

le correzioni sono relative ai file:

- Appunti Algebra 1 (versione 0.9.1.3) [\[link\]](#)
- complementi\_algebra (versione 0.0.6.1) [\[link\]](#)

sono stati riportati un'immagine (con il testo interessato evidenziato), un commento e il codice corretto

Legenda:

r. / rr. = riga di codice del file .tex modificato

p. / pp. = pagina del file .pdf

→ = sostituire il termine a sinistra con quello a destra

alcuni “errori” ricorrenti:

- | al posto di \mid negli insiemi (è brutto, viene tutto attaccato)
- non abusare \quad, soprattutto per separare espressioni che costituiscono una proposizione unica è meglio usare spazi più piccoli; è particolarmente evidente in catene di implicazioni:

$$xy = yx \quad \forall x \in G \Rightarrow x \in Z(G)$$

invece di

$$xy = yx \quad \forall x \in G \Rightarrow x \in Z(G)$$

- non esistono solo le virgole :)  
usare altri segni di punteggiatura – specialmente ; – può aiutare a migliorare la leggibilità
- questa è un po’ una fissa mia, ma “tale per cui” non si può sentire
- quando ci sono delle uguaglianze del tipo  $a = b$  e  $b = c$ , per concludere che  $a = c$ , viene scritto  $b = a = c$  anziché  $a = b = c$ , che può creare confusione
- l’indentazione non è male, ma talvolta ci sono interi paragrafi su una solo riga; se avete auto-wrap sull’editor non ve ne accorgrete neanche, ma per compatibilità con altri programmi sarebbe meglio spezzare su più righe
- inoltre è meglio spezzare le righe in punti di cesura (può essere un segno di punteggiatura o anche una pausa implicita), piuttosto che a casaccio

alcune cose generali da ritoccare (se c'avete voglia):

- convenzione consistente per le maiuscole nei titoli:
  - o “all’inglese”, quindi tutte le parole che non sono articoli, congiunzioni e simili hanno l’iniziale maiuscola;
  - o “all’italiana”, quindi solo la prima parola e i nomi propri
- riscrivere tutti i quozienti con \fraktor,  
che è più gradevole di \frac o lo slash /
- riscrivere i simboli di restrizione di funzione come  $\varphi|_K$  ( $\varphi|_{\{K\}}$ ), anziché  $\varphi|_K$  ( $\varphi_{|\{K\}}$ )
- ricontrollare i numeri di teoremi/proposizioni/lemmi/osservazioni

---

## Teoria

---

r. 141; p. 6

**Osservazione 1.7 —** Si ricorda che se  $G/Z(G)$  è ciclico, allora  $G$  è abeliano (e quindi  $G/Z(G)$  è banale), infatti, sia:

$$G/Z(g) = \langle gZ(G) \rangle$$

typo

$$g \rightarrow G$$

$$\backslash [ \ \backslash faktor\{G\}\{Z(G)\} = \backslash left\langle gZ(G)\backslash right\rangle$$

---

r. 202; p. 7

**Osservazione 1.13 —** Si osserva che se  $H$  è l'unico sottogruppo di  $G$  di un certo ordine, allora  $H$  è caratteristico in  $G$  (segue immediatamente dal fatto che gli automorfismi preservano gli ordini degli elementi).

aggiunta

In modo analogo, se  $H$  è caratterizzato da una proprietà conservata da automorfismi, allora è caratteristico.

---

r. 206; p. 7

**Esercizio 1.14.** Il centro di un gruppo,  $Z(G)$  è un sottogruppo caratteristico.

punteggiatura

Il centro di un gruppo  $Z(G)$  è un sottogruppo caratteristico.

---

**Proposizione 1.23 ( $\text{St}(x) \leq G$ )**

Dato un gruppo  $G$  e un'azione  $\varphi : G \rightarrow S(X)$ , si ha che  $\text{St}(x) \leq G$ .<sup>a</sup>

<sup>a</sup>In generale lo stabilizzatore non è un sottogruppo normale.

*Dimostrazione.* Si osserva che  $e \in \text{St}(x)$ , in quanto  $\varphi_e(x) = id(x) = x$ , inoltre, presi  $g, h \in \text{St}(x)$ , ovvero  $\varphi_g(x) = \varphi_h(x) = x$ , allora:

$$\varphi(gh) = \varphi_{gh}(x) = \varphi_g \circ \varphi_h(x) = \varphi_g(\varphi_h(x)) = \varphi_g(x) = x \implies gh \in \text{St}(x)$$

dove si ha che  $\varphi_{gh}(x) = \varphi_g \circ \varphi_h(x)$  in quanto  $\varphi$  è un omomorfismo. Infine, preso  $g \in \text{St}(x)$ , si ha  $g^{-1} \in \text{St}(x)$ , infatti  $\varphi_g$  è bigettiva e quindi ammette inversa:

$$(\varphi_g)^{-1} \circ \varphi_g(x) = x \implies (\varphi_g)^{-1}(\varphi_g(x)) = x \implies (\varphi_g)^{-1}(x) = x$$

con  $(\varphi_g)^{-1}(x) = (\varphi(g))^{-1}(x) = (\varphi(g^{-1}))(x) = \varphi_{g^{-1}}(x)$  e per quanto detto:

$$\varphi_{g^{-1}}(x) = x \implies g^{-1} \in \text{St}(x)$$

typo

$$\varphi(gh) \rightarrow \varphi(gh)(x)$$

```
\[ \varphi(gh)(x) = \varphi_{gh}(x) = \varphi_g \circ \varphi_h(x) = \varphi_g(\varphi_h(x)) = \varphi_g(x) = x \implies gh \in \text{St}(x)
```

che è ben definita e per quanto detto all'inizio è iniettiva:

$$\varphi_g(x) = \varphi_h(x) \iff g \text{St}(x) = h \text{St}(x)$$

(quindi due elementi di un'orbita sono uguali se e solo se le classi laterali dei rispettivi elementi che generano le applicazioni sono uguali modulo  $\text{St}(x)$ , dunque per ogni elemento dell'orbita c'è una classe laterale di  $\text{St}(x)$ ) e surgettiva:

$$\forall y \in \text{Orb}(x), y = \varphi_g(x) \implies g \text{St}(x) \mapsto y$$

lieve riscrittura

(quindi due elementi di un'orbita sono uguali se e solo se le classi laterali modulo  $\text{St}(x)$  dei rispettivi elementi che generano le applicazioni sono uguali, dunque per ogni elemento

dell'orbita c'è una e una sola classe laterale modulo  $\text{St}(x)$ ) e surgettiva:

r. 399; p. 11

**Proposizione 1.25**

Sia  $G$  un gruppo finito e  $X$  un insieme, allora:

$$|G| = |\text{Orb}(x)| |\text{St}(x)| \quad \forall x \in X$$

aggiunto titolo

[Lemma orbita-stabilizzatore]

---

rr. 433, 434; p. 13

Abbiamo già osservato che è un'azione (ovvero che  $\varphi$  è un omomorfismo). In questo caso:

$$\text{Orb}(x) = \{\varphi_g(x) | g \in G\} = \{gxg^{-1} | g \in G\} = \mathcal{C}\ell_G(x)$$

dove  $\mathcal{C}\ell_G(x)$  prende il nome di **classe di coniugio** di  $x$ . Mentre:

$$\text{St}(x) = \{g \in G | \varphi_g(x) = gxg^{-1} = x\} = Z_G(x)$$

dove  $Z_G(x)$  si dice **centralizzatore** di  $x$ . Per quanto detto in precedenza si ha:

$$|G| = |\mathcal{C}\ell_G(x)| |Z_G(x)|$$

aggiunte

dove  $\$Cl_G(x)$  prende il nome di **classe di coniugio** di  $x$  (si indica anche con  $C_x$  quando è chiaro il gruppo). Mentre:

$$\begin{aligned} \{ \text{St}(x) = \{g \in G | \varphi_g(x) = gxg^{-1} = x\} = \{g \in G | gx = xg\} = Z_G(x) \end{aligned}$$

---

r. 448; p. 13

**Osservazione 1.29 —** Osserviamo che  $Z_G(x) = G \iff x \in Z(G)$ , infatti la per un elemento del centro si ha che  $\forall g \in G$  l'elemento commuta, e dunque il suo centralizzatore è tutto il gruppo.

---

rimozione

r. 453; p. 13

**Osservazione 1.30 —** Per un'azione di coniugio si ha che  $x \in Z(G)$  se e solo se  $\text{Orb}(x) = \{x\}$  (ovvero  $\varphi_g(x) = x, \forall g \in G$ ).

aggiunta

Per un'azione di coniugio si ha che  $x \in Z(G)$  se e solo se  $\text{Orb}(x) = \{x\}$  e  $\text{St}(x) = G$  (ovvero  $\varphi_g(x) = x, \forall g \in G$ ).

rr. 479-480; p. 14

$$p^n = |Z(G)| + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \implies |Z(G)| + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \equiv 0 \pmod{p}$$

con  $\frac{|G|}{|Z_G(x)|} > 1$ , poiché se un elemento sta nel centro tutti gli addendi sono 1

per quanto detto, viceversa deve essere che  $\frac{|G|}{|Z_G(x)|} = p^{k_x}, k_x > 0$ , poiché  $G$  è un  $p$ -gruppo, dunque:

$$|Z(G)| \equiv 0 \pmod{p} \implies |Z(G)| \geq 2$$

riscrittura, typo, aggiunta

con  $\frac{|G|}{|Z_G(x)|} > 1$ , poiché  $Z_G(x) = G$  se e solo se  $x \in Z(G)$ ,  
viceversa deve essere che  $\frac{|G|}{|Z_G(x)|} = p^{k_x}, k_x > 0$ , poiché  $G$  è un  $p$ -gruppo (e quindi anche  $Z_G(x)$ ), dunque:

r. 507; p. 15

*Dimostrazione.* Sia  $|G| = pn$ , procediamo per induzione su  $n$ , nel caso  $n = 1$  il teorema è ovvio. Supponiamo vera la tesi per i gruppi di ordine  $pm$ , con  $1 \leq m < n$  e proviamola per  $n$ . Distinguiamo due casi:

- Se esiste  $H \subsetneq G$  con  $p \mid |H|$ , ovvero  $|H| = pm \implies$  vale il teorema di Cauchy per ipotesi induttiva (essendo  $m < n$ ), quindi  $\exists x \in H : \text{ord}_H(x) = p$ , ma essendo  $H \subset G \implies x \in G$  e quindi la tesi è vera.

typo

$$H \rightarrow |H|$$

### §1.7 Azione di coniugio su un sottogruppo

Sia  $X = \{H \leqslant G\}$  e  $\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g(X)$ , con  $\varphi_g : X \longrightarrow X : H \longmapsto gHg^{-1}$ . Si verifica facilmente che  $\varphi$  è un omomorfismo; mostriamo invece che  $\varphi_g$  è una permutazione, per l'iniettività si osserva che:

$$\varphi_g(H) = \varphi_g(K) \iff gHg^{-1} = gKg^{-1} \iff H = K$$

mentre per la surgettività si ha che  $\forall H \in X, \exists L \in X$ :

$$\varphi_g(L) = H \iff gLg^{-1} = H \implies L = g^{-1}Hg$$

typo, aggiunta

$$\begin{aligned} \varphi_g(X) &\rightarrow \varphi_g \\ \Rightarrow &\rightarrow \Leftrightarrow \end{aligned}$$

Si verifica facilmente che  $\varphi_g$  è un omomorfismo; mostriamo invece che  $\varphi_g$  è una permutazione (cioè bigettiva), per l'iniettività si osserva che:

con  $\varphi_g : G \longrightarrow G : x \longmapsto gx$ , l'applicazione  $\lambda$  prende il nome di **rappresentazione regolare a sinistra** di  $G$ , si vuole dimostrare che  $\lambda$  è un omomorfismo iniettivo. Osserviamo innanzitutto che  $\lambda$  è ben definita, cioè  $\varphi_g \in S(G)$ , infatti  $\varphi_g$  è iniettiva (segue dalle leggi di cancellazione) e surgettiva, perché  $\forall y \in G, \exists g^{-1}y \in G : \varphi_g(g^{-1}y) = y$ . Verifichiamo che  $\lambda$  è un omomorfismo:

$$\lambda(g_1g_2) = \varphi_{g_1g_2}$$

rimozione

**Definizione 1.39.** Un'azione  $\lambda$  si dice **fedele** se è iniettiva.

Ad esempio l'azione di rappresentazione regolare a sinistra è fedele:

$$\ker \lambda = \{g \in G \mid \lambda(g) = id\} = \{g \in G \mid \lambda_g(e) = e\} = \{g \in G \mid ge = e\} = \{e\}$$

da cui  $\lambda$  fedele.

## riscrittura

```
\[ \ker \lambda = \{g \in G \mid \lambda(g) = id\} = \{e\}
  \]
infatti $\lambda(e) = \lambda_e = id$ e inoltre
\[ \lambda(g) = \lambda_g = id \sim\implies \lambda_g(e) = e \sim\implies ge = e
\sim\implies g = e
\]
```

Ad esempio l'azione di rappresentazione regolare a sinistra è fedele:

$$\ker \lambda = \{g \in G \mid \lambda(g) = id\} = \{e\}$$

infatti  $\lambda(e) = \lambda_e = id$  e inoltre

$$\lambda(g) = \lambda_g = id \implies \lambda_g(e) = e \implies ge = e \implies g = e$$

da cui  $\lambda$  fedele.

*Dimostrazione.* Si consideri innanzitutto il caso  $d = p^k$ ,  $p$  primo, e mostriamolo per induzione: per  $k = 1$  la tesi è equivalente al [Teorema di Cauchy](#) (anche solo per i gruppi abeliani). Supponiamo la tesi per  $k - 1$ . Poiché in particolare  $p \mid |G|$  scegliamo un sottogruppo  $H$  di  $G$  di ordine  $p$ ; tale sottogruppo è normale poiché  $G$  è abeliano.  $p^{k-1} \mid |G/H| \implies$  per ipotesi induttiva  $\exists K \leq G, |K| = p^{k-1}$ .

