiente mostrare che ideali diversi, contenenti  $I$ , vengono mandati dalla proiezione in ideali diversi: difatti i rispettivi gruppi additivi vengono mandati, per l'analogo teorema sui gruppi, in gruppi distinti. ♣

*Osservazione.* Vale sempre che

$$IJ \subseteq I \cap J$$

c'è uguaglianza in caso di *comassimalità*

$$I + J = A \Rightarrow IJ = I \cap J$$

*Dimostrazione.* Dato l'assorbimento per moltiplicazione

$$IJ \subseteq J, \quad JI \subseteq I \Rightarrow IJ \subseteq I \cap J$$

Se  $I, J$  sono comassimali, allora

$$I + J = A \Rightarrow \exists i \in I, j \in J \text{ tali che } i + j = 1$$

e per ogni elemento  $x \in I \cap J$  si ha che

$$x = xi + xj \in IJ$$

perché entrambi gli addendi appartengono a  $IJ$ . ♣

**Teorema A.5** (cinese degli anelli). *Dati due ideali  $I, J \subseteq A$  comassimali, si ha che*

$$A/IJ \cong A/I \times A/J$$

*Dimostrazione.* La mappa

$$\begin{aligned} f: A &\rightarrow A/I \times A/J \\ a &\mapsto (a + I, a + J) \end{aligned}$$

è un omomorfismo di nucleo

$$\ker f = I \cap J$$

Inoltre  $f$  è suriettivo se e solo se  $I + J = A$ : se  $f$  è suriettivo, prendiamo un elemento  $a$  nella controimmagine di  $(1 + I, 1 + J)$ , ossia un elemento tale che  $a - 1 \in I$  e  $a \in J$ . Pertanto

$$a - 1 = i \Rightarrow 1 = a + i \in I + J$$

Se invece  $1 \in I + J$ , allora possiamo trovare due elementi tale che

$$1 = i + j$$

e scelta una qualunque coppia  $(x + I, y + J)$ , abbiamo che

$$y + j(x - y) = xj + yi = x + i(y - x)$$

Dunque, se  $I + J = A$ , abbiamo  $\ker f = I \cap J = IJ$  per l'osservazione di sopra. ♣

**Definizione** (ideale primo). Un ideale  $I \subseteq A$  si dice *primo* quando

$$\forall x, y \in A \quad xy \in I \Rightarrow x \in I \text{ o } y \in I$$

**Definizione** (ideale massimale). Un ideale  $I \subseteq A$  si dice *massimale*, se è massimale rispetto all'inclusione tra gli ideali propri di  $A$ .

**Teorema A.6.** Dato un ideale  $I \subseteq A$ , valgono le seguenti relazioni con il rispettivo anello quoziente:

$$I \text{ è primo} \Leftrightarrow A/I \text{ è un dominio}$$

$$I \text{ è massimale} \Leftrightarrow A/I \text{ è un campo}$$

*Dimostrazione.* Per la prima proposizione, osserviamo che

$$xy \in I \Leftrightarrow \pi(xy) = 0 \Leftrightarrow \pi(x)\pi(y) = 0$$

allora

$$\pi(x)\pi(y) = 0 \Leftrightarrow \pi(x) = 0 \text{ o } \pi(y) = 0$$

che è equivalente a

$$xy \in I \Leftrightarrow x \in I \text{ o } y \in I$$

Per la seconda, ci basta invocare il teorema di corrispondenza e ricordare che un anello è anche un campo se e solo se ha solo ideali banali. ♣

*Osservazione.*  $A$  è un dominio se e solo se l'ideale  $\{0\}$  è primo, è un campo se e solo se l'ideale  $\{0\}$  è massimale.

*Osservazione.* Un ideale massimale è anche primo, perché ogni campo è anche un dominio.

$$\begin{array}{ccc} I \text{ massimale} & \longleftrightarrow & A/I \text{ campo} \\ \downarrow & & \downarrow \\ I \text{ primo} & \longleftrightarrow & A/I \text{ dominio} \end{array}$$

**Lemma A.7** (del massimale). Ogni ideale proprio è contenuto in un ideale massimale.

*Dimostrazione.* Prendiamo un ideale proprio  $I$  e consideriamo l'insieme di tutti gli ideali propri che lo contengono

$$\mathcal{M} = \{J \subseteq A \text{ ideale proprio} \mid I \subseteq J\}$$

Questa famiglia non è vuota, visto che  $I \in \mathcal{M}$ , e ogni catena  $C$  di ideali ha

$$X = \bigcup C$$

come massimale:  $X$  è un ideale perché possiamo testare somme e prodotti tra due elementi nel primo ideale in  $C$  che contiene gli elementi in questione, è un ideale proprio perché se  $1 \in X$ , allora già sarebbe appartenuto a un ideale di  $C$ . La tesi segue dal Lemma di Zorn. ♣

### A.2.1 Prodotto diretto tra anelli

Il prodotto cartesiano tra due anelli  $A \times B$ , con le operazioni ovvie, è ancora un anello. Inoltre, se ne nessuno dei due è banale

$$(1, 0)(0, 1) = (0, 0)$$

il prodotto non è un dominio. I nilpotenti e gli invertibili nel prodotto sono prodotto dei rispettivi sottoinsiemi:

$$\mathcal{N}_{A \times B} = \mathcal{N}_A \times \mathcal{N}_B \quad (A \times B)^\times = A^\times \times B^\times$$

**Lemma A.8** (Fatto Piacevole). Gli ideali del prodotto sono tutti e soli i prodotti di ideali dei fattori.

*Dimostrazione.* Prendiamo  $I \subseteq A \times B$  e consideriamo le proiezioni  $\pi_A$  e  $\pi_B$ . Queste sono omomorfismi suriettivi, quindi  $\pi_A(I)$  è un ideale di  $A$  e  $\pi_B(I)$  è un ideale di  $B$ . Basta ora far vedere che  $\pi_A(I) \times \pi_B(I) \subseteq I$ , perché abbiamo già l'inclusione opposta, che è un fatto puramente insiemistico. Se  $(a, y), (x, b) \in I$ , deve starci anche  $(a, b)$ : ma  $(1, 0)(a, y) = (a, 0) \in I$ , analogamente  $(0, b) \in I$ , dunque

$$(a, b) = (a, 0) + (0, b) \in I$$

♣

### A.2.2 Estensione e Contrazione di Ideali

Dati due anelli, ognuno col proprio ideale  $I \subseteq A$  e  $J \subseteq B$ , e un omomorfismo  $f$  tra i due

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \uparrow & & \uparrow \\ I & & J \end{array}$$

Tenendo a mente la proposizione A.3

**Definizione.** Chiamiamo ideale contratto  $J^c$  la sua controimmagine

$$J^c = f^{-1}(J)$$

**Definizione.** Chiamiamo ideale esteso  $I^e$  il generato dalla sua immagine

$$I^e = (f(I))$$

Poiché possiamo spezzare la mappa  $f$  passando per il quoziente

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow \varphi & \\ A/\ker f & & \end{array}$$

e il comportamento degli ideali attraverso la proiezione  $\pi$  è completamente determinato dal Teorema di Corrispondenza (A.4), possiamo limitarci a studiare cosa succede attraverso l'omomorfismo  $\varphi$ , che essendo iniettivo possiamo scambiare con l'omomorfismo di inclusione.

Prendiamo quindi  $A \subseteq B$ , abbiamo

1.  $J^c = J \cap A$
2.  $I^e = (I)$

**Lemma A.9.** La contrazione di un ideale primo è ancora un ideale primo.

*Dimostrazione.*  $J$  è primo se e solo se  $B/J$  è un dominio. Consideriamo la mappa composizione

$$\varphi : A \hookrightarrow B \rightarrow B/J$$

questa è un omomorfismo di nucleo

$$\ker \varphi = J \cap A = J^c$$

Dunque per il primo teorema di omomorfismo esiste un omomorfismo iniettivo

$$A/J^c \hookrightarrow B/J$$

e i sottoanelli di domini sono a loro volta domini. ♣

Teoremi analoghi con ideali massimali, o estensioni, non funzionano.

### A.2.3 Fatti sul radicale

**Definizione.** Dato un ideale  $I \subseteq A$ , chiamo radicale l'insieme

$$\sqrt{I} := \{x \in A \mid x^n \in I\}$$

costituito da tutti gli elementi che, elevati a una qualche potenza finita, cadono in  $I$ .

*Osservazione.* Il radicale  $\sqrt{I}$  è un ideale. Infatti è un sottoinsieme additivamente chiuso

$$a^n \in I, b^m \in I \Rightarrow (a+b)^{n+m} \in I$$

e assorbente per moltiplicazione

$$a^n \in I \Rightarrow (sa)^n = s^n a^n \in sI = I$$

Inoltre, ovviamente, contiene l'ideale di partenza:  $I \subseteq \sqrt{I}$ .

*Osservazione.*  $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ . Infatti grazie alla seguente implicazione

$$I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$$

possiamo scrivere la catena di inclusioni

$$\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$$

dove le prime due inclusioni sono l'inclusione dell'ideale di partenza, mentre l'ultima si ottiene da

$$a^n \in I, b^m \in J \Rightarrow (ab)^{m+n} \in I \cap J$$

Da questo segue anche che  $\sqrt{I} = A$  se e solo se  $I = A$ .

*Osservazione.* Se  $P$  è un ideale primo, allora  $\sqrt{P} = P$ . Infatti se  $x^n \in P$ , ho  $x = x \cdot x \cdots x$  per  $n$  volte e almeno uno dei fattori sta in  $P$

**Lemma A.10.** L'ideale dei nilpotenti è intersezione di tutti gli ideali primi di  $A$

$$\mathcal{N} = \bigcap_{P \subseteq A} P$$

*Dimostrazione.* Chiaramente se  $x$  è nilpotente  $x^n \in P$  per ogni ideale primo  $P$ .