Prendendo la controimmagine di  $K$  tramite la proiezione al quoziante troviamo il sottogruppo di  $G$  cercato. A questo punto possiamo scrivere in generale  $d = p_1^{k_1} \dots p_s^{k_s}$ ; per ogni  $i$  troviamo sottogruppi  $H_i$  di ordini  $p_i^{k_i}$  (tutti normali). Si ha quindi che  $H_1 H_2 \leq G$  per normalità, inoltre  $|H_1 \cap H_2| = 1$  poiché l'ordine di un elemento in tale intersezione deve dividere  $(p_1^{k_1}, p_2^{k_2}) = 1$ . Pertanto  $|H_1 H_2| = p_1^{k_1} p_2^{k_2}$ . Ragionando per induzione otteniamo che il sottogruppo  $H_1 \dots H_k$  ha ordine  $d$  come voluto.  $\square$

typo, spostato l'accapo

$$G \rightarrow G/H$$

tale sottogruppo è normale poiché  $G$  è abeliano.  $p^{k-1} \mid |G/H| \implies$  per ipotesi induttiva  $\exists K \leq G/H : |K| = p^{k-1}$ .

Prendendo la controimmagine di  $K$  tramite la proiezione al quoziante troviamo il sottogruppo di  $G$  cercato. A questo punto possiamo scrivere in generale

rr. 686, 696; p. 19

Segue per il teorema di corrispondenza che  $\pi_{Z(G)}^{-1}(\mathcal{H}_i) = H_i \trianglelefteq G$ , ovvero si preserva la normalità dei sottogruppi, inoltre, segue sempre dal teorema che:

$$p^i = [\mathcal{G} : \mathcal{H}_i] = [G : H] = p^i$$

dunque la catena esiste e  $|H_i| = p^{n-i}$  per  $1 \leq i \leq m$ . Essendo  $Z(G)$  abeliano, i sottogruppi di ogni suo ordine (che esistono sempre per il Lemma Di Ranieri) sono normali in  $Z(G)$ , inoltre  $|Z(G)| = p^z$  (dunque si hanno sottogruppi normali di ordine  $p^l$  per  $l \mid z$ ), pertanto esiste la catena:

$$\{e\} = H_n < \dots < H_m = Z(G) \quad \text{con } |H_j| = p^{n-j}, \forall m \leq j \leq n$$

Bisogna infine verificare che  $H_j \trianglelefteq G$ , dunque:

$$gH_jg^{-1} = H_j \quad \forall g \in G$$

ma  $H_j \subset Z(G)$  (sta nel centro, quindi è invariante per coniugio con tutti i  $g \in G$ , e in particolare quelli richiesti) dunque è sempre verificata l'ultima uguaglianza.  $\square$

## rimozione, riscrittura

ma  $H_j \subset Z(G)$  (quindi è invariante per coniugio rispetto a ogni  $g \in G$ ) dunque è sempre verificata l'ultima uguaglianza.

---

r. 729; p. 20

con  $|\text{Orb}(x)| = m_x$ , con  $m_x = \min\{k > 0 \mid \sigma^k(x) = x\}$ , perché se  $\sigma^k(x) = x$ , allora  $\sigma^{k+1}(x) = \sigma(x)$ , pertanto, sia  $k \in \mathbb{N}$  tale che  $\sigma^k(x) \in \{x, \dots, \sigma^{k-1}(x)\}$ , allora  $\exists h :$

$$\sigma^k(x) = \sigma^h(x) \quad \text{con } 0 \leq h < k$$

Dunque vale che  $\sigma^{k-h}(x) = x \in \{x, \dots, \sigma^{k-1}(x)\}$  e per la minimalità di  $k$  si ha che  $h = 0$ . L'azione di  $\langle \sigma \rangle$  su  $X$  divide  $X$  in orbite e su ogni orbita  $\sigma$  agisce ciclicamente (ovvero  $\sigma(\text{Orb}(x)) = \text{Orb}(x)$ ).

## riscrittura

\quad \text{con } 0 \leq h \leq k-1\$

---

**Osservazione 1.49** — Si osserva che:

- Cicli disgiunti commutano.
- L'ordine di una permutazione ciclica è la lunghezza del suo ciclo:

$$\sigma = (x_1, \dots, x_k) \implies \text{ord } \sigma = k$$

quindi  $\sigma^k = id$  e se  $d < k$ , allora  $\sigma^d(x_1) = x_{d+1} \neq x$ .

typo

$$x \rightarrow x_1$$

quindi  $\sigma^k = id$  e se  $d < k$ , allora  $\sigma^d(x_1) = x_{d+1} \neq x$ .

infine, per quanto riguarda le permutazioni ottenute dalla composizione di due 2-cicli, possiamo scegliere e permutare due coppie di elementi, come nei casi precedenti, tuttavia, essendo i cicli disgiunti commutano (banalmente perché lasciano fissi gli altri elementi del dominio), quindi bisogna anche dividere per il numero di scambi per i cicli della stessa lunghezza, ovvero  $2!$  dunque:

$$\binom{4}{2} \frac{2!}{2} \binom{2}{2} \frac{2!}{2} \cdot \frac{1}{2!} = 3$$

e dal conteggio delle permutazioni di  $S_4$  divise per cicli di diversa lunghezza si ottiene:  $6 + 8 + 6 + 3 + 1 = 24 = |S_4|$ .

aggiunta, riscrittura

nei casi precedenti, tuttavia, essendo i cicli disgiunti, questi commutano (banalmente perché lasciano fissi gli altri elementi del dominio), quindi bisogna anche

dividere per il numero di permutazioni dei cicli della stessa lunghezza, ovvero  $2!$  dunque:

e dal conteggio delle permutazioni di  $S_4$  divise per cicli di diversa lunghezza si ottiene:  $1 + 6 + 8 + 6 + 3 = 24 = |S_4|$ .

rr. 851-852; p. 23

*Dimostrazione.* Sia  $\sigma_i$  un  $l_i$ -ciclo, ovvero  $\text{ord } \sigma_i = l_i$ , vogliamo dimostrare che:

$$\text{ord } \sigma = [l_1, \dots, l_k] = d$$

osserviamo che  $\sigma^d = (\sigma_1 \dots \sigma_k)^d = \sigma_1^d \dots \sigma_k^d$ , in quanto i cicli  $\sigma_i$  sono disgiunti (pertanto commutano), essendo  $d = [l_1, \dots, l_k] \implies d \mid l_i, \forall i \in \{1, \dots, k\}$ , pertanto:

$$\sigma^d = \sigma_1^d \dots \sigma_k^d = id \implies \text{ord } \sigma = m \mid d$$

riscrittura

osserviamo che  $\sigma^d = (\sigma_1 \dots \sigma_k)^d = \sigma_1^d \dots \sigma_k^d$ , in quanto i cicli  $\sigma_i$  sono disgiunti (pertanto commutano)  
ed essendo  $d = [l_1, \dots, l_k]$  si ha che  $d \mid l_i, \forall i \in \{1, \dots, k\}$ , pertanto:

---

rr. 873-875; p. 23

*Dimostrazione.* Per dimostrare l'affermazione bisogna mostrare che ogni permutazione è prodotto di trasposizioni (in generale non disgiunte). Poiché ogni permutazione, per quanto affermato nella [Proposizione 1.50](#), è il prodotto di cicli (permute cicliche) disgiunti, è sufficiente mostrare che i cicli sono tutti prodotto di trasposizioni, infatti si può osservare che:

$$(1 \dots k) = (1 \ k)(1 \ k-1) \dots (1 \ 2)$$

dove l'uguaglianza è tra funzioni, quindi ci basta mostrare che danno la stessa immagine. Se  $i > k$ , allora entrambe le funzioni mandano  $i \mapsto i$ , se  $i \leq k$ , allora la funzione a sinistra manda  $i \mapsto i+1$  e  $k \mapsto 1$ , quella a destra lascia fisso  $i$  fino al ciclo  $(1 \ i)$  che manda  $i \mapsto 1 \mapsto i+1$  che rimane fisso in  $i+1$ , mentre  $k \mapsto \dots \mapsto 1$ .  $\square$

riscrittura

```
$i \leq k$, allora la funzione a sinistra manda $i \longmapsto i+1$ e $k \longmapsto 1$; quella a destra lascia fisso $i$ fino al ciclo $\cycle{1,i}$ che manda $i \longmapsto 1$,  
il ciclo $\cycle{1,i+1}$ manda $1 \longmapsto i+1$ e infine i cicli successivi lasciano fisso $i+1$ (quindi complessivamente abbiamo $i \longmapsto i+1$),  
mentre $k$ viene lasciato fisso da tutti i cicli tranne $\cycle{1,k}$, quindi $k \longmapsto 1$.
```

---

Ci resta da verificare che il segno di una trasposizione è  $-1$ . Sia  $\sigma = (a\ b)$ , analizziamo il segno delle varie coppie, distinguendo le seguenti possibilità:

- $\{i, j\} \cap \{a, b\} = \emptyset$ , in tal caso  $\sigma$  lascia fissi gli elementi,  $\sigma(i) = i, \sigma(j) = j \implies \frac{\sigma(i)-\sigma(j)}{i-j} = 1$ .
- $\{i, a\}$  (o  $\{i, b\}$ ), in tal caso  $\frac{\sigma(i)-\sigma(a)}{i-a} = \frac{i-b}{i-a}$ , però vi è anche  $\frac{\sigma(i)-\sigma(b)}{i-b} = \frac{i-a}{i-b}$  e quindi il fattore dà  $1$ .
- Infine, nel caso in cui  $\{i, j\} = \{a, b\}$  si ha:

$$\frac{\sigma(a)-\sigma(b)}{a-b} = \frac{b-a}{a-b} = -1$$

typo, riscrittura

*analizziamo*  $\rightarrow$  *analizzando*

```
\item $\{i,a\}$ con $i \neq b$ (il caso $\{i,b\}$ con $i \neq a$ è analogo),  
in tal caso $\frac{\sigma(i)-\sigma(a)}{i-a} = \frac{i-b}{i-a}$,  
però vi è anche il fattore $\frac{\sigma(i)-\sigma(b)}{i-b} = \frac{i-a}{i-b}$ e il loro prodotto dà $1$.
```

---

Se, invece,  $x \neq b_i$ , a sinistra si ha  $\tau \sigma \underbrace{\tau^{-1}(x)}_{\neq a_1, \dots, a_k}$  (cioè poiché non si parte da alcun  $b_i$ ),

quindi  $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$ , e quindi  $\tau \circ \tau^{-1}(x) = x$ ; a destra invece, non essendo  $x$  alcun  $b_i$  viene lasciato fisso, ciò conclude che le due funzioni sono uguali e che quella a sinistra è quindi un  $k$ -ciclo.

- Mostriamo ora che due permutazioni con la stessa fattorizzazione in cicli disgiunti sono coniugate. Siano:

$$\sigma = (a_1 \dots a_l)(b_1 \dots b_s) \dots (z_1 \dots z_t)$$

$$\rho = (a'_1 \dots a'_l)(b'_1 \dots b'_s) \dots (z'_1 \dots z'_t)$$

per dimostrare la tesi è sufficiente trovare  $\tau \in S_n$  tale che  $\tau \circ \sigma \circ \tau^{-1} = \rho$ . Scegliamo  $\tau$  definita da:

$$\tau(a_i) = a'_i, \tau(b_i) = b'_i, \dots, \tau(z_i) = z'_i$$

ed eventualmente si aggiungono altri elementi. Verifichiamo allora che  $\tau \circ \sigma \circ \tau^{-1} = \rho$ , consideriamo (WLOG) il primo ciclo:

$$a'_i \xrightarrow{\tau^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{\tau} a'_{i+1}$$

e quindi  $a'_i \longmapsto a'_{i+1}$ , pertanto  $\tau \circ \sigma \circ \tau^{-1}$  e  $\rho$  coincidono sempre.

## riscrittura varie, rimossi alcuni simboli di composizione per snellire

Se, invece,  $x \neq b_i$ , a sinistra si ha  $\tau^{-1}(x) \neq a_1, \dots, a_k$  (perché non si parte da alcun  $b_i$ ), quindi  $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$ , e quindi  $\tau \circ \sigma \circ \tau^{-1}(x) = \tau \circ \tau^{-1}(x) = x$ ; a destra invece, essendo  $x \neq b_i$  viene lasciato fisso, ciò conclude che le due funzioni sono uguali e quindi  $\tau \circ \sigma \circ \tau^{-1}$  è un  $k$ -ciclo.

**Esempio 1.66**

In  $S_5$  le classi di coniugio di  $\sigma = (1\ 2)(3\ 4)$  sono  $C_\sigma = \{(a\ b)(c\ d) \in S_5\}$ , con:

$$\#C_\sigma = \frac{\binom{5}{2} \binom{3}{2} 1!1!}{2!} = 15$$

e da ciò si ricava anche che:

$$\#Z_{S_5}(\sigma) = \frac{|S_5|}{|C_\sigma|} = \frac{5!}{15} = 8$$

typo, riscritta la cardinalità con  $|\cdot|$  per coerenza di notazione

*le classi di coniugio ... sono → la classe di coniugio ... è*

**Esempio 1.67**

Sia  $\sigma = (3\ 5)(14) \in S_5$  e sia  $\rho = (1\ 2)(3\ 4)$ , cerchiamo  $\tau \in S_5$  tale che:

$$\tau \circ \sigma \circ \tau^{-1} = \rho$$

si può scegliere  $\tau = (1\ 3)(2\ 5)$ , da cui:

$$(1\ 3)(2\ 5)(3\ 5)(14)(1\ 3)(2\ 5) = (1\ 2)(3\ 4) = \rho$$

aggiungi dei simboli di composizione per chiarezza

```
\[ \cycle{1,3}\cycle{2,5}\circ\cycle{3,5}\cycle{14}\circ\cycle{1,3}\cycle{2,5} = \cycle{1,2}\cycle{3,4} = \rho
```

### Esempio 1.74

Sia  $G$  un gruppo con  $|G| = p^2$ , dalla formula delle classi avevamo ottenuto che  $G$  è necessariamente abeliano, quindi  $G$  è isomorfo a  $\mathbb{Z}/p^2\mathbb{Z}$  o  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ . Se  $G$  è ciclico, allora  $G \cong \mathbb{Z}/p^2\mathbb{Z}$ . Mostriamo che se non lo è, allora  $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  e in questo caso tutti gli elementi di  $G$  hanno ordine  $p$ .