Mostriamo che, viceversa, se  $x$  appartiene a tutti gli ideali primi allora è nilpotente. Ragioniamo per assurdo: fissato  $x$  nell'intersezione, assumiamo

$$x^n \neq 0 \quad \forall n \in \mathbb{N}$$

Consideriamo la famiglia di ideali

$$\mathcal{F} = \{I \subseteq A \mid x^n \notin I \forall n \in \mathbb{N}\}$$

Osserviamo che per ipotesi  $0 \in \mathcal{F}$ , quindi la famiglia non è vuota. Inoltre è induttiva! (L'unione di una catena di ideali è un ideale e la proprietà di famiglia si conserva). Dunque, per il Lemma di Zorn, abbiamo un ideale  $P$  massimale in  $\mathcal{F}$ .

Mostriamo che  $P$  deve essere primo, giungendo all'assurdo. Preso  $ab \in P$  se uno degli ideali

$$P + (a) \quad P + (b)$$

appartenesse alla famiglia  $\mathcal{F}$ , allora sarebbe sottoinsieme di  $P$  (e dunque  $a \in P$ ). Se nessuno dei due appartenesse alla famiglia, allora

$$x^n \in P + (a) \quad x^m \in P + (b)$$

ma

$$x^{n+m} \in (P + (a))(P + (b)) = P$$

che dunque dev'essere primo. ♣

**Teorema A.11.** Ogni radicale è l'intersezione di tutti i primi contenenti l'ideale di partenza

$$\sqrt{I} = \bigcap_{I \subseteq P} P$$

*Dimostrazione.* Il radicale  $\sqrt{I}$  è costituito dai nilpotenti del quoziente  $A/I$ , la tesi segue dal teorema di corrispondenza. ♣

## A.3 Domini

### A.3.1 Campo dei quozienti. $\mathbb{Q}(A)$

**Definizione.** Un insieme  $S$  di elementi di un dominio  $A$  è detto *parte moltiplicativa* se

1. è moltiplicativamente chiuso
2.  $1 \in S$
3.  $0 \notin S$

*Osservazione.*  $A$  è dominio se e solo se  $A - \{0\}$  è parte moltiplicativa.

Costruiamo il campo dei quozienti del dominio  $A$  come il quoziente di  $A \times (A \setminus \{0\})$  per la relazione di equivalenza

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

Denotiamo questo insieme con  $\mathbb{Q}(A)$ . Indichiamo i suoi elementi come  $\frac{a}{b}$  e definiamo la somma e il prodotto in modo che

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

*Osservazione.*  $(\mathbb{Q}(A), +, \cdot)$  sopra definito è un campo e

$$\begin{aligned} q: A &\hookrightarrow \mathbb{Q}(A) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

è omomorfismo iniettivo.

**Teorema A.12.**  $(\mathbb{Q}(A), +, \cdot)$  è il più piccolo campo in cui possiamo immergere  $A$ . Nel senso che l'immersione di  $A$  in un campo  $\mathbb{K}$  si estende all'immersione di  $\mathbb{Q}(A)$  in  $\mathbb{K}$ .

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & \mathbb{K} \\ q \downarrow & \nearrow \bar{\varphi} & \\ \mathbb{Q}(A) & & \end{array}$$

*Dimostrazione.* L'estensione è naturale

$$\bar{\varphi}: \frac{a}{b} \mapsto \varphi(a)\varphi(b)^{-1}$$

Una volta verificato che è un omomorfismo, questo dev'essere necessariamente iniettivo perché  $\mathbb{Q}(A)$  è un campo, pertanto ha solo ideali banali. ♣

### A.3.2 Divisibilità.

In modo naturale, diciamo che  $a \mid b$  se esiste  $c$  tale che  $b = ac$ . E' immediato tradurre la relazione di divisibilità in termini di ideali generati, infatti

$$a \mid b \Leftrightarrow (b) \subseteq (a)$$

**Definizione.** Diciamo che due elementi  $a, a' \in A$  sono *associati* quando si dividono vincendevolmente

$$(a) = (a') \Leftrightarrow a' = au \text{ per } u \in A^\times$$

lo indicheremo con  $a \sim a'$ .

Possiamo definire il MCD tra due elementi  $a, b$  come quegli elementi  $d$  tali che

1.  $d \mid a$  e  $d \mid b$ .
2. Se  $c \mid a$  e  $c \mid b$ , allora  $c \mid d$ .

è immediato osservare che gli MCD di una coppia sono associati.

**Definizione (Primo).** Diciamo che un elemento non invertibile e non nullo  $x \in A \setminus (A^\times \cup \{0\})$  è *primo* se

$$x \mid ab \Rightarrow x \mid a \text{ o } x \mid b$$

**Definizione (Irriducibile).** Diciamo che un elemento non invertibile e non nullo  $x \in A \setminus (A^\times \cup \{0\})$  è *irriducibile* se

$$x = ab \Rightarrow a \in A^\times \text{ o } b \in A^\times$$

I seguenti risultati sono semplicemente la traduzione delle ultime definizioni nel linguaggio degli ideali:

**Teorema A.13.** Un elemento  $x$  è primo se e solo se l'ideale da lui generato  $(x)$  è primo e non banale.

$$x \text{ è primo} \Leftrightarrow (x) \text{ è primo} \neq \{0\}$$

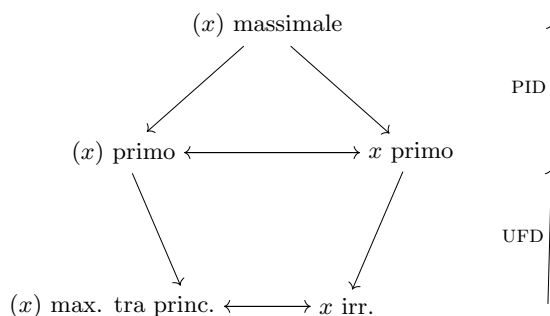
Un elemento  $x$  è massimale se e solo se l'ideale da lui generato  $(x)$  è massimale tra i principali.

$$x \text{ è irriducibile} \Leftrightarrow (x) \text{ è massimale tra i principali}$$

**Teorema A.14.** Ogni elemento primo è anche irriducibile.

$$x \text{ è primo} \Rightarrow x \text{ è irriducibile}$$

Riassumiamo in uno schemino tutte le relazioni legate alla divisibilità:



## A.4 Domini Speciali

Diamo un po' di definizioni insieme

**Definizione.** Ci piacciono i seguenti domini speciali:

(UFD): Ogni elemento non nullo e non invertibile si scrive in modo unico come prodotto di irriducibili.

(PID): Tutti gli ideali sono principali.

(ED): Esiste una funzione grado

$$d : A \setminus \{0\} \rightarrow \mathbb{N}$$

tale che

1.  $d(a) \leq d(ab)$  su tutti i valori in cui è definita.
2. Presi comunque due elementi  $a, b$  con  $b \neq 0$  esistono  $q, r$  tali che

$$a = qb + r$$

e tali che  $d(r) < d(b)$  oppure  $r = 0$ .

**Teorema A.15.** Vale la seguente catena di implicazioni

$$(ED) \Rightarrow (PID) \Rightarrow (UFD)$$

*Dimostrazione.* Segue dai lemmi A.17 e A.20. ♣

**Esempi e Controesempi.**

1.  $\mathbb{Z}$  con la funzione  $|\cdot|$  è un dominio euclideo.
2.  $\mathbb{K}[x]$  con la funzione  $\deg(\cdot)$  è un dominio euclideo.
3.  $\mathbb{Z}[i]$  con la norma  $N(x) = x\bar{x}$  è un dominio euclideo.
4.  $\mathbb{K}[[x]]$  con la funzione  $\deg(f) = \min\{n \in \mathbb{N} \mid a_n \neq 0\}$  è un dominio euclideo.
5.  $\mathbb{Z}[x]$  è UFD ma non è PID.
6.  $\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]$  è PID ma non ED.

### A.4.1 Dominio Euclideo

**Lemma A.16.** Gli elementi invertibili sono tutti e soli quelli di grado minimo.

*Dimostrazione.* Osserviamo innanzitutto che ha senso parlare di grado minimo, poiché l'immagine del grado è un sottoinsieme non vuoto dei naturali.

Se  $x$  è invertibile, per ogni  $a \in A$  non nullo

$$d(x) \leq d(x \cdot ax^{-1}) = d(a).$$

Viceversa, sia  $x$  un elemento di grado minimo e  $a$  un elemento qualunque. Abbiamo che

$$a = qx + r$$

e, escludendo  $d(r) < d(x)$ , dobbiamo avere che  $r = 0$ . Quindi  $x$  divide ogni elemento ed è pertanto invertibile. ♣

**MCD.** Esiste il MCD e lo possiamo calcolare con l'algoritmo di Euclide.

**Lemma A.17.** Abbiamo che  $ED \Rightarrow PID$ .

*Dimostrazione.* Prendiamo un ideale  $I$  di un ED e sia  $x$  il suo elemento di grado minimo. Vogliamo dimostrare che

$$I = (x)$$

per assurdo. Supponiamo che esista  $y \in I$  tale che

$$x = qy + r$$

con  $r \neq 0$ , abbiamo allora necessariamente che  $d(r) < d(x)$ . Purtroppo però

$$r = x - qy \in I$$

contraddice la minimalità di  $x$ . ♣

### A.4.2 Dominio a Ideali Principali

**MCD.** Il MCD( $a, b$ ) esiste: è il generatore dell'ideale

$$(a, b) = (d)$$

**Teorema A.18.** Gli ideali primi sono anche massimali.

*Dimostrazione.*

$$(x) \text{ primo} \Rightarrow x \text{ è un elemento primo} \quad (\text{A.13})$$

$$\Rightarrow x \text{ è irriducibile} \quad (\text{A.14})$$

$$\Rightarrow (x) \text{ è massimale tra gli ideali primi} \quad (\text{A.13})$$

$$\Rightarrow (x) \text{ è massimale} \quad (\text{PID})$$

♣

*Osservazione.* Ripercorrendo la catena di implicazioni sopra, ci si accorge che abbiamo mostrato anche l'equivalenza tra le definizioni di irriducibile e primo nei PID.

### A.4.3 Dominio a Fattorizzazione Unica

**MCD.** Negli anelli UFD l'MCD( $a, b$ ) esiste, perché possiamo caratterizzarlo attraverso la fattorizzazione, come sugli interi. Però non è detto che appartenga all'ideale  $(a, b)$ . Per esempio: in  $\mathbb{Z}[x]$  abbiamo che  $(2, x) = 1$  ma non esistono polinomi  $f, g$  tali che

$$1 = 2f + xg$$

infatti valutando l'espressione in 0 otteniamo  $1 = 2f(0)$ .

**Teorema A.19** (Caratterizzazione degli UFD). Un dominio  $A$  è UFD se e solo se valgono le seguenti condizioni

1. irriducibile  $\Rightarrow$  primo

2. Ogni catena discendente di divisibilità è stazionaria.

*Dimostrazione.* Cominciamo con la freccia più interessante, ovvero che ogni elemento di un anello con le suddette proprietà ammette fattorizzazione unica.

La proprietà 2 ci garantisce l'esistenza della fattorizzazione. Ragioniamo per assurdo: prendiamo  $x \in A \setminus (A^\times \cup \{0\})$  e supponiamo che non ammetta fattorizzazione. Non può essere irriducibile, altrimenti avremmo trovato una fattorizzazione, pertanto si può scrivere come

$$x = y_0 z_0 \quad \text{con } y_0, z_0 \notin A^\times$$

Però questa non può essere una fattorizzazione, pertanto uno dei due non è né irriducibile né fattorizzabile, diciamo  $y_0$ . Allora lo possiamo scrivere come

$$y_0 = y_1 z_1$$

e trovandoci nelle stesse ipotesi di prima, possiamo iterare il procedimento indefinitamente, ottenendo

$$\cdots \mid y_2 \mid y_1 \mid y_0$$

una catena discendente infinita e non stazionaria, assurdo.

*La proprietà 1 ci garantisce l'unicità della fattorizzazione.* Procediamo per induzione forte sulla lunghezza minima  $l_x$  della fattorizzazione di un certo elemento  $x$ . Se  $l_x = 1$  e

$$p = x = q_1 \cdots q_s$$

poiché  $p$  è irriducibile, tutti i  $q_i$  tranne uno sono invertibili e quello che si salva non può che essere associato a  $p$ . Supponiamo ora che tutti gli elementi per cui  $l_x < n$  abbiamo fattorizzazione unica e prendiamo un elemento  $x$  tale che  $l_x = n$ . Allora prese

$$p_1 \cdots p_n = x = q_1 \cdots q_s$$

sappiamo che  $p_n$  è irriducibile e quindi primo, dunque

$$p_n \mid q_1 \cdots q_s \Rightarrow \text{WLOG } p_n \mid q_s$$

poiché anche  $q_n$  è irriducibile e quindi primo, devono essere associati. Pertanto dobbiamo avere che

$$p_1 \cdots p_{n-1} = \tilde{x} = q_1 \cdots q_{s-1}$$

ma le due fattorizzazione sono uguali per ipotesi induttiva, poiché  $l_{\tilde{x}} \leq n-1 < n$ .

*Viceversa*, se  $A$  è UFD, presa una catena discendente di divisibilità

$$\cdots \mid a_2 \mid a_1 \mid a_0$$

possiamo considerare gli insiemi  $A_n$  di tutti i fattori di  $a_n$  presi con molteplicità e osservare che la catena discendente

$$\cdots \subseteq A_2 \subseteq A_1 \subseteq A_0$$

si stabilizza, perché le cardinalità corrispondenti formano una catena discendente di interi. Inoltre, preso un elemento irriducibile  $x$ , se

$$x \mid ab$$

un associato di  $x$  deve comparire nella fattorizzazione di almeno uno tra  $a$  e  $b$ , quindi  $x$  divide almeno uno dei due e pertanto soddisfa la definizione di elemento primo. ♣

**Lemma A.20.** *Segue che PID  $\Rightarrow$  UFD.*

*Dimostrazione.* La prima condizione l'abbiamo già mostrata. Presa una catena discendente di divisibilità, possiamo tradurla in una catena ascendente di ideali

$$(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots$$

Però l'ideale  $I = \bigcup (a_i)$  è generato da un elemento  $a$ , perché tutti gli ideali sono principali. Ma per come è definito  $I$ , l'elemento  $a$  già apparteneva a un certo  $(a_n)$ , generando lui come tutti i suoi successori. ♣

**Esempi.**

1.  $\mathbb{K}[x, \sqrt{x}, \sqrt[3]{x}, \dots]$  non è UFD. Infatti

$$\cdots \mid \sqrt[8]{x} \mid \sqrt[4]{x} \mid \sqrt[2]{x} \mid x$$

è una catena discendente infinita di divisibilità.

2.  $\mathbb{Z}[\sqrt{-5}]$  non è UFD. Infatti 2 è irriducibile ma non primo. Se

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

in norma abbiamo una contraddizione, mentre

$$(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = 2 \cdot 3$$

dunque

$$2 \mid (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

ma

$$4 = N(2) \nmid N(1 \pm \sqrt{-5}) = 6$$

**Definizione.** Chiamiamo *contenuto* del polinomio  $f \in A[x]$  l'MCD dei suoi coefficienti

$$c: A[x] \rightarrow A$$

$$a_0 + \cdots + a_n x^n \mapsto \text{MCD}(a_0, \dots, a_n)$$

**Definizione.** Chiamiamo *primitivo* un polinomio  $f$  con contenuto unitario

$$c(f) = 1$$

**Teorema A.21** (Lemma di Gauss). *In ogni anello  $A[x]$ :*

1. *Il prodotto di polinomi primitivi è primitivo.*
2. *La funzione contenuto è completamente moltiplicativa.*
3. *Se  $f \in A[x]$  e  $f = hg$  in  $\mathbb{Q}(A)[x]$ , esistono  $h_1, g_1 \in A[x]$ , con lo stesso grado di  $h$  e  $g$ , tali che  $f = h_1 g_1$ .*

*Dimostrazione.* Prendiamo due polinomi  $h, g \in A[x]$  il cui prodotto non è primitivo e mostriamo che almeno uno dei due non è primitivo. Se  $hg$  non è primitivo, possiamo trovare un primo  $\pi$  di  $A$  tale che

$$\pi \mid hg \quad \text{in } A[x]$$

e ridurci a ragionare nell'anello  $A_{(\pi)}[x]$ , dove

$$\bar{h}\bar{g} = \overline{hg} = 0$$

Dalle considerazioni fatte sui divisori di zero all'inizio del capitolo, segue che l'anello dei polinomi costruito su un dominio è a sua volta un dominio, pertanto possiamo assumere, senza perdita di generalità

$$\bar{h} = 0 \Rightarrow \pi \mid h \Rightarrow \pi \mid c(h)$$

da cui segue il primo punto.

Il secondo punto segue subito dal primo, separando ogni polinomio  $f$  in parte primitiva e contenuto:

$$f = c(f)\tilde{f}$$

Per il terzo punto, riscriviamo  $g$  e  $h$  facendo minimo comune multiplo, in modo che

$$g = \frac{\tilde{g}}{d}, \quad h = \frac{\tilde{h}}{d'} \quad \text{con } d, d' \in A \text{ e } \tilde{g}, \tilde{h} \in A[x]$$

sapendo che

$$\tilde{g}\tilde{h} = dd'f$$

visto  $\tilde{g}$  e  $\tilde{h}$  sono primitivi, anche  $dd'f$  lo deve essere e, pertanto,  $dd' \in A^\times$ . In questo modo i polinomi tildati devono avere coefficienti in  $A$ . temo che questo punto abbia bisogno di più attenzioni. ♣