Consideriamo ( $e \neq$ )  $x \in G$  e  $H = \langle x \rangle \trianglelefteq G$  (in quanto  $G$  abeliano); prendiamo  $y \in G \setminus \langle x \rangle$  e analogamente  $K = \langle y \rangle \trianglelefteq G$ , da ciò segue che  $H \cap K = \{e\}$ , infatti  $H$  e  $K$  sono sottogruppi ciclici di  $G$  di ordine  $p$  e quindi hanno in comune solo l'elemento neutro. Osservando infine che  $HK = G$ , per cardinalità:

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2$$

le ipotesi del [Teorema 1.72](#) sono verificate, dunque:

$$G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

riscritto per chiarezza

Osservando infine che per cardinalità  $|HK| = |G|$ :

si dice **prodotto semidiretto** di  $H$  e  $K$  via  $\varphi$ :

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

(o anche  $K_{\varphi} \ltimes H$ ) l'insieme ottenuto come prodotto cartesiano  $H \times K$  con l'operazione definita da:

$$(h, k)(h', k') = (h \cdot_H \varphi_k(h'), k \cdot_K k')$$

riscrittura (credo che la  $\varphi$  stia sempre nel pedice a dx. anche se si inverte il simbolo di semidiretto, altrimenti sembra pedice di K)

(o anche  $K \ltimes_{\{\varphi\}} H$ ) l'insieme ottenuto come prodotto cartesiano  $H \times K$  con l'operazione definita da:

**Osservazione 1.77** — Si osserva che  $H \rtimes_{\varphi} K$  è il prodotto diretto se e solo se  $\varphi_k = e$ ,  $\forall k \in K$ . Infatti:

$$(h, k)(h', k') = (h \cdot \varphi_k(h'), kk') = (hh', kk') \iff \varphi_k(h') = h' \quad \forall k \in K$$

e dunque  $\varphi_k = id_H$ .

typo, aggiunta

Si osserva che  $H \rtimes_{\varphi} K$  è il prodotto diretto se e solo se  $\varphi_k = id_H$ ,  $\forall k \in K$  (cioè  $\varphi$  banale).

---

**Osservazione 1.81 —** Siano  $\overline{H} = H \times \{e_K\}$  e  $\overline{K} = \{e_H\} \times K$ , si osserva che  $\overline{H}, \overline{K} \leq G = H \rtimes_\varphi K$ , infatti sono chiusi per prodotto (ristretto):

$$(h, e_K)(h', e_K) = (h \cdot \varphi_{e_K}(h'), e_K) = (h \cdot id(h'), e_K) = (hh', e_K)$$

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

e si verifica facilmente anche per inverso. Si osserva che  $\overline{H} \trianglelefteq G^{\text{a}}$ , in quanto  $H = \ker \pi$ , con:

$$\pi : H \rtimes_\varphi K \longrightarrow K : (h, k) \longmapsto k$$

con  $\pi$  omomorfismo come si vede:

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

Per come li abbiamo presi si nota subito che  $\overline{HK} = G$  e  $\overline{H} \cap \overline{K} = \{e\}$ , quindi valgono le ipotesi del [Teorema 1.79](#), pertanto:

$$\overline{H} \times \overline{K} \cong G = H \rtimes_\varphi K$$

---

<sup>a</sup> $\overline{K}$  in generale non è normale, lo è solo se il prodotto è diretto, infatti in quel caso vale il [Teorema 1.72](#).

typo

*Teorema 1.79 → Teorema 1.78*

$\times \rightarrow \bowtie$

Per come li abbiamo presi si nota subito che  $\overline{H} \cap \overline{K} = \{e\}$  e  $\overline{H} \times \overline{K} \cong G$ , quindi valgono le ipotesi del [Teorema 1.78](#), pertanto:

$$[\overline{H} \times \overline{K} \cong G = H \rtimes_\varphi K]$$

Forse si può riscrivere meglio (insieme all'Osservazione 1.73):

l'idea è far vedere che non cambia molto tra prodotto interno  $HK$  ed esterno  $H \times K$ .

Infatti, dati  $H, K \trianglelefteq G$  tali che  $H \cap K = \{e\}$  e  $HK = G$ ,

sappiamo che  $G \cong H \times K$ .

Definendo  $\overline{H} = H \times \{e\}$ ,  $\overline{K} = \{e\} \times K$  abbiamo che  $\overline{H} \cap \overline{K} = \{(e, e)\}$  e  $\overline{HK} = H \times K$ .

Quindi  $HK = G \cong H \times K = \overline{HK}$ , cioè  $HK \cong \overline{HK}$ .

(o qualcosa del genere, non so bene se ho scritto quello che volevo dire)

**Esempio 1.82** ( $S_n \cong \mathcal{A}_n \rtimes_{\varphi} \langle (1 2) \rangle$ )

Verifichiamo che  $S_n$  è prodotto semidiretto di  $H = \mathcal{A}_n$  e  $K = \langle (1 2) \rangle$ <sup>a</sup> usando il Teorema 1.78, per quanto detto nel (1) del Corollario 1.68 sappiamo che  $\mathcal{A}_n \triangleleft S_n$ , inoltre, sempre per il punto (1), essendo  $|\mathcal{A}_n| = \frac{n!}{2}$ , segue per cardinalità che  $HK = S_n$ . Essendo  $\mathcal{A}_n = \ker sgn$  e  $\langle (1 2) \rangle$  una trasposizione  $H \cap K = \{e\}$  (in quanto il nucleo dell'omomorfismo segno contiene solo permutazioni pari), pertanto segue la tesi:

$$S_n \cong \mathcal{A}_n \rtimes_{\varphi} \langle (1 2) \rangle$$

Osserviamo inoltre che:

$$\varphi : \langle (1 2) \rangle \longrightarrow \text{Aut}(\mathcal{A}_n) : (1 2) \longmapsto \varphi_{(1 2)}, id \longmapsto id$$

$$\text{con } \varphi_{(1 2)} : \mathcal{A}_n \longrightarrow \mathcal{A}_n : \rho \longmapsto (1 2)\rho(1 2).$$

<sup>a</sup>In generale va bene qualsiasi trasposizione (che esiste sempre in  $S_n$  per  $n \geq 2$ ).

typo, riscrittura

*Corollario 1.68 → Osservazione 1.63*

usando il \hyperref[t:1.78]{Teorema 1.78}, per quanto detto nell'Osservazione 1.63 sappiamo che  $\mathcal{A}_n \triangleleft S_n$  e  $|\mathcal{A}_n| = \frac{n!}{2}$ , segue

per cardinalità che  $HK = S_n$ . Essendo  $\langle (1, 2) \rangle$  una permutazione dispari,  $H \cap K = \{e\}$ , pertanto segue la tesi:

r. 1265; p. 34

Si osserva che  $\text{ord } \varphi_y = \text{ord}_{\mathbb{Z}/q\mathbb{Z}^*}(\bar{l})$  e:

$$\varphi_y(x) = x^l \implies (\varphi_y(x))^k = x^{lk}$$

quindi  $\text{ord } \varphi_y = p \iff l^p \equiv 1 \pmod{q} \iff \text{ord } l = p$ . Le  $p - 1$  scelte per  $\varphi_y$  danno tutte gruppi isomorfi, quindi se  $p \mid q - 1$  ci sono esattamente due gruppi di ordine  $pq$  a meno di isomorfismo. Infatti, detti:

typo

$$(\varphi_y(x))^k \rightarrow (\varphi_y)^k(x)$$

$$\forall \varphi_y(x) = x^l \implies (\varphi_y)^k(x) = x^{l^k}$$

### Esempio 1.90

Classificare i gruppi abeliani di ordine 1000. Per fare ciò osserviamo che  $1000 = 2^3 \cdot 5^3$ , allora:

$$G = G(2) \times G(5)$$

con  $|G(2)| = 2^3$ , e  $|G(5)| = 5^3$  pertanto le  $p$ -componenti possono essere scritte come prodotto di gruppi ciclici nei seguenti modi:

$$G(2) \cong \begin{cases} \mathbb{Z}/2^3\mathbb{Z} \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases} \quad \text{e} \quad G(5) \cong \begin{cases} \mathbb{Z}/5^3\mathbb{Z} \\ \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{cases}$$

Dunque i gruppi abeliani di ordine 1000 (a meno di isomorfismo) sono  $3 \cdot 3 = 9$ , in quanto per il [Teorema di Struttura](#) abbiamo una fattorizzazione unica come prodotto di gruppi cicli finiti, e per tale fattorizzazione abbiamo 3 scelte per la 2-componente e 3 scelte per la 5-componente.

typo

*scritti* → *scritte*

con  $|G(2)| = 2^3$ , e  $|G(5)| = 5^3$  pertanto le  $p$ -componenti possono essere scritte come prodotto di gruppi ciclici nei seguenti modi:

*Dimostrazione.* **Esistenza:** Sia  $|G| = n$ , con  $n = p_1^{e_1} \dots p_s^{e_s}$ , procediamo per induzione su  $s$ . Nel caso in cui  $s = 1$ , si ha  $|G| = p_1^{e_1} \implies G = G(p_1)$ . Supponiamo la tesi vera  $\forall m : 2 \leq m < n$ , possiamo scrivere  $n = mm'$  con  $(m, m') = 1$  e  $m, m' < n$ , allora (in notazione additiva) vogliamo verificare che:

$$G \cong mG \times m'G$$

È facile verificare che  $mG, m'G < G$  (basta vedere la chiusura per l'operazione), ed essendo  $G$  abeliano si ha anche  $mG, m'G \triangleleft G$ ; si osserva inoltre che, essendo  $(m, m') = 1$ , allora  $\exists h, k \in \mathbb{Z}$ :

$$mh + m'k = 1 \implies m(gh) + m'(gk) = g \quad \forall g \in G \implies G \subseteq mG + m'G$$

il contrario è ovvio, dunque:

$$mG + m'G = G$$

## rimozione, tipo, spazio, aggiunta

la tesi vera  $\forall m : 2 \leq m < n$ , possiamo scrivere  $n = m m'^{\prime}$  con  $(m, m'^{\prime}) = 1$  e  $m, m'^{\prime} < n$ , allora vogliamo verificare che:

$$n \rightarrow m'$$

È facile verificare che  $mG, m'^{\prime}G < G$  (basta vedere la chiusura per l'operazione), ed essendo  $G$  abeliano si ha anche  $mG, m'^{\prime}G \triangleleft G$ ; si osserva inoltre che, essendo  $(m, m'^{\prime}) = 1$ , allora  $\exists h, k \in \mathbb{Z}$ :

$$\begin{aligned} mh + m'^{\prime}k = 1 &\implies m(gh) + m'^{\prime}(gk) = g \quad \text{quad} \\ \forall g \in G &\implies G \subseteq mG + m'^{\prime}G \end{aligned}$$

il contrario è ovvio, dunque:

$$\begin{aligned} \forall g \in G &\implies G \subseteq mG + m'^{\prime}G \\ \therefore mG + m'^{\prime}G &= G \end{aligned}$$

dove  $mG + m'^{\prime}G$  è  $mGm'^{\prime}G$  scritto in notazione additiva.

Inoltre, sia  $x \in mG \cap m'G$ , ovvero  $x = mg = m'g'$ , allora si osserva che  $m'x = m'mg = nx = 0$  e  $mx = mm'g' = nx = 0$ , dunque:

$$\text{ord}(x) \mid m \quad \text{e} \quad \text{ord}(x) \mid m' \implies \text{ord}(x) \mid (m, m') = 1 \implies x = 0$$

Quindi  $mG \cap m'G = \{e\}$ , pertanto sono verificate ipotesi del Teorema 1.72, dunque è vero che  $G \cong mG \times m'G$ . Osserviamo che:

$$mG = G_{m'} = \{g \in G \mid m'g = 0\} \quad \text{e} \quad m'G = \{g \in G \mid mg = 0\}$$

Verifichiamo (WLOG)  $m'G = G_m$  mostrando la doppia inclusione tra insiemi;  $m'G \subseteq G_m$ , ovvero  $m'x \in G_m$ , perché  $mm'x = nx = 0$ , viceversa, preso  $x \in G_m$ , ovvero  $mx = 0$ , per quanto visto sopra abbiamo che:

### typo, spazi, aggiunta, punteggiatura

Inoltre, sia  $x \in mG \cap m'G$ , ovvero  $x = mg = m'g$ , allora si osserva che  $m'x = m'mg = ng = 0$  e  $mx = mm'g = ng = 0$ , dunque:  
 $\begin{aligned} & \forall \text{ord}(x) \mid m \quad \text{e} \quad \text{ord}(x) \mid m' \implies \text{ord}(x) \mid (m, m') = 1 \implies x = 0 \end{aligned}$

$\begin{aligned} & \forall mG = G_{m'} = \{g \in G \mid m'g = 0\} \quad \text{e} \quad m'G = G_m = \{g \in G \mid mg = 0\} \\ & \end{aligned}$

Verifichiamo (WLOG)  $m'G = G_m$  mostrando la doppia inclusione tra insiemi;  
 $m'G \subseteq G_m$ , ovvero  $m'g \in G_m \forall g \in G$ , perché  $mg = 0$ , viceversa, preso

rr. 1424, 1429; p. 38

Poiché  $|G_m|, |G_{m'}| < |G|$ , perché  $G_m$  contiene tutti e soli gli elementi di  $G$  di ordine che divide  $m$ , inoltre  $G_m \neq \{0\}$  (per Cauchy, dato che  $1 < m < n$ ), quindi  $G_{m'} \not\leq G$  e viceversa. Possiamo quindi applicare l'ipotesi induttiva e scrivere:

$$G_m = \prod_{i \in I} G(p_i) \quad \text{e} \quad G_{m'} = \prod_{j \in J} G(p_j)$$

con  $I \cup J = \{1, \dots, s\}$  e  $I \cap J = \emptyset$  (poiché  $(m, m') = 1$ ).

Unicità: La scrittura come prodotto di  $p$ -componenti è unica, perché se  $G$  fosse anche isomorfo ad altri  $p$ -gruppi:

$$G \cong H_1 \times \dots \times H_n \quad \text{con } H_i \text{ } p_i\text{-gruppo e } H_i < G$$

riscrittura, typo

$$n \rightarrow s$$

quindi  $G_m, G_{m'} \lneq G$ . Possiamo quindi applicare l'ipotesi induttiva e scrivere:

$\forall [ G \cong H_1 \times \dots \times H_s \quad \text{con } H_i \text{ } p_i\text{-gruppo e } H_i < G ]$

rr. 1439-1440; p. 38

### Lemma 1.91

Sia  $G$  un  $p$ -gruppo abeliano, e sia  $x_1$  un elemento di ordine massimo in  $G$ , preso  $\bar{x} \in G/\langle x_1 \rangle$  esiste  $y \in \pi^{-1}(\bar{x}) : \text{ord}_G(y) = \text{ord}_{G/\langle x_1 \rangle}(\bar{x})$ .

usare \faktor [da vedere, magari è meglio così]

Sia  $G$  un  $p$ -gruppo abeliano, e sia  $x_1$  un elemento di ordine massimo in  $G$ , preso  $\bar{x} \in \overline{G}/\langle x_1 \rangle$  esiste  $y \in \pi^{-1}(\bar{x}) : \text{ord}_G(y) = \text{ord}_{\overline{G}/\langle x_1 \rangle}(\bar{x})$ .

rr. 1443-1457; p. 38

*Dimostrazione.* Osserviamo che  $\pi^{-1}(\bar{x}) = x + \langle x_1 \rangle$ , dunque  $y \in \pi^{-1}(\bar{x})$  è della forma:

$$y = x + ax_1$$

Sappiamo che  $\pi(y) = \pi(x) = \bar{x}$ , allora  $p^r = \text{ord}(\pi(y)) = \text{ord}(\bar{x}) \mid \text{ord}(y)$  (per le proprietà di omomorfismo), scegliamo  $y$  (cioè  $a$ ) in modo che:

$$0 = p^r y = p^r x + p^r a x_1 \iff p^r x = -p^r a x_1$$

dove  $\text{ord}(\bar{x}) = p^r \implies p^r x \in \langle x_1 \rangle \implies p^r x = b x_1$ , tuttavia, dato che  $x_1$  ha ordine massimo  $p^{r_1}$ , deve essere che  $r \leq r_1$ , ma:

$$0 = p^{r_1} x = p^{r_1 - r} p^r x = p^{r_1 - r} b x_1$$

ma  $\text{ord}(x_1) = p^{r_1} \implies p^r \mid b \implies b = p^r b_1$ . Scegliendo  $a = -b_1$  si ha:

$$p^r y = p^r x - p^r b_1 x_1 = b x_1 - \underbrace{p^r b_1}_{=b} x_1 = 0$$

da scrivere meglio (non c'è niente di formalmente sbagliato ma è piuttosto faticosa da leggere)

---

r. 1467; p. 39

*Dimostrazione.* Esistenza: Sia  $G$  un  $p$ -gruppo,  $|G| = p^n$ , proviamo la tesi per induzione su  $n$ . Per  $n = 1$  si ha che  $|G| = p \implies G \cong \mathbb{Z}/p\mathbb{Z}$ , e quindi la tesi è verificata. Supponiamo la tesi vera per  $1 \leq m < n$  e proviamola per  $n$ ; sia  $x_1 \in G$  un elemento di ordine massimo,  $\text{ord}(x_1) = p^{r_1}$ :

- Se  $r_1 = n$ , allora  $G$  è **ciclo**  $\implies G \cong \mathbb{Z}/p^n\mathbb{Z}$ .

typo

*ciclo*  $\rightarrow$  *ciclico*

`\item Se $r\_1 = n$, allora $G$ è ciclico $\implies G \cong \mathbb{Z}\{p^n\}$.`

---

r. 1484; p. 39

è un isomorfismo, infatti  $\pi$  è un omomorfismo, è surgettivo (in quanto si possono mandare tutti i generatori  $x_i$  di  $H$  nelle  $t$ -uple di generatori di  $G/\langle x_1 \rangle$ ); per l'iniettività si osserva che gli elementi del nucleo sono del tipo:

$$\pi(a_2x_2 + \dots + a_tx_t) = (a_2\bar{x}_2, \dots, a_t\bar{x}_t) = (0, \dots, 0) \iff a_i\bar{x}_i = 0 \quad \forall i \in \{2, \dots, t\}$$

cioè se e solo se  $\text{ord}_{G/\langle x_1 \rangle}(\bar{x}_i) = p^{r_i} \mid a_i, \forall i \in \{2, \dots, t\}$ . Segue che  $\pi|_H$  è un isomorfismo e si ha:

$$H \cong \langle \bar{x}_2 \rangle \times \dots \times \langle \bar{x}_t \rangle \cong \langle x_2 \rangle \times \dots \times \langle x_t \rangle$$

da spiegare meglio perché questo implica l'iniettività

---

r. 1506; p. 40

dove supponiamo  $r_1 \geq \dots \geq r_t$  e  $k_1 \geq \dots \geq k_s$ . Deve essere necessariamente che  $t = s$ , perché, considerando:

$$G_p = \{g \in G \mid pg = 0\}$$

con  $G_p$  gruppo caratteristico (poiché gli isomorfismi conservano gli ordini degli elementi) e quindi:

usare \mid

$$\{ g \in G \mid pg = 0 \}$$

---

r. 1556; p. 42

possiamo costruire sottogruppi di ogni ordine<sup>10</sup>; inoltre, dato che  $G$  è abeliano il prodotto di sottogruppi è un sottogruppo:

$$H_{p_1} \dots H_{p_r} < H$$

e inoltre:

$$H_{p_1} \dots H_{p_r} \cong H_{p_1} \times \dots \times H_{p_r}$$

typo

$$H \rightarrow G$$

$$\{ H_{p_1} \dots H_{p_r} \mid p_1, \dots, p_r \in \mathbb{P} \}$$

dunque, se  $p \nmid i \implies p^n m - i$  e  $p^\alpha - i$  non sono divisibili per  $p$ ; se fosse  $i = p^k j$ , con  $(j, p) = 1$ , allora  $p^\alpha - i = p^\alpha - p^k j = p^k \underbrace{(p^{\alpha-k} - j)}_{\text{non divisibile per } p}$ , con  $k < \alpha$ , (analogamente per  $p^n m - i$ ), per quanto abbiamo detto deve essere necessariamente che:

aggiunto un  $\cdot$  per chiarezza

$p^\alpha - i = p^\alpha - p^k j = p^k \cdot \underbrace{(p^{\alpha-k} - j)}_{\text{non divisibile per } p}$ , con  $k < \alpha$ , (analogamente per  $p^n m - i$ ), per quanto abbiamo detto deve essere necessariamente che:

---

unendo ciò a quanto detto si ha che  $p^{n-\alpha} \mid \sum_{i=1}^s \frac{|G|}{|\text{St}(M_i)|}$ , quindi non tutte le orbite possono essere divisibili per una potenza maggiore di  $p^{n-\alpha}$ , ovvero esiste almeno un  $i$  tale per cui  $p^{n-\alpha+1} \nmid |\text{Orb}(M_i)|$  (ovvero non può essere diviso per una potenza più grande di quanto detto), da ciò segue:  $p^{n-\alpha+1} \nmid |\text{Orb}(M_i)| = \frac{|G|}{|\text{St}(M_i)|} = \frac{p^n m}{|\text{St}(M_i)|}$ , pertanto deve essere necessariamente che:

$$p^\alpha \mid |\text{St}(M_i)| = t$$

cioè, affinché il rapporto non sia divisibile per  $p^\alpha$ , al denominatore deve esserci una potenza di  $p$  maggiore o uguale ad  $\alpha$ . D'altra parte, sia  $x \in M_i$ , la funzione:

$$\varphi_x : \text{St}(M_i) \longrightarrow M_i : y \longmapsto yx$$

riscrittura, typo

$$p^\alpha \rightarrow p^{n-\alpha+1}$$

$\$p^{\alpha} - i = p^{\alpha} - p^{kj} = p^k \cdot \underbrace{(p^{\alpha-k} - j)}_{\text{non divisibile per } p},$  con  $k < \alpha$ , (analogamente per  $p^{nm} - i$ ), per quanto abbiamo detto deve essere necessariamente che:

unendo ciò a quanto detto si ha che  $\$p^{n-\alpha} \mid \sum_{i=1}^s |\text{Orb}(M_i)|$ , quindi non tutte le orbite possono essere divisibili per una potenza maggiore di  $p^{n-\alpha}$ , ovvero esiste almeno un  $i$

cioè, affinché il rapporto non sia divisibile per  $p^{n-\alpha+1}$ , al denominatore deve esserci una potenza di  $p$  maggiore o uguale ad  $\alpha$ . D'altra parte, dato  $x \in M_i$ , la funzione

(essendo  $p$ -gruppi). Poiché per ipotesi  $p \nmid m$ , allora esiste  $i$  tale che  $a_i = 0$  (dunque c'è un 1 nella fattorizzazione che impedisce la divisibilità di  $m$  per  $p$ )  $\Rightarrow \text{Orb}(g_iS) = \{g_iS\} \Rightarrow \text{St}(g_iS) = H$  (ovvero per tale  $i$  si ha una classe laterale  $g_iS$  la cui orbita è solo se stessa, e quindi il suo stabilizzatore è tutto  $H$ ). Da ciò segue che  $\forall h \in H$ :

$$hg_iS = g_iS \iff hg_i \in g_iS \iff h \in g_iSg_i^{-1} \iff H \subset g_iSg_i^{-1}$$

typo

*fattorizzazione → somma*

(essendo  $p$ -gruppi). Poiché per ipotesi  $p \nmid m$ , allora esiste  $i$  tale che  $a_i = 0$  (dunque c'è un 1 nella somma

---

rr. 1674, 1688; p. 46

- (4) Sia  $n_p$  il numero dei  $p$ -sottogruppi di Sylow, per quanto detto al punto (3) i  $p$ -sottogruppi di Sylow sono tutti coniugati, dunque per ciò che abbiamo visto sul numero di coniugi rispetto all'azione di coniugio si ha  $n_p = |\mathcal{C}\ell(S)| = [G : N_G(S)]$ , da cui:

$$n_p = \frac{|G|}{|N_G(S)|} \implies |G| = n_p |N_G(S)| \implies n_p \mid |G|$$

Sia  $X$  l'insieme dei  $p$ -Sylow di  $G$ , consideriamo l'azione di coniugio:

$$\phi : S \longrightarrow S(X) : s \longmapsto \varphi_s$$

con  $\varphi_s : X \longrightarrow X : H \longmapsto sHs^{-1}$  bigezione;  $\phi$  ha un'unica orbita banale, ovvero quella del gruppo  $S$ ,  $\text{Orb}(S) = \{S\}$ , infatti, per ogni altra orbita si ha:

$$\text{Orb}(H) = \{sHs^{-1} \mid s \in S\} = \{H\} \iff sHs^{-1} = H \quad \forall s \in S$$

ovvero:

$$S \subset N_G(H)$$

ma sappiamo anche che  $H \not\leq N_G(H)$ , pertanto si deve avere che:

$$HS < N_G(H)$$

(poiché  $S$  normalizza  $H$  il prodotto di sottogruppi **da** un sottogruppo), ma questo è assurdo se  $S \neq H$ , perché avremmo:

aggiunto un · per chiarezza, typo

$$da \rightarrow dà$$

$$\begin{aligned} \&[ n_p = \frac{|G|}{|N_G(S)|} \implies |G| = n_p \cdot |N_G(S)| \implies n_p \mid |G| \end{aligned}$$

(poiché  $S$  normalizza  $H$  il prodotto di sottogruppi dà un sottogruppo), ma questo è assurdo se  $S \neq H$ , perché avremmo:

rr. 1764-1765, 1773; p. 49

se mandassimo tutti gli elementi nell'identità otterremmo un prodotto **semidiretto**, alternativamente, riscrivendo  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  come  $\langle x \rangle \times \langle y \rangle$  (i cui elementi saranno  $\{e, x, y, xy\}$ ), abbiamo due elementi di ordine 2 che vanno in  $-id$  e l'elemento neutro e un altro elemento di ordine 2 che vanno in  $id$ . Possiamo dunque costruire tre prodotti semidiretti che danno origine a gruppi isomorfi, supponiamo (WLOG) che:

$$\varphi_x = id \quad \varphi_y = -id \quad \varphi_{xy} = -id$$

dunque abbiamo:

$$\langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{e} \quad \langle z \rangle \cong \mathbb{Z}/3\mathbb{Z}$$

possiamo osservare che:

$$\varphi_x(Z) = xzx^{-1} = id(z) = z \implies x \text{ commuta con } z$$

typo

*semidiretto → diretto*

*e → mentre*

*Z → z*

se mandassimo tutti gli elementi nell'identità otterremmo un prodotto diretto, alternativamente, riscrivendo  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  come  $\langle x \rangle \times \langle y \rangle$  (i cui elementi saranno  $\{e, x, y, xy\}$ ), abbiamo due elementi di ordine 2 che vanno in  $-id$ , mentre l'elemento neutro e un altro elemento di ordine 2 vanno in  $id$ . Possiamo dunque costruire tre prodotti semidiretti che danno

$\forall \varphi_x(z) = xzx^{-1} = id(z) = z \implies x \text{ commuta con } z$

r. 1797; p. 50

### §1.15 Gruppo dei Quaternioni

**Definizione 1.103.** Si definisce gruppo dei **quaternioni** il gruppo con la seguente presentazione:

$$Q_8 = \langle i, j | i^4 = 1, i^2 = j^2, ij = j^3i \rangle$$

usare `\mid`

```
\[ Q_8 = \left\langle i, j \mid i^4 = 1, i^2 = j^2, ij = j^3i \right\rangle
```

---

r. 1824; p. 50

**Osservazione 1.106 —** Osserviamo che  $\langle i \rangle, \langle j \rangle \triangleleft Q_8$  perché hanno indice 2, inoltre  $\langle i^2 \rangle, \langle j^2 \rangle \triangleleft Q_8$  (per verifica diretta).

typo

, → =

Osserviamo che  $\langle i \rangle, \langle j \rangle \triangleleft Q_8$  perché hanno indice 2, inoltre  $\langle i^2 \rangle = \langle j^2 \rangle \triangleleft Q_8$  (per verifica diretta).