**Teorema A.22.**  $A$  è UFD  $\Rightarrow A[x]$  è UFD

*Dimostrazione.* Vogliamo utilizzare la caratterizzazione dei domini a fattorizzazione unica (A.19). Iniziamo verificando che dato un polinomio  $f \in A[x]$  irriducibile, questo è anche primo. Ovviamente

$$c(f) \mid f \Rightarrow c(f) = f \text{ o } c(f) = 1$$

Se  $c(f) = f$ , allora  $f \in A$  e necessariamente  $f$  dev'essere irriducibile in  $A$ . Se  $c(f) = 1$ , allora  $f$  è primitivo e deve necessariamente essere irriducibile anche in  $\mathbb{Q}(A)[x]$ , altrimenti potremmo riportare la decomposizione in  $A[x]$  mediante il Lemma di Gauss. Essendo  $\mathbb{Q}(A)[x]$  un ED,  $f$  è anche primo, lì dentro. L'ideale primo generato da  $f$  si contrae a un ideale primo in  $A[x]$ , dunque  $f$  è primo anche nell'anello in esame. Riassumendo:

$$f \text{ irriducibile in } A[x] \Rightarrow f \text{ irriducibile in } \mathbb{Q}(A)[x] \quad (\text{A.21})$$

$$\Rightarrow f \text{ primo in } \mathbb{Q}(A)[x] \quad (\text{A.18})$$

$$\Rightarrow f \text{ primo in } A[x] \quad (\text{A.9})$$

Mostriamo ora che ogni catena discendente di divisibilità è stazionaria. Prendiamo una sequenza di polinomi  $\{f_n\}$  tale che

$$\cdots \mid f_3 \mid f_2 \mid f_1 \mid f_0$$

Possiamo decomporre ogni polinomio nel prodotto della parte primitiva per il contenuto

$$f = c(f)f'$$

e, osservando che la relazione di divisibilità è soddisfatta se e solo se lo è per componenti

$$f \mid g \Leftrightarrow c(f) \mid c(g) \text{ e } f' \mid g',$$

ci riduciamo a contemplare due diverse catene discendenti di divisibilità

$$\cdots \mid c(f_3) \mid c(f_2) \mid c(f_1) \mid c(f_0)$$

stazionaria perché  $A$  è UFD

$$\cdots \mid f'_3 \mid f'_2 \mid f'_1 \mid f'_0$$

stazionaria perché  $\mathbb{Q}(A)[x]$  è UFD. ♣

**Teorema A.23** (Criterio di Eisenstein). Dato  $f \in A[x]$  primitivo e  $p \in A$  primo, se

1.  $p \nmid a_n$ .
2.  $p \mid a_i$  per  $0 \leq i \leq n-1$ .
3.  $p^2 \nmid a_0$

allora  $f$  è irriducibile.

*Dimostrazione.* Ragioniamo per assurdo. Se il nostro polinomio si decomponesse in

$$f = gh$$

guardando questa relazione in  $A/(p)[x]$  scopriamo che

$$a_n x^n = \bar{f} = \bar{h}\bar{g} = \bar{h}\bar{g}$$

e dunque  $\bar{0} = \bar{h}_0 \bar{g}_0 = \bar{h}_0 \bar{g}_0$ , che significa

$$p \mid h_0 \text{ e } p \mid g_0 \Rightarrow p^2 \mid h_0 g_0 = a_0$$

il che contraddice le ipotesi! ♣

**Esempi.**

1. In  $\mathbb{K}[x][t]$ , l'elemento  $f = t^n - x$  è irriducibile per il criterio di Eisenstein con  $p = x$ .
2.  $\mathbb{K}[\{x_i\}_{i \in \mathbb{N}}]$  non è Noetheriano

$$(x_0) \subsetneq (x_0, x_1) \subsetneq (x_0, x_1, x_2) \subsetneq \dots$$

ma è UFD. Infatti preso un polinomio  $f$ , questo è composto da un numero finito di addendi di grado finito, quindi è contenuto in  $\mathbb{K}[x_1, \dots, x_m]$  per un qualche intero  $m$ , che è un ED. Qui dentro ammette fattorizzazione unica. Inoltre, nella fattorizzazione non compaiono termini del tipo  $x_k$  con  $k > m$ : se così fosse, guardandoli come polinomi in  $x_k$ , non sarebbero rispettate le condizioni sulla funzione grado in  $\mathbb{K}[x_1, \dots, x_k]$ .

## K Teoria dei Campi e di Galois

### K.1 Richiami

**Definizione.** Data un'estensione di campi  $K \subseteq L$  (o anche  $L/K$ ), un elemento  $\alpha \in L$  si dice *algebrico* su  $K$  quando

$$\exists f \in K[x] \quad \text{tale che} \quad f(\alpha) = 0$$

Un elemento si dice *trascendente* se non è algebrico.

**Definizione.** Un'estensione di campi  $K \subseteq L$  si dice *algebraica* quando ogni elemento di  $L$  è algebrico su  $K$

**Definizione.** L'indice di un'estensione

$$[L : K]$$

è la dimensione di  $L$  visto come  $K$  spazio vettoriale.

**Definizione.** Diciamo che un'estensione  $K \subseteq L$  è *semplice* se esiste un elemento  $\alpha \in L$  tale che

$$L = K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[x] \quad g(x) \neq 0 \right\}$$

Possiamo costruire l'estensione semplice a partire dall'anello dei polinomi su  $K$ , applicandovi l'omomorfismo di valutazione in  $\alpha$

$$\begin{aligned} \varphi_\alpha: K[x] &\rightarrow K[\alpha] \subseteq L \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

l'immagine  $K[\alpha]$  è un sottoanello di un campo ed è quindi un dominio, di cui possiamo costruire il campo dei quozienti

$$\mathbb{Q}(K[\alpha]) = K(\alpha)$$

Possiamo però mostrare che, se  $\alpha$  è algebrico, questa operazione non è necessaria. Infatti, il nucleo dell'omomorfismo di valutazione è costituito da tutti quei polinomi che si annullano in  $\alpha$ , i quali costituiscono un ideale principale (perché  $K[x]$  è ED, dunque PID):

$$\ker \varphi_\alpha = (\mu(x))$$

Abbiamo già osservato che l'immagine è un dominio, dunque  $(\mu(x))$  è un'ideale primo (A.6). Abbiamo

$$K[\alpha] \cong \frac{K[x]}{(\mu(x))}$$

Ma, poiché ci troviamo in un PID,  $(\mu(x))$  è anche un ideale massimale (A.18) e dunque  $K[\alpha]$  è un campo, che coincide con il proprio campo dei quozienti:

$$K[\alpha] = \mathbb{Q}(K[\alpha]) = K(\alpha)$$

In questo caso, dobbiamo avere anche che  $\mu(x)$  è un polinomio irriducibile, possiamo quindi scegliere un rappresentante privilegiato tra i generatori del nucleo:

**Definizione.** Chiamiamo *polinomio minimo* di  $\alpha$  l'unico generatore monico di  $\ker \varphi_\alpha$ , che indicheremo con  $\mu_\alpha$ :

$$\ker \varphi_\alpha = (\mu_\alpha(x))$$

**Osservazione.** Nel caso di estensioni algebriche semplici

$$[K(\alpha) : K] = \deg \mu_\alpha$$

questo perché  $K[\alpha]$  è un  $K$ -spazio vettoriale di base

$$1, \alpha, \dots, \alpha^{\deg \mu_\alpha - 1}$$

**Definizione.** Dato un insieme  $S \subseteq L$  definiamo

$$K(S) = \bigcap_{K, S \subseteq F \subseteq L} F$$

**Definizione.** Chiamiamo *Torre di Estensioni* una catena di inclusioni tra campi

$$K \subseteq F \subseteq L \quad \text{o anche} \quad \begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

Elenchiamo ora una serie di proprietà delle torri di estensioni:

**Lemma K.1.**  $L/K$  è finita  $\Leftrightarrow L/F$  e  $F/K$  sono finite

$$\text{e in tal caso } [L : K] = [L : F][F : K]$$

**Dimostrazione.** è un conto sulle dimensioni come spazi vettoriali. ♣

**Lemma K.2.**  $L/K$  è finita  $\Rightarrow L/K$  è algebrica.

**Dimostrazione.** Diciamo  $[L : K] = n$ . Preso un elemento  $\alpha \in L$ , le sue potenze

$$1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^n$$

sono troppe per essere linearmente indipendenti, quindi esistono  $a_0, \dots, a_n \in K$  tali che

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$$

che possiamo leggere come l'annullarsi del polinomio

$$a_0 + a_1x + \dots + a_nx^n \in K[x]$$

nel nostro elemento  $\alpha$ . ♣

**Osservazione.** Il viceversa è falso! L'estensione  $[\bar{\mathbb{Q}} : \mathbb{Q}]$  ha dimensione infinita, perché devono starci, per dire, tutte le radici dell'unità.

Tuttavia, aggiungendo un'ipotesi riusciamo a invertire il risultato:

**Lemma K.3.**  $L/K$  algebrica e finitamente generata  $\Rightarrow$  finita.

**Dimostrazione.** Aggiungendo un elemento per volta,

$$K = K(\alpha_1) = K(\alpha_1, \alpha_2) = \dots = K(\alpha_1, \dots, \alpha_n) = L$$

l'estensione ottenuta è sempre finita per il lemma K.1. ♣



**Lemma K.4.**  $L/K$  algebrica  $\Leftrightarrow L/F$  e  $F/K$  algebriche.

*Dimostrazione.*  $\Rightarrow$ . Un polinomio a coefficienti in  $K$  ha, a maggior ragione, coefficienti in  $F$ , quindi  $L/F$  è automaticamente algebrica. Analogamente, ogni elemento in  $F$  è anche un elemento di  $L$ , quindi è algebrico su  $K$ .

$\Leftarrow$ . Preso un elemento  $\alpha$  di  $L$ , troviamo un polinomio a coefficienti in  $F$

$$\mu = a_0 + a_1x + \cdots + a_nx^n$$

su cui si annulla. A questo punto, possiamo costruire la sottoestensione

$$F_0 = K(a_0, \dots, a_n) \subseteq F$$

che, essendo finitamente generata, ci permette di invocare il lemma K.3 per concludere che è algebrica! Infine, possiamo aggiungere ad  $F_0$  la radice di  $\mu$  da cui siamo partiti, producendo un'altra estensione finita

$$K = F_0 = F_0(\alpha) = L$$

e dunque algebrica. Così, ogni  $\alpha \in L$  è algebrico su  $K$ . ♣

**Definizione.** Un campo  $\Omega$  è detto *algebricamente chiuso* quando ogni polinomio  $f \in \Omega[x]$  ammette almeno una radice in  $\Omega$ .

**Definizione.**  $\overline{\Omega}$  è detta *chiusura algebrica* di  $\Omega$  se:

1.  $\overline{\Omega}$  è algebricamente chiuso.
2.  $\overline{\Omega}/\Omega$  è algebrica.

**Teorema K.5** ( $\exists! \overline{K}$ ). Ogni campo  $K$  ammette una chiusura algebrica  $\overline{K}$  e ogni due sue chiusure  $\overline{K}, \overline{\overline{K}}$  sono  $K$ -isomorfe, ovvero esiste un isomorfismo

$$\varphi : \overline{K} \rightarrow \overline{\overline{K}}$$

tale che  $\varphi|_K = id$ .

## K.2 Separabilità

**Teorema K.6** (di immersione). *Sia  $K(\alpha)/K$  un'estensione algebrica semplice. Ogni immersione*

$$\varphi : K \hookrightarrow \bar{K}$$

*ammette esattamente tante estensioni a un omomorfismo*

$$\tilde{\varphi} : K(\alpha) \hookrightarrow \bar{K}$$

*quante le radici di  $\varphi(\mu_\alpha)$ .*

*Dimostrazione.* Consideriamo l'estensione algebrica come quoziente

$$K(\alpha) \cong \frac{K[x]}{(\mu_\alpha)}$$

e definiamo l'estensione a partire da  $K[x]$  in modo che

$$\Phi : K[x] \rightarrow \bar{K}$$

$$1 \mapsto 1$$

$$x \mapsto \beta$$

imponendo che il nucleo corrisponda con l'ideale generato dal polinomio minimo di  $\alpha$

$$(\mu_\alpha) = \ker \Phi = \{p \in K[x] \mid \varphi(p)(\beta) = 0\}$$

otteniamo una mappa iniettiva, come cercato. Dobbiamo pertanto scegliere  $\beta$  tra le radici di  $\varphi(\mu_\alpha)$ ; facendolo siamo sicuri che

$$(\mu_\alpha) \subseteq \ker \Phi$$

ed essendo  $(\mu_\alpha)$  massimale e l'immagine non banale (perché stiamo quantomeno immergendo il campo), otteniamo

$$(\mu_\alpha) = \ker \Phi.$$

♣

*Osservazione.* Il teorema si generalizza facilmente per induzione ad estensioni finite. Vale inoltre un risultato analogo per estensioni infinite, che garantisce l'esistenza dell'estensione. La dimostrazione è appena più tecnica; è un'applicazione del Lemma di Zorn sull'insieme delle sottoestensioni per cui riusciamo ad estendere l'immersione.

**Definizione** (Separabile). Un polinomio  $f \in K[x]$  si dice *separabile* se ha tutte le radici distinte in  $\bar{K}$ .

Un'estensione algebrica  $L/K$  si dice *separabile* se, comunque scegliamo  $\alpha \in L$ , il corrispondente polinomio minimo  $\mu_\alpha$  è separabile.

**Teorema K.7** (Criterio della derivata). *Se siamo in caratteristica 0 o su un campo finito, allora tutti i polinomi irriducibili sono separabili.*

*Dimostrazione.* Consideriamo  $f$  assieme alla sua derivata formale  $f'$ . È chiaro, per come è definita la derivata, che  $f$  ha radici multiple se e solo se ha radici in comune con  $f'$ . Consideriamo

$$\text{MCD}(f, f')$$

che, poiché  $f$  è irriducibile, può essere solo 1 o  $f$ .

Osserviamo che l'MCD di due polinomi appartiene all'anello di definizione di questi, dunque, se sono coprimi, trovandoci in un ED

$$\exists g, h \quad fg + f'h = 1$$

lo sono a maggior ragione nell'anello costruito sulla chiusura algebrica. Così, se  $\text{MCD}(f, f') = 1$ , abbiamo finito. Altrimenti dobbiamo avere che  $f' = 0$ , ma è chiaro che, in caratteristica zero, questo non può succedere e, se ci mettiamo in  $\mathbb{F}_p[x]$ , possiamo mostrare che

$$f' = 0 \quad \Rightarrow \quad f = g^p$$

semplicemente scrivendo esplicitamente il polinomio e osservando che tutti i coefficienti che hanno una speranza di essere non-nulli sono quelli dei termini  $x^{pk}$ . ♣

**Teorema K.8** (delle immersioni separabili). *Sia  $K(\alpha)/K$  un'estensione algebrica, di grado  $n$ . Se è separabile, ogni immersione*

$$\varphi : K \hookrightarrow \bar{K}$$

*ammette esattamente  $n$  estensioni.*

*Dimostrazione.* Il grado di  $\mu_\alpha$  è  $n$ , che dunque ammette esattamente  $n$  radici distinte. Il teorema K.6 conclude. ♣

*Osservazione.* Il teorema precedente si generalizza per induzione al caso di estensioni finite.

**Definizione.** In un'estensione algebrica  $L/K$  si dicono *coniugati* di un elemento  $\alpha \in L$ , tutte le soluzioni del polinomio minimo  $\mu_\alpha$ .

*Osservazione.* Le estensioni dell'immersione del teorema di sopra (K.8) sono proprio gli omomorfismi di coniugio  $\varphi_i$ , che mandano  $\alpha_1 \mapsto \alpha_i$ .

**Teorema K.9** (dell'Elemento primitivo). *Ogni estensione separabile finita è semplice.*

*Dimostrazione.* Se  $K$  è un campo finito, il suo gruppo moltiplicativo è ciclico, dunque ogni generatore è primitivo. Rimane il caso in cui  $K$  è infinito. Prendiamo  $E/K$  estensione separabile e finita, dove possiamo assumere che

$$E = K(\alpha, \beta)$$

Consideriamo gli  $n = [E : K]$  omomorfismi di coniugio che ci garantisce il teorema K.8

$$\varphi_1, \dots, \varphi_n : E \rightarrow \bar{K}$$

e costruiamo il polinomio a coefficienti in  $\bar{K}[x]$

$$F(x) = \prod_{i < j} (\varphi_i(\alpha + x\beta) - \varphi_j(\alpha + x\beta)).$$

Osserviamo che questo polinomio non è identicamente nullo

$$F \equiv 0 \quad \Leftrightarrow \quad \exists i \neq j \text{ tale che } \begin{cases} \varphi_i(\alpha) = \varphi_j(\alpha) \\ \varphi_i(\beta) = \varphi_j(\beta) \end{cases}$$

dunque, essendo di grado finito in un campo infinito, ammette una “non radice”  $t \in K$  tale che  $F(t) \neq 0$ , chiamiamo

$$\gamma = \alpha + t\beta$$

Vogliamo mostrare che  $K(\gamma) = K(\alpha, \beta)$ . Il polinomio minimo  $\mu_\gamma$  ha tra le radici almeno

$$\varphi_1(\gamma), \dots, \varphi_n(\gamma)$$

che sono tutti distinti

$$\varphi_i(\gamma) \neq \varphi_j(\gamma) \quad \forall i \neq j$$

altrimenti  $\gamma$  sarebbe soluzione del polinomio  $F$ . Possiamo allora affermare che

$$[K(\gamma) : K] = \deg \mu_\gamma \geq n = [K(\alpha, \beta) : K],$$

e che, avendo  $K(\gamma) \subseteq E$  per costruzione,  $K(\gamma) = E$ . ♣

*Osservazione.* La separabilità si distribuisce in tutte le direzioni lungo le torri di estensioni.

### K.3 Normalità

Introduciamo ora un'altra utile proprietà di alcune estensioni

**Definizione** (Normalità). Un'estensione algebrica  $F/K$  si dice *normale* se, preso comunque un  $K$ -omomorfismo

$$\varphi: F \rightarrow \bar{K} \quad \text{tale che } \varphi|_K = id$$

questo rispetta l'estensione:  $\varphi(F) = F$ .

**Esempi.**

1. Tutte le estensioni di grado 2 sono normali.
2.  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  non è normale.

**Teorema K.10** (normale). *In un'estensione  $F/K$  algebrica e normale, ogni polinomio  $f \in K[x]$  irriducibile e con almeno una radice in  $F$ , ha tutte le radici in  $F$ .*

*Dimostrazione.* Consideriamo tutte le radici che  $f$  ammette in  $\bar{K}$ :  $\alpha_1, \dots, \alpha_n$ . Possiamo assumere senza perdita di generalità che  $\alpha_1 \in F$ . Definiamo i  $K$ -omomorfismi  $\varphi_1, \dots, \varphi_n$  in modo che

$$\begin{aligned} \varphi_i: K(\alpha_1) &\rightarrow \bar{K} \\ \alpha_1 &\mapsto \alpha_i \end{aligned}$$

Possiamo estenderli grazie al teorema K.6 a  $K$ -omomorfismi

$$\tilde{\varphi}_i: F \rightarrow \bar{K}$$

ma  $F/K$  è normale, pertanto

$$\tilde{\varphi}_i(F) = F \quad \forall i \in \{1, \dots, n\}$$

dunque  $\alpha_i \in F$  per ogni  $i$ , come volevamo. ♣

**Teorema K.11** (Caratterizzazione della normalità). *Sia  $F/K$  un'estensione (algebrica) finita. Questa è normale se e solo corrisponde al campo di spezzamento di una famiglia di polinomi in  $K[x]$ .*

*Dimostrazione.*  $\Rightarrow$ . La finitezza ci dice che l'estensione è anche finitamente generata

$$F = K(\alpha_1, \dots, \alpha_n)$$

ci basta dunque prendere la famiglia di polinomi  $\{\mu_{\alpha_i}\}_i$  e, per il teorema precedente, questi polinomi si spezzano in  $F$ .