---

**Osservazione 1.109 (Ordine degli elementi)** — Dunque in  $Q_8$  1 ha ordine 1,  $-1$  ha ordine 2, mentre  $i, -i, j, -j, k, -k$  hanno ordine 4.

Abbiamo visto che  $Q_8$  è un gruppo di ordine 8 non è abeliano, e per quanto detto  $Q_8 \not\cong D_4$ , poiché ha  $Q_8$  ha sei elementi di ordine 4, mentre  $D_4$  ne ha soltanto uno.

**Osservazione 1.110 (Sottogruppi di  $Q_8$ )** — Per quanto riguarda i sottogruppi di  $Q_8$  osserviamo in primis che  $\langle -1 \rangle = Z(Q_8)$  ed è caratteristico (perché è il centro oppure perché è l'unico sottogruppo di ordine 2);  $\langle i \rangle, \langle j \rangle, \langle k \rangle$  sono sottogruppi di ordine 4, dunque sono normali. Abbiamo quindi dimostrato che tutti i sottogruppi (includendo ovviamente quelli banali) di  $Q_8$  sono normali.

## riscrittura

Abbiamo visto che  $Q_8$  è un gruppo di ordine 8 non abeliano ma non è isomorfo a  $D_4$ , poiché  $Q_8$  ha sei elementi di ordine 4 ( $\pm i, \pm j, \pm k$ ) e un solo elemento di ordine 2 ( $-1$ ), mentre  $D_4$  ha due elementi di ordine 4 (le rotazioni di  $\pm 90^\circ$ ) e cinque elementi di ordine 2 (le simmetrie e la rotazione di  $180^\circ$ ). \\

---

rr. 1941-1942; p. 53

Se  $Q_8$  si immergesse in  $S_4$ , con  $|S_4| = 2^3 \cdot 3$ , sarebbe un suo 2-Sylow; poiché  $D_n$  si immerge sempre in  $S_n$ <sup>20</sup>, sappiamo che  $D_4 \hookrightarrow S_4$ , ed in particolare  $D_4$  è un 2-Sylow di  $S_4$ , ma ciò significa che  $Q_8$  non è in  $S_4$ , poiché non è un coniugato di  $D_4$ .

Si ragiona in maniera analoga per  $S_5$ , infatti  $|S_5| = 2^3 \cdot 3 \cdot 5$  e  $D_4 \subset S_4 \subset S_5$ , dunque i due 2-Sylow di  $S_4$  sono isomorfi a quelli di  $S_5$ , ed ancora una volta ciò significa che  $Q_8$  non si immerge nel gruppo.

Sia  $|S_6| = 2^4 \cdot 3^2 \cdot 5$ , detto  $P_2$  un 2-Sylow di  $S_6$ , osserviamo che se fosse  $Q_8 \hookrightarrow S_6$ , dovremmo avere:

<sup>20</sup>In tal caso infatti basta mandare  $x \in D_4$  nella corrispondente permutazione dei vertici.

aggiunta, typo

Se  $Q_8$  si immergesse in  $S_4$ , con  $|S_4| = 2^3 \cdot 3$ , sarebbe un suo 2-Sylow; poiché  $D_n$  si immerge sempre in  $S_n$  (per  $n \geq 3$ )<sup>21</sup>, sappiamo che  $D_4 \hookrightarrow S_4$ ,

ed in particolare  $D_4$  è un 2-Sylow di  $S_4$ , ma ciò significa che  $Q_8$  non è contenuto in  $S_4$ , poiché non è un coniugato di  $D_4$ . \\

---

r. 1969; p. 53

Dunque il fatto che  $\sigma^2 = \rho^2 = \eta^2$  hanno ordine 2 (quindi sono fatte da sole trasposizioni) e che sono quadrati (quindi i cicli di lunghezza pari compaiono a coppie), ci dice che le trasposizioni sono prodotti di un numero pari di trasposizioni, pertanto l'unica possibilità è che:

$$\sigma^2 = \rho^2 = \eta^2 = (a\ b)(c\ d)$$

riscrittura

ci dice che  $\sigma$ ,  $\rho$ ,  $\eta$  sono prodotti di un numero pari di trasposizioni, pertanto l'unica possibilità è che siano del tipo:

---

rr. 1984, 1987; p. 54

in particolare con la notazione dei cicli abbiamo che l'immagine di  $\varphi_i$  di  $Q_8$  è data da:

$$(1 \ i \ -1 \ i)(j \ k \ -j \ -k)$$

analogamente per  $\varphi_j(Q_8)$ :

$$(1 \ j \ -1 \ -j)(i \ -k \ -i \ k)$$

e numerando in qualsiasi ordine gli elementi di  $Q_8$  possiamo scrivere le permutazioni corrispondenti in  $S_8$ :

bisogna spaziare meglio questi elementi all'interno del ciclo

---

r. 2017; p. 55

<sup>a</sup>La direzione del prodotto semidiretto è data dal fatto che  $\mathbb{Z}/15\mathbb{Z}$  è l'unico normale tra i due sottogruppi.

<sup>b</sup>Andrebbe aggiunto il perché ma non è chiarissimo dalle note della Del Corso.

si applica un lemma per spostare prodotti diretti e semidiretti quando gli elementi di un gruppo commutano con tutti quelli degli altri (o qualcosa del genere, spero si sia capito)

$\text{ord}(x) = 3$ ,  $x^4 = x$  e se  $\text{ord}(x) = 5$ ,  $x^{-4} = (x^4)^{-1} = (x^{-1})^{-1} = x$   
quindi  $x$  commuta con  $y$

---

rr. 2089, 2094, 2097; p. 56

**Definizione 2.10.** Un anello  $A$  si dice **dominio d'integrità** se:

$$D(A) = \{x \in A \mid x \text{ è un divisore di } 0\} = \{0\}$$

Definiamo inoltre l'insieme degli elementi invertibili di  $A$ :

$$A^* = \{x \in A \mid x \text{ è invertibile}\}$$

e dei nilpotenti:

$$\mathcal{N} = \{x \in A \mid x \text{ è nilpotente}\}$$

usare `\mid`

$$\boxed{\begin{aligned} \mathbf{D(A)} &= \{x \in A \mid \text{text{$x$ è un divisore di $0$}}\} = \{0\} \end{aligned}}$$

$$\boxed{\begin{aligned} \mathbf{A^*} &= \{x \in A \mid \text{text{$x$ è invertibile}}\} \end{aligned}}$$

$$\boxed{\begin{aligned} \mathbf{A^*} &= \{x \in A \mid \text{text{$x$ è invertibile}}\} \end{aligned}}$$

---

r. 2102; p. 57

**Esercizio 2.11.** Calcolare i divisori di zero, gli invertibili ed i nilpotenti di:

$$\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

spazi

$$\boxed{\begin{aligned} \mathbf{\mathbb{Z}}, \quad \mathbf{\mathbb{Z}/n\mathbb{Z}}, \quad \mathbf{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}} \end{aligned}}$$

---

(1) Per provare che  $(A^*, \cdot)$  è un gruppo abeliano, è sufficiente verificare le proprietà richieste dalla definizione:

- (a) Chiusura: osserviamo che  $\forall x, y \in A^*$ , allora  $\exists x^{-1}y^{-1} \in A$ , pertanto  $xy \in A^*$ , poiché  $y^{-1}x^{-1} \in A^*$ .
- (b) Associatività: poiché  $A \subseteq A^*$ , allora, essendo  $A$  associativo rispetto al  $\cdot$ , allora anche gli elementi di un suo qualsiasi sottoinsieme saranno associativi tra loro.
- (c) Elemento Neutro:  $1 \in A$ , infatti, l'inverso di  $1$  è se stesso, quindi  $1$  è invertibile.
- (d) Inverso: Segue per la stessa definizione di  $A^*$  che ogni suo elemento debba avere inverso moltiplicativo nel gruppo,  $\forall x \in A, \exists x^{-1} \in A$ :

$$x \cdot x^{-1} = x^{-1} \cdot x = 1 \quad \forall x \in A$$

- (e) L'abelianità segue immediatamente dall'abelianità di  $A$  (infatti  $A^* \subset A$ , dunque l'abelianità vale in particolare per gli elementi di  $A^*$ ).

## riscrittura, typo, rimozione

$$A \subseteq A^* \rightarrow A^* \subseteq A$$

$$1 \in A \rightarrow 1 \in A^*$$

```
\item Chiusura: osserviamo che $\forall x, y \in A^*$, allora $x^{-1}, y^{-1} \in A \implies (xy)^{-1} \in A$, pertanto $xy \in A^*$.

\item Associatività: poiché $A^* \subseteq A$, allora, essendo $A$ associativo rispetto al $\cdot$, allora anche gli elementi di un suo qualsiasi sottoinsieme saranno associativi tra loro.

\item Elemento Neutro: $1 \in A^*$, infatti, l'inverso di $1$ è se stesso, quindi $1$ è invertibile.

\item Inverso: Segue per la stessa definizione di $A^*$ che ogni suo elemento debba avere inverso moltiplicativo nel gruppo,
$\forall x \in A, \exists x^{-1} \in A$:
\begin{array}{l}
x \cdot x^{-1} = x^{-1} \cdot x = 1 \\
\end{array}
```

(2) Supponiamo per assurdo che  $D(A) \cap A^* \neq \emptyset$ , e consideriamo  $x \in D(A) \cap A^*$ , poiché  $x \in D(A)$ , allora  $\exists z \in A, z \neq 0$ , tale per cui:

$$xz = zx = 0$$

d'altra parte, poiché  $x \in A^*$ , allora  $\exists x^{-1}$  tal per cui:

$$xy = yx = 1$$

da cui segue:

$$(zx)y = z(xy) \implies 0 \cdot y = z \implies z = 0$$

ma ciò è assurdo, pertanto l'ipotesi  $D(A) \cap A^*$  è vuoto.

riscrittura, aggiunta, rimozione

*tale per cui → tale che*

\item Supponiamo per assurdo che  $D(A) \cap A^* \neq \emptyset$ , e consideriamo  $x \in D(A) \cap A^*$ , poiché  $x \in D(A)$ , allora  $\exists z \in A, z \neq 0$ , tale che:

d'altra parte, poiché  $x \in A^*$ , allora  $\exists y \in A$  tale che:

$$\begin{aligned} & (zx)y = z(xy) \implies 0 \cdot y = z \cdot 1 \implies z = 0 \\ & \text{ma ciò è assurdo, pertanto } D(A) \cap A^* \text{ è vuoto.} \end{aligned}$$

con:

$$\ker \varphi_x = \{y \in A \mid \varphi_x(y) = xy = 0\} = \{0\}$$

infatti, non essendo  $x$  un divisore di zero, l'unica possibilità, in base all'annullamento del prodotto è che  $y = 0 \implies xy = 0$ . Poiché  $|A| < +\infty$  l'omomorfismo è anche surgettivo, dunque è una bigezione, pertanto  $1 \in \text{Im } \varphi_x \implies \exists a \in A$  tale che  $\varphi_x(a) = xa = 1 \implies x \in A^*$ .

□

**Definizione 2.13.** Dato  $B \subset A$  non vuoto, si dice che  $B$  è un **sottoanello** di  $A$  se è chiuso rispetto alle operazioni  $+$  e  $\cdot$  ristrette a  $B$ .

**Definizione 2.14.** Dato  $I \subset A$ , con  $A$  anello commutativo, si dice che  $I$  è un **ideale** di  $A$  se:

- $(I, +) < (A, +)$ .
- Vale la **proprietà di assorbimento** a destra e sinistra:<sup>23</sup>

$$aI \subset I \quad \text{e} \quad Ia \subset I \quad \forall a \in A$$

**Osservazione 2.15 —** Per verificare che un sottoinsieme di un anello commutativo con identità è un ideale ci basta verificare soltanto che  $(I, +)$  è chiuso per l'operazione  $+$  e che valga la proprietà di assorbimento, infatti, da ciò segue che  $(-1)a \in I$ , dove  $(-1)$  esiste in  $A$  è un gruppo rispetto al  $+$ .