$\Leftarrow$ . Supponiamo che  $F$  sia il campo di spezzamento della famiglia di polinomi  $\{f_i\}_{i \in I}$ , con radici  $\{\alpha_i, j\}_{i,j}$ . Abbiamo che

$$F = K(\{\alpha_{i,j}\})$$

Preso un  $K$ -automorfismo

$$\varphi: F \rightarrow \bar{K}$$

abbiamo già osservato che questo deve necessariamente permutare i coniugati, dunque sicuramente

$$\varphi(F) \subseteq F$$

ma, visto che  $\varphi$  è iniettivo,  $\varphi(F)$  e  $F$  hanno lo stesso grado e pertanto sono la stessa estensione di  $K$ . ♣

Consideriamo ora il problema del comportamento della normalità attraverso le torri di estensioni

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

e chiediamoci:

- Se  $L/K$  è normale, lo è anche  $L/F$ ?  
Sì! Se  $\varphi$  è un  $F$ -omomorfismo è anche un  $K$ -omomorfismo, che già rispettava l'estensione

$$\varphi(L) = L$$

- Se  $L/K$  è normale, lo è anche  $F/K$ ? No!

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

L'ultimo campo a destra è il luogo in cui  $x^4 - 2$  si spezza, pertanto è normale. Possiamo però costruire un  $K$ -omomorfismo che manda  $\sqrt[4]{2}$  in  $i\sqrt[4]{2}$ .

- Se  $L/F$  e  $F/K$  sono normali, lo è anche  $L/K$ ? No!

$$\mathbb{Q} - \mathbb{Q}(\sqrt{2}) - \mathbb{Q}(\sqrt[4]{2})$$

Abbiamo già osservato che le estensioni di grado due sono normali, purtroppo  $\mathbb{Q}(\sqrt[4]{2})$  non spezza il polinomio minimo  $x^4 - 2$ .

## K.4 Teoria di Galois

**Definizione.** Un'estensione  $E/K$  algebrica si dice *di Galois* se è sia normale che separabile.

(Da qui in avanti svilupperemo la Teoria di Galois per estensioni *finite*, pertanto quando diremo che un'estensione ha questa proprietà, sottintenderemo la finitezza.)

In questo caso il gruppo degli automorfismi

$$\text{Aut}_K(E) = \{\varphi : E \rightarrow E \mid \varphi_K = \text{id}\}$$

per normalità è costituito dalle estensioni delle immersioni di  $K$  nella sua chiusura algebrica

$$\text{Aut}_K(E) = \{\varphi : E \rightarrow \bar{K} \mid \varphi_K = \text{id}\}$$

che, per separabilità, sono tante quante il grado dell'estensione

$$|\text{Aut}_K(E)| = [E : K]$$

e viene chiamato *gruppo di Galois* dell'estensione

$$\text{Gal}(E/K) := \text{Aut}_K(E)$$

Possiamo anche parlare del gruppo di Galois di un polinomio, riferendoci indirettamente al gruppo di Galois dell'estensione corrispondente a quella del suo campo di spezzamento, le due definizioni sono equivalenti per la proposizione K.11.

Pensarla in quest'ottica ci permette di procedere con una piacevole osservazione:

*Osservazione.* Il gruppo di Galois è composto da tutti e soli quegli omomorfismi che coniugano le radici di  $f$ , pertanto

$$\text{Gal}(f) \hookrightarrow S_n$$

Inoltre, se  $f$  è irriducibile, l'azione del gruppo su queste radici è *transitiva*, nel senso che appartengono tutte alla stessa orbita.

**Esempi.**

1. Se  $E/K$  è di grado 2 e separabile, allora è di Galois e

$$\text{Gal}(E/K) \cong \mathbb{Z}_2$$

2.  $\text{Gal}(x^3 - 2) \cong S_3$
3.  $\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}_6$ .
4.  $\text{Gal}(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}) \cong \mathbb{Z}_3$

*Osservazione.* Come si comporta la proprietà di Galois sulle torri? La separabilità si estende in tutte le direzioni, pertanto si comporta tanto male quanto la normalità. In particolare, l'unica proposizione che vale è:

**Lemma K.12.** *Data una torre*

$$K \text{ --- } F \text{ --- } L$$

se  $L/K$  è di Galois, allora anche  $L/F$  è di Galois.

Introduciamo ora due lemmi fondamentali.

**Lemma K.13** (del gruppo logaritmico). *Siano  $E/K$  un'estensione di Galois e  $H < \text{Gal}(E/K)$ , allora*

$$E^H = K \iff H = \text{Gal}(E/K)$$

*Dimostrazione.* Dimostriamo un'implicazione alla volta.

$\Leftarrow$ . Gli elementi di  $H$  fissano  $K$  per definizione, è quindi chiara la prima inclusione

$$K \subseteq E^{\text{Gal}(E/K)}.$$

Inoltre presa un'estensione semplice  $K(\alpha)$  non banale

$$K \subset K(\alpha) \subseteq E$$

esiste un omomorfismo che manda  $\alpha$  in un suo coniugato

$$\varphi : K(\alpha) \rightarrow E \quad \text{tale che } \varphi(\alpha) \neq \alpha$$

che possiamo estendere a un'immersione (K.6)

$$\tilde{\varphi} : E \rightarrow \bar{K} \quad \text{che fissa } E.$$

Abbiamo pertanto scovato un automorfismo  $\tilde{\varphi}|_E \in \text{Gal}(E/K)$  che non fissa  $\alpha$ , che ci costringe ad accettare che

$$E^{\text{Gal}(E/K)} \subseteq K.$$

$\Rightarrow$ . Per il teorema dell'elemento primitivo K.9 possiamo assumere che

$$E = K(\alpha).$$

Consideriamo il polinomio che ha per radici tutti i suoi coniugati


$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$$

e osserviamo che per ogni  $\gamma \in H$  si ha

$$\gamma f = \prod_{\sigma \in H} (x - \gamma\sigma(\alpha)) = \prod_{\gamma\sigma \in H} (x - \gamma\sigma(\alpha)) = f$$

dunque tutti i suoi coefficienti devono essere fissati da ogni elemento di  $H$ , che pertanto vive in  $E^H[x] = K[x]$ . Avendo  $\alpha$  come radice, cade nell'ideale  $(\mu_\alpha)$ , quindi

$$|\text{Gal}(E/K)| = \deg \mu_\alpha \leq \deg f = |H|$$

da cui la tesi. 

**Lemma K.14** (del gruppo all'esponente). *Siano  $E/K$  un'estensione di Galois,  $H < \text{Gal}(E/K)$  e  $\sigma \in \text{Gal}(E/K)$ , allora*

$$\sigma(E^H) = E^{\sigma H \sigma^{-1}}$$

*Dimostrazione.* Ci basta scrivere le definizioni

$$E^{\sigma H \sigma^{-1}} = \{\alpha \in E \mid \sigma \tau \sigma^{-1}(\alpha) = \alpha \quad \forall \tau \in H\}$$

ossia, chiamando  $\beta = \sigma^{-1}(\alpha)$ ,

$$= \{\sigma(\beta) \in E \mid \tau(\beta) = \beta \quad \forall \tau \in H\}$$

ma  $\sigma$  è un automorfismo di  $E$ , pertanto " $\sigma(\beta) \in E$ " mi elenca tutti gli elementi di  $E$ , così che

$$= \sigma(E^H).$$



**Teorema K.15** (di corrispondenza). Sia  $L/K$  un'estensione di Galois finita. La mappa

$$\alpha: \{F \text{ campo} \mid K \subseteq F \subseteq L\} \rightarrow \{H < \mathcal{G}al(L/K)\} \\ F \mapsto \mathcal{G}al(L/F)$$

è bigettiva con inversa

$$\beta: H \mapsto L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$$

Inoltre

$$H < \mathcal{G}al(L/K) \Leftrightarrow L^H/K \text{ è di Galois}$$

e in questo caso

$$\mathcal{G}al(L^H/K) \cong \frac{\mathcal{G}al(L/K)}{\mathcal{G}al(L/L^H)}$$

*Dimostrazione.* Applicando la definizione

$$\alpha(\beta(H)) = \alpha(L^H) = \mathcal{G}al(L/L^H)$$

e usando il lemma K.13 appena dimostrato, abbiamo che

$$(L)^H = L^H \Rightarrow \mathcal{G}al(L/L^H) = H$$

Analogamente

$$\beta(\alpha(F)) = \beta(\mathcal{G}al(L/F)) = L^{\mathcal{G}al(L/F)} = F$$

dove abbiamo il lemma nel senso più naturale.

Per la seconda parte, applichiamo il secondo lemma:

$$H < \mathcal{G}al(L/K) \Leftrightarrow \sigma H \sigma^{-1} = H \quad \forall \sigma \in \mathcal{G}al(L/K) \\ \Leftrightarrow \sigma(L^H) = L^H \quad \forall \sigma \in \mathcal{G}al(L/K)$$

ovvero se e solo se  $L^H$  viene rispettato da tutti i  $K$ -automorfismi di  $L$ , ossia se e soltanto se è a sua volta un'estensione di Galois. In tal caso, ci concentriamo sulla funzione di restrizione

$$\mathbf{res}: \mathcal{G}al(L/K) \rightarrow \mathcal{G}al(L^H/K) \\ \sigma \mapsto \sigma|_{L^H}$$

che è un omomorfismo di nucleo

$$\ker \mathbf{res} = \mathcal{G}al(L/L^H)$$

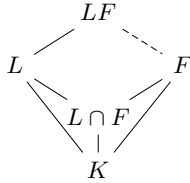
dunque il Primo Teorema di Omomorfismo ci serve la tesi. ♣

## K.5 Relazioni tra estensioni e gruppi di Galois

**Lemma K.16.** Valgono i seguenti fatti:

1.  $H < K \Leftrightarrow L^H \supseteq L^K$
2.  $L^{H \cap K} = L^H L^K$
3.  $L^{\langle H, K \rangle} = L^H \cap L^K$

**Teorema K.17** (dell'estensione a caso). Se  $L/K$  è un'estensione di Galois e  $F/K$  è un'estensione algebrica (tale che entrambe stiano in una qualche sovraestensione?), allora  $LF/F$  è di Galois.