## rimozione, riscrittura

infatti, non essendo  $x$  un divisore di zero, l'unica possibilità, in base all'annullamento del prodotto è che  $y = 0$ . Poiché  $|A| < +\infty$  l'omomorfismo è anche surgettivo, dunque è una bigezione,

Per verificare che un sottoinsieme di un anello commutativo con identità è un ideale ci basta verificare soltanto che  $(I, +)$  è chiuso per l'operazione  $+$  e che valga la proprietà di assorbimento, infatti, da ciò segue che  $0 = 0a \in I$  e  $-a = (-1)a \in I$ , quindi  $I$  è un gruppo rispetto a  $+$ .

rr. 2220, 2225; p. 59

**Definizione 2.18.** Dato un sottoinsieme non vuoto di un anello  $S \subset A$ , si definisce **ideale generato** da  $S$  in  $A$ :

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

Osserviamo che se  $S = \{x\}$  possiamo definire l'ideale generato da un elemento:

$$(x) = \{ax \mid a \in A\} = Ax$$

in tal caso l'ideale prende anche il nome di **ideale principale**.

usare `\mid` (forse per quello grande è meglio solo aggiungere `\sim` prima e dopo)

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

```
\[ (x) = \{ax \mid a \in A\} = Ax
```

---

rr. 2251-2252; p. 59

**Esempio 2.20 (Ideali generati)**

Alcuni esempi di ideali generati possono essere:

- $n\mathbb{Z} = (n)$ , con  $n \in \mathbb{Z}$ .
- Dato  $K \subset F$  e  $\alpha \in F$  algebrico su  $K$ , sia  $\mu_\alpha(x) \in K[x]$  il polinomio minimo di  $\alpha$ , sappiamo che:

$$(\mu_\alpha(x)) = \{p(x) \in K[x] \mid p(\alpha) = 0\}$$

typo, aggiunta, usare `\mid`

```
\item Dati $K \subset F$ campi e $\alpha \in F$ algebrico su $K$, sia  
$\mu_\alpha(x) \in K[x]$ il polinomio minimo di $\alpha$, sappiamo che:  
\[ (\mu_\alpha(x)) = \{p(x) \in K[x] \mid p(\alpha) = 0\}
```

## §2.2 Operazioni tra ideali

### Proposizione 2.21 (Operazioni tra ideali)

Dato  $A$  un anello commutativo e  $I, J \subset A$  ideali, abbiamo che:

- $I \cap J$  è un ideale.
- $I + J = (I, J) = \{i + j \mid i \in I, j \in J\}$  è un ideale.
- $IJ = (\{xy \mid x \in I, y \in J\})$  è un ideale.
- $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\}$  è un ideale. In particolare  $\sqrt{0} = \mathcal{N}$  è un ideale.
- $(I : J) = \{x \in A \mid xJ \subseteq I\}$  è un ideale.

usare `\mid`

```
\item $I + J = (I, J) = \{i + j \mid i \in I, j \in J\}$ è un ideale.  
\item $IJ = (\{xy \mid x \in I, y \in J\})$ è un ideale.  
\item $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\}$ è un  
ideale. In particolare $\sqrt{0} = \mathcal{N}$ è un ideale.  
\item $(I : J) = \{x \in A \mid xJ \subseteq I\}$ è un ideale.
```

rr. 2278-2279, 2285; p. 60

- Dato  $I + J = \{i + j \mid i \in I, j \in J\}$ , presi  $x, y \in I + J$ , ovvero:

$$x = i_1 + j_1 \quad \text{e} \quad y = i_2 + j_2 \implies x + y = (\underbrace{i_1 + i_2}_{\in I}) + (\underbrace{j_1 + j_2}_{\in J}) \in I + J$$

inoltre,  $\forall a \in A$  si ha che:

$$ax = \underbrace{ai_1}_{\in I} + \underbrace{aj_1}_{\in J} \in I + J \quad \forall x \in I + J$$

dunque  $I + J$  è un ideale. Verifichiamo che  $I + J = (I, J)$ ; osserviamo che ovviamente:

$$\forall i + j \in I + J, i + j \in (I, J) \implies I + J \subseteq (I, J)$$

usare `\mid`, spazi, riscrittura

```
\item Dato $I + J = \{i + j \mid i \in I, j \in J\}$, presi $x, y \in I + J$, ovvero:  
$[ x = i_1 + j_1 \quad \text{e} \quad y = i_2 + j_2 \implies x + y = (\underbrace{i_1 + i_2}_{\in I}) + (\underbrace{j_1 + j_2}_{\in J}) \in I + J ]$
```

```
$[ \forall i \in I, \forall j \in J, i + j \in (I, J) \implies I + J \subseteq (I, J)$
```

r. 2294; p. 60

$$(S) = \bigcap_{\substack{S \subseteq X \subseteq A \\ X \text{ ideale}}} X$$

dove l'intersezione è appunto il più piccolo ideale di  $A$  che contiene  $S$ . Dobbiamo dimostrare ora quanto detto; osserviamo che  $(S)$  è contenuto nell'intersezione in quanto è uno dei termini di quest'ultima; il contenimento opposto segue dal fatto che  $\forall x \in S$  si ha  $x = \sum a_i s_i \in X$  (poiché  $X$  è un ideale che contiene  $S$ , per come l'abbiamo definito), d'altra parte, per vedere che un ideale generato  $(S)$  è contenuto a sua volta in un ideale  $\mathcal{I}$  di  $A$ , basta vedere che  $S \subseteq \mathcal{I}$  (ed è ciò che abbiamo appena fatto con  $S$ ). A questo punto, tornando all'inclusione iniziale, ci basta

hai detto in modi diversi la stessa cosa, ma hai mostrato un'inclusione sola

- Verifichiamo che  $\sqrt{I} = \{x \in A \mid x^n \in I, n \in \mathbb{N}\}$  è un ideale, presi  $x, y \in \sqrt{I}$ , ovvero  $x^n, y^m \in I$ ,  $n, m \in \mathbb{N}$ , vogliamo provare che  $x + y \in \sqrt{I}$  (ovvero che esiste  $d \in \mathbb{N}$  tale che  $(x + y)^d \in I$ ), osserviamo che:

$$(x + y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{m+n-i}$$

dove  $\forall i \in \{0, \dots, m+n\}$  si ha che  $i \geq n \implies x^i \in I$ , oppure che  $n+m-i \geq m \implies y^{n+m-i} \in I$ , dunque tutti i termini di  $(x + y)^{n+m}$  stanno in  $I$  e quindi  $x + y \in \sqrt{I}$ . Osserviamo che  $\forall a \in A$  si che:

$$(ax)^n = a^n \underbrace{x^n}_{\in I} \in I \implies ax \in \sqrt{I}$$

- Dato  $(I : J) = \{x \in A \mid xJ \subseteq I\}$  e presi  $x, y \in (I : J)$  si ha che:

$$(x + y)J = \underbrace{xJ}_{\subseteq I} + \underbrace{yJ}_{\subseteq I} \implies x + y \in (I : J)$$

inoltre,  $\forall a \in A$  abbiamo:

$$axJ = a(xJ) \subseteq aI \subseteq I \implies ax \in (I : J) \quad \forall x \in (I : J)$$

usare  $\mid$ , riscrittura

```
\item Verifichiamo che  $\sqrt{I} = \{x \in A \mid x^n \in I, n \in \mathbb{N}\}$  è un ideale, presi  $x, y \in \sqrt{I}$ , ovvero  $x^n, y^m \in I$ ,  $n, m \in \mathbb{N}$ , vogliamo
```

dove  $\forall i \in \{0, \dots, m+n\}$  si ha che  $i \leq n \implies x^i \in I$ , e che  $i \leq m \iff n+m-i \geq m \implies y^{n+m-i} \in I$ , dunque tutti i termini di  $(x+y)^{n+m}$  stanno in  $I$

```
\item Dato  $(I : J) = \{x \in A \mid xJ \subseteq I\}$  e presi  $x, y \in (I : J)$  si ha che:
```

```
\[ (ax)J = a(xJ) \subseteq aI \subseteq I \implies ax \in (I : J) \quad \forall x \in (I : J)
```

$$m\mathbb{Z} + n\mathbb{Z} = \{am + bn \mid a, b \in \mathbb{Z}\} = \{dx \mid x \in \mathbb{Z}\}$$

Consideriamo ora  $n = p_1^{e_1} \dots p_r^{e_r}$ , possiamo considerare:

$$\sqrt{n\mathbb{Z}} = p_1 \dots p_r \mathbb{Z}$$

poiché:

$$\sqrt{n\mathbb{Z}} = \{x \in \mathbb{Z} \mid x^k \in n\mathbb{Z}, k \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid n \mid x^k, k \in \mathbb{Z}\}$$

ma  $n \mid x^k \implies p_i \mid x^k, \forall i \in \{1, \dots, r\}$ , ovvero  $p_1 \dots p_r \mid x \implies x \in p_1 \dots p_r \mathbb{Z}$ . Viceversa  $x = p_1 \dots p_r m \in \sqrt{n\mathbb{Z}}$  perché, detto  $e = \max e_i$ :

$$x^e = p_1^e \dots p_r^e m^e = ny \in n\mathbb{Z}$$

quindi ad esempio:

$$\sqrt{100\mathbb{Z}} = 10\mathbb{Z}$$

Infine, osserviamo che:

$$(m\mathbb{Z} : n\mathbb{Z}) = \frac{m}{(m, n)}\mathbb{Z}$$

quindi ad esempio:

$$(75\mathbb{Z} : 18\mathbb{Z}) = \frac{75}{(75, 18)} = 25\mathbb{Z}$$

questo poiché:

$$(75\mathbb{Z} : 18\mathbb{Z}) = \{x \in \mathbb{Z} \mid 18x \in 75\mathbb{Z}\} = 25\mathbb{Z}$$

infatti  $18x \in 75\mathbb{Z} \iff 75 \mid 18x \iff 25 \mid 6x \iff 25 \mid x$ .

usare `\mid` (nel radicale, dato che ci sono delle divisibilità, è meglio usare i due punti)

$$\sqrt{m\mathbb{Z} + n\mathbb{Z}} = \{am + bn \mid a, b \in \mathbb{Z}\} = \{dx \mid x \in \mathbb{Z}\}$$

Consideriamo ora  $n = p_1^{e_1} \dots p_r^{e_r}$ , allora:

$$\sqrt{n\mathbb{Z}} = \{x \in \mathbb{Z} \mid x^k \in n\mathbb{Z}, k \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid n \mid x^k, k \in \mathbb{Z}\}$$

$$(75\mathbb{Z} : 18\mathbb{Z}) = \{x \in \mathbb{Z} \mid 18x \in 75\mathbb{Z}\} = 25\mathbb{Z}$$

rr. 2392, 2394; p. 63

*Dimostrazione.* Dimostriamo singolarmente i fatti:

- (1) Se  $I \cap A^* = \emptyset$ , poiché vale sempre che  $1 \in A^*$ , allora c'è almeno un elemento di  $A$  che non sta nell'ideale, quindi  $I \subsetneq A$ . Viceversa, sia  $I$  ideale proprio e supponiamo  $x \in I \cap A^*$ , allora  $x$  è invertibile, dunque  $\exists y \in A$  tale che  $xy = 1$ , ma:

$$1 = \underbrace{x}_{\in I} \underbrace{y}_{\in A} \in I \implies a \cdot 1 \in I^{25} \quad \forall a \in A \implies A \subset I$$

che è assurdo in quanto avevamo supposto  $I \subset A$ , dunque  $I \cap A^* = \emptyset$ .

<sup>25</sup>In pratica se c'è l'identità in  $I$  c'è esattamente ogni elemento dell'anello che contiene l'ideale.

aggiunta, riscrittura, spazio

\item Se  $I \cap A^* = \emptyset$ , poiché vale sempre che  $1 \in A^*$  quindi  $A^* \neq \emptyset$ , allora c'è almeno un elemento di  $A$  che non sta nell'ideale, quindi  $I \subsetneq A$ .

\[ 1 = \underbrace{x}\_{\in I} \underbrace{y}\_{\in A} \in I \implies a \cdot 1 \in I \text{In pratica se c'è l'identità in } I \text{ c'è ogni elemento dell'anello.} \forall a \in A \implies A \subset I

rr. 2407-2408; p. 64

### §2.3 Anelli quoziante e omomorfismi di anelli

**Definizione 2.27.** Dati  $A$  e  $B$  anelli,  $f : A \rightarrow B$  è un **omomorfismo di anelli** se:

- $f(a_1 + a_2) = f(a_1) + f(a_2), \forall a_1, a_2 \in A$ .
- $f(a_1 a_2) = f(a_1)f(a_2), \forall a_1, a_2 \in A$ .

spazi

\item  $f(a_1 + a_2) = f(a_1) + f(a_2) \quad \forall a_1, a_2 \in A$ .  
\item  $f(a_1 a_2) = f(a_1)f(a_2) \quad \forall a_1, a_2 \in A$ .

r. 2435; p. 64

**Osservazione 2.30 —** Si verifica facilmente che l'operazione è ben definita, infatti, presi:

$$a + I = a' + I \quad \text{e} \quad b + I = b' + I$$

segue:

$$(a' + I) \cdot (b' + I) = a'b' + I = (a + I)(b + I) + I = ab + I$$

riscrittura

$$\begin{aligned} ab + I &= (a + I) \cdot (b + I) = (a^{\prime\prime} + I) \cdot (b^{\prime\prime} + I) \\ &= a^{\prime\prime}b^{\prime\prime} + I \end{aligned}$$

$$ab + I = (a + I) \cdot (b + I) = (a' + I) \cdot (b' + I) = a'b' + I$$

rr. 2455, 2457; p. 64

### Proposizione 2.33

Gli ideali sono tutti e soli i nuclei degli omomorfismi di anello definiti su  $A$ .