Inoltre

$$\text{Gal}(LF/F) \cong \text{Gal}(L/L \cap F)$$

*Dimostrazione.* Come sempre, la separabilità non ha davvero bisogno di essere controllata, ci concentriamo quindi sulla normalità. Prendiamo un  $F$ -automorfismo  $\varphi$  di  $LF$ . Per la normalità dell'estensione

$$\varphi(L) = L.$$

Sapendo per ipotesi che  $\varphi|_F = \text{id}$ :

$$\varphi(LF) = \varphi(L)\varphi(F) = LF$$

come volevamo. Vogliamo ora far vedere che l'omomorfismo di restrizione

$$\text{res}: \text{Gal}(LF/F) \rightarrow \text{Gal}(L/K)$$

$$\varphi \mapsto \varphi|_L$$

è iniettivo; infatti un  $F$ -omomorfismo che agisce come l'identità su  $L$  è necessariamente banale!

$$\ker \text{res} = \{\varphi \in \text{Gal}(LF/F) \mid \varphi|_L = \text{id}\} = \{\text{id}\}$$

Dunque possiamo identificare il gruppo di Galois appena individuato con un sottogruppo di  $\text{Gal}(L/K)$  e pertanto, per il teorema di corrispondenza K.15 possiamo associarvi un'estensione di  $K$ :

$$L^{\text{res}(\text{Gal}(LF/F))} = L \cap F$$

è chiaro che se un elemento appartiene ad entrambi i campi, vi rimane, perché i  $\varphi$  fissano tutti gli elementi di  $F$  per definizione! Inoltre, se un elemento  $\alpha$  vive in  $L$  ma non in  $F$ , non appartiene sicuramente al campo di partenza  $K \subseteq F$ , quindi ha almeno un coniugato in cui viene mandato da almeno un elemento di  $\text{Gal}(LF/F)$ . O meglio

$$\alpha \in L^{\text{res}(\text{Gal}(LF/F))} \Rightarrow \alpha \in L F^{\text{Gal}(LF/F)} = F$$

per il lemma K.13. Dobbiamo pertanto concludere che

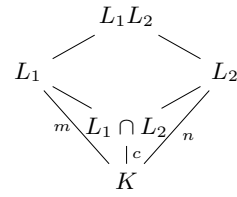
$$\text{res}(\text{Gal}(LF/F)) \cong \text{Gal}(L/L \cap F)$$



**Definizione.** Diciamo che due estensioni  $L_1/K$  e  $L_2/K$  sono *linearmente disgiunte* quando

$$L_1 \cap L_2 = K$$

*Osservazione.* In generale si ha

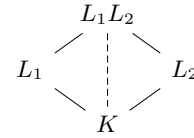


e visto che  $c \mid (m, n)$ , se le due estensioni hanno grado coprimo allora devono essere linearmente disgiunte!

*Osservazione.*  $L_1$  e  $L_2$ , estensioni di Galois, sono linearmente disgiunte se e solo se

$$[L_1 L_2 : K] = [L_1 : K][L_2 : K]$$

**Teorema K.18** (dei prodotti di Galois). Siano  $L_1/K$  e  $L_2/K$  estensioni di Galois, allora l'estensione  $L_1 L_2/K$  è di Galois.



Inoltre

$$\text{Gal}(L_1 L_2/K) \hookrightarrow \text{Gal}(L_1/K) \times \text{Gal}(L_2/K)$$

e questa immersione è un'isomorfismo se e solo se le estensioni di partenza sono linearmente disgiunte.

*Dimostrazione.*  $L_1 L_2/K$  è di Galois: infatti

$$\varphi(L_1 L_2) = \varphi(L_1)\varphi(L_2) = L_1 L_2$$

perché le due estensioni sono normali.

Consideriamo ora l'omomorfismo di restrizione

$$\text{res}: \text{Gal}(L_1 L_2/K) \rightarrow \text{Gal}(L_1/K) \times \text{Gal}(L_2/K)$$

$$\varphi \mapsto (\varphi|_{L_1}, \varphi|_{L_2})$$

che è iniettivo, perché se un'omomorfismo agisce in modo identico su tutti i generatori del campo, lo farà su tutto il campo.

Prendiamo i due sottogruppi  $H_1, H_2 \triangleleft \text{Gal}(L_1 L_2/K)$  tali che

$$(L_1 L_2)^{H_i} = L_i$$

Se supponiamo le due estensioni linearmente disgiunte, allora

$$H_1 \cong \text{Gal}(L_1 L_2/L_1) \cong \text{Gal}(L_2/L_1 \cap L_2) \cong \text{Gal}(L_2/K)$$

usando in mezzo la proposizione K.17. Inoltre

$$H_1 \cap H_2 = \{\text{id}\} \quad \text{e} \quad H_1 H_2 = \text{Gal}(L_1 L_2/K)$$

quindi possiamo applicare il teorema di struttura G.18

$$H_1 \times H_2 \cong \text{Gal}(L_1 L_2/K)$$

il che è equivalente alla suriettività di  $\text{res}$ .

Viceversa, l'isomorfismo ci dice che

$$\langle H_1, H_2 \rangle = \text{Gal}(L_1 L_2/K)$$

e pertanto

$$L_1 \cap L_2 = L_1 L_2^{H_1} \cap L_1 L_2^{H_2} = L_1 L_2^{\langle H_1, H_2 \rangle} = K.$$



### K.5.1 Gruppo di Galois di un ciclotomico

**Teorema K.19** (dei ciclotomici). *Siano  $n$  un intero positivo e  $\xi$  una radice  $n$ -esima primitiva dell'unità, allora*

$$\text{Gal}(\mu_\xi) \cong \mathbb{Z}_n^\times$$

*Dimostrazione.* Iniziamo osservando che tutti i coniugati di  $\xi$  sono radici di

$$f = x^n - 1 = \mu_\xi(x)g(x)$$

Tutte le radici di  $\mu_\xi$  hanno ordine moltiplicativo  $n$  in  $\mathbb{C}^\times$ : per definizione sono i coniugati di  $\xi$ , dunque c'è un isomorfismo che li scambia.

Mostriamo che tutte le radici primitive sono coniugate di  $\xi$ ; anzi, più in generale che per ogni primo  $p$  che non divide  $n$ ,  $\xi^p$  non è una radice di  $g$ , mentre chiaramente è una radice di  $f$ . Se, per assurdo, avessimo che

$$g(\xi^p) = 0$$

allora potremmo ridurci modulo  $p$  per osservare che  $\bar{g}$  ha radici multiple e in comune con  $\bar{\mu}_\xi$

$$\overline{g(x^p)} = \left(\overline{g(x)}\right)^p$$

mentre  $\bar{f}$  non ne ha

$$\bar{f}' = nx^{n-1} \neq 0 \quad \Rightarrow \quad (\bar{f}, \bar{f}') = 1$$

Possiamo così concludere che  $\mu_\xi$  ha come radici tutte e sole le radici  $n$ -esime primitive dell'unità, pertanto

$$\deg \mu_\xi = \phi(n) = |\text{Gal}(\mu_\xi)|$$

Infine, verifichiamo che la mappa

$$\begin{aligned} \Phi: \mathbb{Z}_n^\times &\rightarrow \text{Gal}(\mu_\xi) \\ i &\mapsto \varphi_i: \xi \mapsto \xi^i \end{aligned}$$

è un isomorfismo. ♣

### K.5.2 Gruppo di Galois di un campo finito

**Teorema K.20** (Frobenius). *Dato un primo  $p$  e un intero positivo  $n$*

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \langle \Phi \rangle$$

dove  $\Phi$  è l'automorfismo di Frobenius:

$$\begin{aligned} \Phi: \mathbb{F}_{p^n} &\rightarrow \mathbb{F}_p \\ x &\mapsto x^p \end{aligned}$$

*Dimostrazione.* La mappa  $\Phi$  è un omomorfismo perché

$$\begin{aligned} (a+b)^p &= a^p + b^p \\ (ab)^p &= a^p b^p \end{aligned}$$

e, fissando l'unità, è non banale. Pertanto dev'essere un automorfismo! Dunque abbiamo, quantomeno,

$$\langle \Phi \rangle < \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$$

Inoltre

$$|\langle \Phi \rangle| = n = |\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$$

perché se vale

$$x^{p^m} = x \quad \forall x \in \mathbb{F}_{p^n}$$

dobbiamo avere che il polinomio  $x^{p^m} - x$  ha almeno  $p^n$  radici distinte, quindi ha grado  $p^m \geq p^n$ . Inoltre, per costruzione,

$$x^{p^n} = x \quad \forall x \in \mathbb{F}_{p^n}$$

da cui la tesi. ♣

*Osservazione.* Se volessimo gruppi di galois di estensioni più elaborate, ci basta ricordare che

$$\text{Gal}(\mathbb{F}_{p^{dn}}/\mathbb{F}_{p^d}) < \text{Gal}(\mathbb{F}_{p^{dn}}/\mathbb{F}_p) \cong \langle \Phi \rangle$$

dunque

$$\text{Gal}(\mathbb{F}_{p^{dn}}/\mathbb{F}_{p^d}) \cong \langle \Phi^d \rangle$$

## K.6 Esistenza e unicità della chiusura algebrica

**Teorema K.21** ( $\exists! \bar{K}$ ). *Ogni campo  $K$  ammette una chiusura algebrica  $\bar{K}$  e ogni due sue chiusure  $\bar{K}, \bar{\bar{K}}$  sono  $K$  isomorfe, ovvero esiste un isomorfismo*

$$\varphi: \bar{K} \rightarrow \bar{\bar{K}}$$

tale che  $\varphi|_K = \text{id}$ .

*Dimostrazione.* Concentriamoci sull'esistenza. Prendiamo l'insieme di tutti i polinomi non costanti a coefficienti nel campo in questione e indicizziamoli opportunamente

$$\{p \in K[x] \mid \deg p > 0\} = \{p_\lambda \mid \lambda \in \Lambda\}$$

costruiamo ora l'anello dei polinomi su  $K$  con tante incognite quante i polinomi di  $K[x]$ ; ovvero, chiamato

$$X = \{x_\lambda\}_{\lambda \in \Lambda}$$

consideriamo l'anello

$$K[X]$$

e in questo anello l'ideale

$$I = (p_\lambda(x_\lambda))_{\lambda \in \Lambda} \subseteq K[X]$$

Osserviamo che  $I$  non è massimale, ovvero

$$I \neq (1)$$

se così non fosse avremmo una serie di indici  $\{1, \dots, n\} \subseteq \Lambda$  e coefficienti  $f_1, \dots, f_n \in K[X]$  tali che

$$\sum f_i p_i(x_i) = 1$$

Costruiamo l'estensione

$$L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$$

dove  $\alpha_i$  è una radice di  $p_i$ . Possiamo farlo perché i  $p_i$  sono finiti. Ora abbiamo un bellissimo omomorfismo di valutazione

$$\psi: K[X] \rightarrow L$$

$$1 \mapsto 1$$

$$x_\lambda \mapsto \begin{cases} 0 & \text{se } \lambda \notin \{1, \dots, n\} \\ \alpha_i & \text{se } \lambda = i \in \{1, \dots, n\} \end{cases}$$

che annullando tutti i polinomi considerati ci restituisce

$$1 = \psi(1) = \sum \psi(f_i) \psi(p_i(x_i)) = 0$$

una contraddizione!

Pertanto  $I$  non è massimale, dunque è contenuto in un qualche ideale massimale  $M$  (questo non è banale, abbiamo usato il lemma di Zorn per dimostrare questo lemma A.7)

$$I \subseteq M \subseteq K[X]$$

per cui possiamo porre

$$E_1 = K[X]/_M$$

che è

1. un campo, perché quoziente di un anello per un ideale massimale;
2. contiene  $K$ : essendo l'omomorfismo

$$K \hookrightarrow K[X] \rightarrow E_1$$

non banale perché

$$1 \mapsto 1 \mapsto 1 + M \neq M$$

dev'essere iniettivo.;

3. in cui ogni  $p_\lambda \in K[x]$  ha almeno una radice, infatti

$$p_\lambda(\bar{x}_\lambda) = \overline{p_\lambda(x_\lambda)} = 0$$

Non è però facile dimostrare che  $E_1$  contiene anche le radici dei suoi polinomi, possiamo ovviare al problema costruendo in modo analogo

$$E_2 \subseteq E_3 \subseteq E_4 \subseteq \dots$$

ogni volta infilandoci le radici di tutti i polinomi a coefficienti nel campo precedente. Consideriamo infine il grande campo

$$\Omega = \bigcup_{n \in \mathbb{N}} E_n$$

questo campo sarà algebricamente chiuso perché ogni polinomio di  $\Omega[x]$  ha finiti monomi e pertanto vive in  $E_m$ , per un qualche indice  $m$ , dunque ha radici in  $E_{m+1} \subseteq \Omega$ .

Per concludere, possiamo considerare

$$\bar{K} = \{\alpha \in \Omega \mid \alpha \text{ è algebrico su } K\}$$

e osservare che

1. è un campo: infatti presi  $\alpha, \beta \in \bar{K}$ , abbiamo che

$$\alpha + \beta, \alpha\beta, \alpha^{-1} \in K(\alpha, \beta) \subseteq \bar{K}$$

2. contiene  $K$ : perché stava in  $\Omega$  e tutti i suoi elementi sono banalmente algebrici;
3. è un'estensione algebrica di  $K$ , per definizione;
4. è algebricamente chiuso: preso un qualunque polinomio

$$p(x) \in \bar{K}[x]$$

questo deve vivere in un  $E_m$ , ovvero i coefficienti  $c_0, \dots, c_n$  vivono in  $E_m$ : esiste un'estensione algebrica

$$L = K(c_0, \dots, c_n) \subseteq E_m$$

quindi  $p \in L[x] \subseteq E_m[x]$  deve avere almeno una radice  $\alpha$  in  $E_{m+1}$ , con cui possiamo estendere  $L$  a  $L(\alpha)$ . Per la transitività delle estensioni algebriche sulla torre

$$K \subseteq L \subseteq L(\alpha)$$

scopriamo che  $\alpha \in \Omega$  è algebrico su  $K$  e pertanto appartiene a  $\bar{K}$

che dunque è una chiusura algebrica di  $K$ .

Dimostriamo che è unica. Supponiamo di averne un'altra,  $\bar{\bar{K}}$ . Possiamo immergere il campo  $K$  in una delle sue chiusure

$$\sigma: K \hookrightarrow \bar{K}$$

ed estendere l'immersione all'altra chiusura, grazie alla versione infinita del teorema (K.6), dato che  $\bar{\bar{K}}/K$  è algebrica:

$$\tilde{\sigma}: \bar{\bar{K}} \rightarrow \bar{K}$$

Essendo però  $\tilde{\sigma}(\bar{\bar{K}})$  algebricamente chiusa

$$p(\alpha) = 0 \text{ in } \bar{\bar{K}} \Rightarrow \tilde{\sigma}p(\tilde{\sigma}\alpha) = 0 \text{ in } \bar{K}$$

ogni elemento di  $\bar{\bar{K}}$ , essendo algebrico su  $K$ , è anche un elemento della seconda chiusura  $\bar{K}$ ; pertanto  $\tilde{\sigma}$  è un isomorfismo.





## List of Theorems

|   |    |
|---|----|
| G.1 Teorema . . . . .   | 2  |
| G.4 Teorema (Formula delle Classi) . . . . .                    | 3  |
| G.6 Teorema (di Cauchy) . . . . .                               | 3  |
| G.8 Teorema (Caratterizzazione di $D_n$ ) . . . . .             | 5  |
| G.11 Teorema (Cayley) . . . . .                                 | 6  |
| G.14 Teorema (delle trasposizioni) . . . . .                    | 6  |
| G.16 Teorema . . . . .  | 6  |
| G.17 Teorema (del ribelle) . . . . .                            | 7  |
| G.18 Teorema (di Struttura) . . . . .                           | 8  |
| G.19 Teorema (degli automorfismi prodotto) . . . . .            | 8  |
| G.20 Teorema (dei gruppi solipsisti) . . . . .                  | 9  |
| G.21 Teorema (di decomposizione) . . . . .                      | 10 |
| G.22 Teorema (di Sylow) . . . . .                               | 11 |
| G.23 Teorema . . . . .  | 11 |
| G.24 Teorema (di Struttura dei Gruppi Abelian Finiti) . . . . . | 14 |
| A.2 Teorema (di omomorfismo) . . . . .                          | 17 |
| A.4 Teorema (di corrispondenza) . . . . .                       | 17 |
| A.5 Teorema (cinese degli anelli) . . . . .                     | 17 |
| A.6 Teorema . . . . .   | 18 |
| A.11 Teorema . . . . .  | 19 |
| A.12 Teorema . . . . .  | 20 |
| A.13 Teorema . . . . .  | 20 |
| A.14 Teorema . . . . .  | 20 |
| A.15 Teorema . . . . .  | 21 |
| A.18 Teorema . . . . .  | 21 |
| A.19 Teorema (Caratterizzazione degli UFD) . . . . .            | 21 |
| A.21 Teorema (Lemma di Gauss) . . . . .                         | 22 |
| A.22 Teorema . . . . .  | 23 |
| A.23 Teorema (Criterio di Eisenstein) . . . . .                 | 23 |
| K.5 Teorema ( $\exists! \bar{K}$ ) . . . . .                    | 25 |
| K.6 Teorema (di immersione) . . . . .                           | 26 |
| K.7 Teorema (Criterio della derivata) . . . . .                 | 26 |
| K.8 Teorema (delle immersioni separabili) . . . . .             | 26 |
| K.9 Teorema (dell'Elemento primitivo) . . . . .                 | 26 |
| K.10 Teorema (normale) . . . . .                                | 27 |
| K.11 Teorema (Caratterizzazione della normalità) . . . . .      | 27 |
| K.15 Teorema (di corrispondenza) . . . . .                      | 29 |
| K.17 Teorema (dell'estensione a caso) . . . . .                 | 30 |
| K.18 Teorema (dei prodotti di Galois) . . . . .                 | 30 |
| K.19 Teorema (dei ciclotomici) . . . . .                        | 31 |
| K.20 Teorema (Frobenius) . . . . .                              | 31 |
| K.21 Teorema ( $\exists! \bar{K}$ ) . . . . .                   | 32 |