*Dimostrazione.* Sia  $\varphi : A \rightarrow B$  un omomorfismo di anelli, allora  $\ker \varphi$  è un ideale di  $A$ , infatti  $\ker \varphi \subset A$  perché  $\varphi$  è in particolare un omomorfismo di gruppi, inoltre,  $\forall a \in A$  si ha che:

$$ax \in \ker \varphi \quad \forall x \in \ker \varphi$$

aggiunta, spazio

Sia  $\varphi : A \rightarrow B$  un omomorfismo di anelli, allora  $\ker \varphi$  è un ideale di  $A$ , infatti  $(\ker \varphi, +) \subset (A, +)$  perché  $\varphi$

$$\begin{aligned} ax \in \ker \varphi \quad \forall x \in \ker \varphi \\ (\ker \varphi, +) \subset (A, +) \end{aligned}$$

r. 2491; p. 65

tale che  $f = \varphi \circ \pi_I$ , con  $\varphi$  è iniettivo e  $\text{Im} \varphi = \text{Im} f$ . Non ci resta altro da fare che verificare che  $\varphi$  è anche un omomorfismo di anelli:

$$\varphi((a + I)(b + I)) = \varphi(ab + I) = f(ab) \quad \forall a, b \in A$$

viceversa:

$$f(ab) = f(a)f(b) = \varphi(a + I)\varphi(b + I) \quad \forall a, b \in I$$

dove la seconda uguaglianza è vera per ipotesi.  $\square$

typo

$$I \rightarrow A$$

$$\lfloor f(ab) = f(a)f(b) = \varphi(a+I)\varphi(b+I) \quad \forall a, b \in A$$

---

r. 2517; p. 66

(2) Sappiamo che  $f(I)$  è un sottogruppo di  $B$ , verifichiamo l'assorbimento, sia  $b \in B$ , poiché  $f$  è surgettiva esiste  $a \in A$  tale che  $b = f(a)$ , dunque:

$$bf(x) = f(a)f(x) = f(\underbrace{ax}_{\in I}) \in f(I)$$

aggiunta

$$\lfloor bf(x) = f(a)f(x) = f(\underbrace{ax}_{\in I}) \in f(I) \quad \forall x \in I$$

---

rr. 2533, 2542; p. 66

$$X = \{J \subseteq A \text{ ideale} \mid I \subset J\} \quad \text{e} \quad Y = \left\{ \mathcal{J} \subset \frac{A}{I} \mid \mathcal{J} \text{ ideale} \right\}$$

per il Lemma 2.35, essendo  $\pi_I$  surgettivo, si ha che le immagini e la controimmagine via  $\pi_I$ :

$$J \longmapsto \pi_I(J) \quad \text{e} \quad \mathcal{J} \longmapsto \pi_I^{-1}(\mathcal{J})$$

sono ideali, e ciò conclude la dimostrazione.  $\square$

### Esempio 2.37

Se nel Lemma 2.35  $f$  non fosse surgettiva, allora l'immagine di un ideale **non sarebbe** un ideale, ad esempio presa:

$$f : \mathbb{Z} \hookrightarrow \mathbb{Q} : (2) \longmapsto 2\mathbb{Z}$$

usare `\mid` (per quella grande aggiungere spazi), correzione

*non sarebbe  $\rightarrow$  può non essere*

```
\[ X = \{J \subseteq A \mid \text{ideale} \mid I \subset J\} \quad \text{e} \quad
\qquad Y = \left\{ \mathcal{J} \subset \frac{A}{I} \mid \mathcal{J} \text{ ideale} \right\}
```

Se nel `\hyperref[2.35]{Lemma 2.35}`  $f$  non fosse surgettiva, allora l'immagine di un ideale può non essere un ideale, ad esempio presa:

r. 2569; p. 66

che manda ogni ideale di  $B$  nella propria contrazione ad un **sottoanello** fanno sì che l'applicazione:

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

sia tale che:

$$\ker \varphi = \{a \in A \mid \varphi(a) = a + J = J\} = \{a \in A \mid a \in J\} = J \cap A = \pi_I^{-1}(J)$$

da cui si ha anche che:

$$\frac{A}{J \cap A} \hookrightarrow B/J$$

per il Primo Teorema di Omomorfismo.

usare \mid

$$\begin{aligned} \ker \varphi &= \{a \in A \mid \varphi(a) = a + J = J\} = \{a \in A \mid a \in J\} \\ a \in J &= J \cap A = \pi_I^{-1}(J) \end{aligned}$$

Osserviamo ora che:

$$\ker f = \{a \in A \mid f(a) = (a + I, a + J) = (I, J)\} = \{a \in A \mid a \in I, a \in J\} = I \cap J$$

Verifichiamo separatamente le due implicazioni della seconda parte del teorema:

- Supponiamo che  $I + J = A$ , ovvero che esistono  $i$  e  $j$  tali che  $i + j = 1^{26}$ , e verifichiamo che  $f$  è surgettiva. Per verificare che  $f$  è surgettiva dobbiamo far vedere che:

$$\forall a, b \in A, \exists x \in A : f(x) = (a + I, b + J)$$

per ipotesi sappiamo che  $x \in A \implies x \in I + J$  quindi possiamo prendere  $x = bi + aj \in A$ , per  $i \in I$  e  $j \in J$ , dunque:

$$f(x) = (\underbrace{bi}_{\in I} + aj + I, bi + \underbrace{aj}_{\in J} + J) = (aj + I, bi + J)$$

da cui, osservando che  $j = 1 - i$  e  $i = 1 - j$  per ipotesi abbiamo:

$$(aj + I, bi + J) = (a(1 - i) + I, b(1 - j) + J) = (a + I, b + J)$$

e pertanto abbiamo ottenuto  $f(x) = (a + I, b + J)$ .

<sup>26</sup>Poiché l'identità è in  $I + J$ , allora per la proprietà di assorbimento ogni altro elemento di  $A$  è in  $I + J$ .

usare \mid, rimozione (osservazione superflua, stiamo già supponendo che  $I + J = A$ )

```
\[ \ker f = \{a \in A \mid f(a) = (a+I, a+J) = (I, J)\} = \{a \in A \mid a \in I, a \in J\} = I \cap J
```

**Esempio 2.54 (Ideali primi di  $\mathbb{Z}$ )**

Gli ideali primi di  $\mathbb{Z}$  sono  $(p)$  con  $p$  primo, infatti:

$$xy \in (p) \iff p | xy \iff p | x \vee p | y$$

ovvero se  $x \in (p)$  o  $y \in (p)$ . Se consideriamo invece  $(m)$ , con  $m$  non primo, dunque riducibile  $m = ab$ , con  $1 < a < m$  e  $1 < b < m$ , allora:

$$ab \in (m) \quad \text{ma} \quad a \notin (m) \quad \text{e} \quad b \notin (m)$$

dunque  $(m)$  non è primo.

typo

$$p \rightarrow (p)$$

ovvero se  $x \in (p)$  o  $y \in (p)$ . Se consideriamo invece  $(m)$ , con  $m$  non primo, dunque riducibile  $m = ab$ , con  $1 < a < m$  e  $1 < b < m$ , allora:

1. Sia  $I \subsetneq A$  un ideale proprio e sia  $\mathcal{F}$  la famiglia di tutti gli ideali propri che lo contengono:

$$\mathcal{F} = \{J \subsetneq A \mid I \subseteq J\}$$

osserviamo che  $I \in \mathcal{F} \implies \mathcal{F} \neq \emptyset$ , inoltre  $(\mathcal{F}, \subseteq)$  è induttivo, infatti, detta  $\mathcal{C}$  una catena, essa sarà un sottoinsieme di  $\mathcal{F}$  totalmente ordinato della forma:

$$\mathcal{C} = \{J_n\}^{27} \subseteq \mathcal{F}$$

allora posta  $\bigcup J_n^{28} = J \in \mathcal{F}$ , verifichiamo che  $J$  è maggiorante di  $\mathcal{C}$ . Si ha che:

- $\forall J_n \in \mathcal{C} : J_n \subseteq J$ , segue ovviamente da come abbiamo definito  $J$ , avendolo costruito come l'unione di tutti i  $J_n$ .

<sup>27</sup>I vari  $J_i$  sono contenuti tutti uno dentro l'altro "in catena".

<sup>28</sup>Andrebbe dimostrato che l'unione di ideali in catena, analogamente a quanto accade per i sottogruppi, è un ideale.

<sup>29</sup>Abbiamo verificato addirittura che tale maggiorante sia un massimo della catena.

aggiunta, usare `\mid`, `\text{ideale}`, `\in`

$$i \rightarrow n$$

```
\[ \mathcal{F} = \{J \subseteq A \mid \text{ideale } I \subseteq J\}
```

```
\[ \mathcal{C} = \{J_n\} \footnote{I vari $J_n$ sono contenuti tutti uno dentro l'altro "in catena."} \subseteq \mathcal{F}
```

```
allora posta $J = \bigcup J_n \footnote{Andrebbe dimostrato che l'unione di ideali in catena, analogamente a quanto accade per i sottogruppi, è un ideale.} \in \mathcal{F}$, verifichiamo che
```

```
\item $J \subseteq J \quad \forall J_n \in \mathcal{C}$, segue ovviamente da come abbiamo definito $J$, avendolo costruito come l'unione di tutti i $J_n$.
```

rr. 2758; p. 71

Resta da verificare che tale elemento massimale  $M$  sia un ideale massimale dell'anello (poiché abbiamo dimostrato che è massimale per la famiglia  $\mathcal{F}$  degli ideali che ne contengono uno proprio, la quale ovviamente non è la famiglia di tutti gli ideali propri di  $A$ ), ciò segue subito osservando che, supponendo  $L \subsetneq A$  ideale proprio con  $M \subseteq L$ , allora:

$$I \subseteq M \subseteq L \implies L \subsetneq \mathcal{F}$$

dunque  $L$  è un elemento della famiglia  $\mathcal{F}$ , e per la massimalità di  $M$  in  $\mathcal{F}$ , segue che  $M = L$ .

typo

$$\subset \rightarrow \in$$

$$\forall I \subseteq M \subseteq L \implies L \in \mathcal{F}$$

r. 2782; p. 72

- (1) Presi  $x, y \in A$ , per definizione abbiamo che  $I$  è primo se e solo se  $xy \in I \implies x \in I$  o  $y \in I$ , d'altra parte,  $\frac{A}{I}$  è un dominio se e solo se:

$$(x + I)(y + I) = xy + I = I \iff xy \in I \implies x \in I \text{ o } y \in I$$

riscrittura

$$\begin{aligned} & \forall (x+I)(y+I) = \underbrace{xy + I = I}_{\iff xy \in I} \implies \\ & \quad \underbrace{x+I = I}_{x \in I} \quad \text{e} \quad \underbrace{y+I = I}_{y \in I} \end{aligned}$$

$$(x + I)(y + I) = \underbrace{xy + I = I}_{\iff xy \in I} \implies \underbrace{x + I = I}_{x \in I} \quad \text{e} \quad \underbrace{y + I = I}_{y \in I}$$

*Dimostrazione.* Osserviamo preliminarmente che si ha  $I \subseteq J \subseteq A$ , dunque nella proiezione  $\pi_I$  si ha che:

$$J \longmapsto \pi_I(J) = J/I$$

Dobbiamo dimostrare che  $J$  è primo (massimale) in  $A$  se e solo se  $J/I$  è primo (massimale) in  $A/I$ . Per quanto detto nella Proposizione 2.56  $J$  primo (massimale) è equivalente al fatto che  $A/J$  sia un dominio (campo), e, ugualmente deve essere che  $A/I$  è un dominio ( $J/I$ ) ma dal Secondo Teorema di Omomorfismo di Anelli si ha:

$$\frac{A/I}{J/I} \cong A/J$$

che in entrambi i casi verifica la tesi. □

### riscrittura con qualche aggiunta

Dobbiamo dimostrare che  $J$  è primo (massimale) in  $A$  se e solo se  $\text{\faktor}{J}{I}$  è primo (massimale) in  $\text{\faktor}{A}{I}$ .

Per quanto detto nella \hyperref[2.56]{Proposizione 2.56}  $J$  primo (massimale) in  $A$  è equivalente al fatto che  $\text{\faktor}{A}{J}$  sia un dominio (campo), e analogamente  $\text{\faktor}{J}{I}$  primo (massimale) in  $\text{\faktor}{A}{I}$  è equivalente a  $\text{\displaystyle\frac{A/I}{J/I}}$  dominio (campo).

Ma dal Secondo Teorema di Omomorfismo di Anelli si ha:

$$\begin{aligned} & \left[ \frac{A/I}{J/I} \cong \text{\faktor}{A}{J} \right] \\ & \text{che conclude.} \end{aligned}$$

**Osservazione 2.62 —** La relazione  $\sim$  usata nella definizione precedente è una relazione di equivalenza, infatti:

- $\sim$  è riflessiva in quanto  $\frac{a}{s} \sim \frac{a}{s} \iff as = sa$ , che è vero in quanto abbiamo supposto  $A$  commutativo.
- $\sim$  è simmetrica in quanto  $\frac{a}{s} \sim \frac{b}{t} \iff at = bs \iff \frac{b}{t} \sim \frac{a}{s}$ .
- $\sim$  è transitiva in quanto, dati  $\frac{a}{s} \sim \frac{b}{t}$  e  $\frac{b}{t} \sim \frac{c}{u}$  abbiamo che:  

$$at = bs \quad \text{e} \quad bu = tc$$

da cui, moltiplicando la prima per  $u$  si ha:

$$aut = bus = tcu \implies aut = cts \iff t(au - cs) = 0$$

essendo per ipotesi  $A$  un dominio<sup>a</sup> e  $t \in S$  (dunque  $t \neq 0$ ) segue:

riscritte alcune espressioni per chiarezza e coerenza con la definizione

`\item $\sim$ è riflessiva in quanto $\displaystyle\frac{a}{s} \sim \frac{a}{s}$ iff $as = as$.`

`\[ at = bs \quad \text{e} \quad bu = ct`

`da cui, moltiplicando la prima per $u$ e usando il fatto che $A$ è  
commutativo si ha:`

`\[ (at)u = (bs)u = (bu)s = (ct)s \implies atu = cts \iff t(au - cs) = 0  
\]`

rr. 2896-2897; p. 75

$$(at + bs)s't' = (a't' + b's')st$$

sviluppando l'LHS otteniamo:

$$att's' + bss't' = a'st't' + b'tss' = (a't' + b's')st$$

che dimostra che l'operazione  $+$  è ben definita.<sup>32</sup>

rimozione, riscrittura

sviluppando otteniamo:

$$\begin{aligned} \left[ ats'^{\prime\prime}t'^{\prime\prime} + bss'^{\prime\prime}t'^{\prime\prime} \right] &= (as'^{\prime\prime})tt'^{\prime\prime} + \\ (bt'^{\prime\prime})ss'^{\prime\prime} &= (a'^{\prime\prime}s)tt'^{\prime\prime} + (b'^{\prime\prime}t)ss'^{\prime\prime} = \\ a'^{\prime\prime}t'^{\prime\prime}st + b'^{\prime\prime}s'^{\prime\prime}st & \\ \end{aligned}$$

$$ats't' + bss't' = (as')tt' + (bt')ss' = (a's)tt' + (b't)ss' = a't'st + b's'st$$

rr. 2932, 2939; p. 76

Per l'iniettività studiamo il nucleo:

$$\ker f = \left\{ a \in A \mid f(a) = \frac{a}{1} = \frac{0}{1} \right\} \stackrel{33}{=} \{a \in A \mid a \cdot 1 = 0 \cdot 1 = 0\} = \{0\}$$

dunque l'omomorfismo è iniettivo.  $\square$

**Osservazione 2.67** ( $S = A \setminus \{0\}$ ) — Se  $A$  è un dominio, allora  $S = A \setminus \{0\}$ <sup>a</sup> è una parte moltiplicativa, infatti,  $\forall x, y \in S$ , ovvero  $x \neq 0$  e  $y \neq 0$ , dunque  $xy \in S$ ,  $xy \neq 0$ .

<sup>a</sup>Sarebbe  $A^*$  se  $A$  fosse finito.

usare  $\mid$  (per quella grande gli spazi), riscrittura

$$\begin{aligned} \left[ \ker f = \left\{ a \in A \mid f(a) = \frac{a}{1} = \frac{0}{1} \right\} \right] &= \\ \left[ \frac{a}{1} = \frac{0}{1} \right] &\text{footnote{Ricordiamo che } } 0/1 \text{ è l'elemento neutro di } S^{-1}A. \\ \left\{ a \in A \mid a \cdot 1 = 0 \cdot 1 = 0 \right\} &= \{0\} \end{aligned}$$

Se  $A$  è un dominio, allora  $S = A \setminus \{0\}$ <sup>a</sup> è una parte moltiplicativa, infatti,  $\forall x, y \in S$ , ovvero  $x \neq 0$  e  $y \neq 0$ , vale  $xy \neq 0$ , dunque  $xy \in S$ .

- Per la [Proposizione 2.66](#) sappiamo già che  $A \subset S^{-1}A$ , ed ora abbiamo dimostrato che  $S^{-1}A$  è un campo, ci resta da verificare che  $S^{-1}A (= Q(A))$  sia effettivamente il più piccolo campo che contiene  $A$ . Sia  $K$  un campo tale che  $A \subset K$ , allora  $\frac{1}{a} \in K, \forall a \in A \setminus \{0\}$ , ovvero  $K$  contiene tutti gli inversi degli elementi di  $A$ , allora,  $\forall b \in A, \forall a \in A \setminus \{0\}$ , cioè  $K$  contiene tutti gli elementi di  $S^{-1}A$ ;

$$\frac{b}{a} \in K \implies Q(A) = S^{-1}A \subset K$$

pertanto, essendo contenuto in ogni campo che contiene  $A$ , e contenendolo a sua volta,  $Q(A)$  è il più piccolo campo che contiene  $A$ .

### correzioni varie per chiarezza

\item Per la [\hyperref\[2.66\]{Proposizione 2.66}](#) sappiamo già che  $A \subset Q(A)$ , ed ora abbiamo dimostrato che  $Q(A)$  è un campo, ci resta da verificare che  $Q(A)$  sia effettivamente il più piccolo campo che contiene  $A$ .

Sia  $K$  un campo tale che  $A \subset K$ , allora  $\frac{1}{a} \in K \quad \forall a \in A \setminus \{0\}$ , ovvero  $K$  contiene gli inversi di tutti gli elementi non nulli di  $A$ ;

allora  $K$  contiene anche tutti gli elementi di  $Q(A)$ :

$$[\forall b \in A, \forall a \in A \setminus \{0\} \frac{1}{a} \cdot \frac{b}{a} = \frac{b}{a} \in K \implies S^{-1}A = Q(A) \subset K]$$

pertanto, essendo contenuto in ogni campo che contiene  $A$ ,  $Q(A)$  è il più piccolo campo che contiene  $A$ .

rr. 2986, 2991; p. 77

poiché  $P$  è primo, dunque  $xy \in A \setminus P = S$ . In questo caso indichiamo  $S^{-1}A = A_p$  e prende il nome di **localizzato** dell'anello  $A$  all'ideale  $P$ .

**Osservazione 2.71 —** Dato il localizzato di  $A$  a  $P$ ,  $A_p$ , si osserva che esso è un **anello locale**, ovvero un anello che ha un unico ideale massimale.

typo

$$p \rightarrow P$$

poiché  $P$  è primo, dunque  $xy \in A \setminus P = S$ . In questo caso indichiamo  $S^{-1}A = A_P$  e prende il nome di **localizzato** dell'anello  $A$  all'ideale  $P$ .

Dato il localizzato di  $A$  a  $P$ ,  $A_P$ , si osserva che esso è un **anello locale**, ovvero un anello che ha un unico ideale massimale.

---

**Esercizio 2.73.** Dati  $A = \mathbb{Z}$ ,  $P = 2\mathbb{Z}$  e  $S = \mathbb{Z} \setminus 2\mathbb{Z}$ , verificare che l'ideale  $(2)\mathbb{Z}_{(2)}$  è l'unico ideale massimale di  $\mathbb{Z}_{(2)}$ .

*Soluzione.* La tesi è equivalente a mostrare che  $\mathbb{Z}_{(2)}^* = \mathbb{Z}_{(2)} \setminus (2)\mathbb{Z}_{(2)}$ . Infatti, sappiamo già che  $(2)\mathbb{Z}_{(2)}$  è un ideale, mentre qualunque ideale non contenuto in esso contiene necessariamente un elemento invertibile ed è perciò non proprio. Se  $\frac{a}{b} \notin (2)\mathbb{Z}_{(2)}$  allora sia  $a$  che  $b$  sono dispari, dunque  $\frac{b}{a} \in \mathbb{Z}_{(2)}$  ed è chiaramente l'inverso di  $\frac{a}{b}$ . Viceversa se  $\frac{a}{b}$  è invertibile esiste  $\frac{c}{d} \in \mathbb{Z}_{(2)}$  tale che  $\frac{ac}{bd} = 1$ , cioè  $ac = bd$ . Se uno tra  $a$  e  $c$  fosse pari lo sarebbe anche  $bd$ , e poiché 2 è primo uno tra  $b$  e  $d$  sarebbe pari, contraddicendo la definizione di  $\mathbb{Z}_{(2)}$ . Dunque  $\frac{a}{b} \in \mathbb{Z}_{(2)} \setminus (2)\mathbb{Z}_{(2)}$ .<sup>34</sup> □

### riscrittura con aggiunte

La tesi è equivalente a mostrare che  $\mathbb{Z}_{(2)}^* = \mathbb{Z}_{(2)} \setminus (2)\mathbb{Z}_{(2)}$ .  
 Infatti, sappiamo già che  $(2)\mathbb{Z}_{(2)}$  è un ideale (i suoi elementi sono del tipo  $\frac{a}{b}$  con  $a$  pari e  $b$  dispari), mentre qualunque ideale non contenuto in esso contiene necessariamente un elemento invertibile (cioè un elemento del tipo  $\frac{a}{b}$  con  $a$  e  $b$  entrambi dispari) ed è perciò non proprio, quindi non massimale.

---

**Proposizione 2.76 (Ideali di  $S^{-1}A$ )**

Sia  $I \subset A$  e sia  $S^{-1}A$  l'insieme costruito come sopra, allora:

- (1)  $S^{-1}I$  è un ideale di  $S^{-1}A$ .
- (2)  $\forall J \subset S^{-1}A, \exists I \subset A$  tale che  $J = S^{-1}I$  (cioè ogni ideale di  $S^{-1}A$  si ottiene da un ideale di  $A$ , considerandone il relativo anello delle frazioni).
- (3)  $S^{-1}I$  è un ideale proprio di  $S^{-1}A$  se e solo se  $I \cap S = \emptyset$ .
- (4) Sia  $P$  un ideale primo di  $A$ , con  $P \cap S = \emptyset$ , allora  $S^{-1}P$  è un ideale primo di  $S^{-1}A$ .

*Dimostrazione.* Dimostriamo le singole affermazioni:

- (1) Per verificare che  $S^{-1}I$  sia un ideale verifichiamo prima la chiusura per somma:

riscrittura, typo

*sia* → è

\item \$\forall J \subset S^{-1}A\$, \$\exists I \subset A\$ tale che \$J = S^{-1}I\$ (cioè ogni ideale di \$S^{-1}A\$ si ottiene localizzando un ideale di \$A\$).

\item Per verificare che  $S^{-1}I$  è un ideale verifichiamo prima la chiusura per somma:

rr. 3054, 3061; p. 79

$$\frac{a}{s} \cdot \frac{x}{t} = \underbrace{\frac{ax}{st}}_{\in S} \in S^{-1}I \quad \forall \frac{a}{s} \in S^{-1}A$$

- (2) Sia  $J \subset S^{-1}A$  un ideale, per quanto detto nella [Proposizione 2.66](#), sappiamo che  $S^{-1}A$  è un'estensione di  $A$ , inoltre se consideriamo  $f^{-1}(J)$ , che per il [Lemma 2.35](#), sappiamo essere un ideale, ed in particolare una contrazione di  $J$  ad  $A$ , abbiamo che:

$$f^{-1}(J) = J \cap A = I \subset A$$

vogliamo mostrare che vale  $J = S^{-1}I$ . Osserviamo che  $\forall x \in I$  si ha  $f(x) = \frac{x}{1} \in J$ , dunque:

$$\underbrace{\frac{1}{s}}_{\in S^{-1}A} \cdot \underbrace{\frac{x}{1}}_{\in I} = \frac{x}{s} \in J \implies S^{-1}I \subseteq J$$

spazi

$$\left[ \frac{a}{s} \cdot \frac{x}{t} = \overbrace{ax}^{\in I} \in \underbrace{st}_{\in S} \in S^{-1}I \quad \forall \frac{a}{s} \in S^{-1}A \right]$$

$$\left[ \underbrace{\frac{1}{s}}_{\in S^{-1}A} \cdot \frac{x}{1} = \frac{x}{s} \in J \implies S^{-1}I \subseteq J \right]$$


---

rr. 3066, 3067; p. 79

ovvero il numeratore di ogni elemento in  $S^{-1}J$  è un elemento di  $I$ , dunque considerando l'anello delle frazioni  $S^{-1}I$  esso contiene tutte quelle di  $S^{-1}J$ , da cui si conclude  $\frac{x}{s} \in S^{-1}I \implies J \subseteq S^{-1}I$ .

- (3) Dimostriamo la negazione<sup>35</sup>, ovvero  $S^{-1}I$  non proprio equivale a  $S^{-1}I = S^{-1}A$ , ma essendo il primo un ideale questo è vero se e solo se:

$$\frac{1}{1} \in S^{-1}I \iff \exists x \in I, \exists s \in S : \frac{1}{1} = \frac{x}{s}$$

riscrittura

alla fine del punto (2) avevo scritto [Da riguardare], ma non ricordo perché

\item Dimostriamo la negazione\footnote{Poiché trattandosi di un'equivalenza logica va bene lo stesso.}: sia  $S^{-1}I$  non proprio, questo equivale a  $S^{-1}I = S^{-1}A$ , ma essendo il primo un ideale questo è vero se e solo se:

rr. 3066, 3067, 3074-3075, 3077-3078; p. 79

$s \quad t$

ciò è equivalentemente al fatto che  $\exists \sigma \in S$  e  $\exists p \in P$  tali per cui:

$$\frac{ab}{st} = \frac{p}{\sigma} \iff ab\sigma = \underbrace{p}_{\in P} st \in P \implies ab\sigma \in P$$

ma, essendo per ipotesi che  $\sigma \in P$  e  $P \cap S = \emptyset$ , allora  $ab \in P$ , e poiché  $P$  è primo si deve avere  $a \in P$  e  $b \in P$ , e quindi la frazione di uno dei due deve essere quella in  $S^{-1}P$ :  $\frac{a}{s} \in S^{-1}P$  o  $\frac{b}{t} \in S^{-1}P$  e quindi  $S^{-1}P$  primo.

riscrittura e tipo vari

ciò è equivalente al fatto che  $\exists \sigma \in S$  e  $\exists p \in P$  tali che:

$$[\frac{ab}{st} = \frac{p}{\sigma} \iff ab\sigma = p st \in P]$$

ma, essendo per ipotesi che  $\sigma \in S$  e  $P \cap S = \emptyset$ , allora  $ab \in P$ , perché  $P$  è primo;

inoltre, sempre perché  $P$  è primo, si deve avere  $a \in P$  quad \text{o} \quad b \in P \implies \frac{a}{s} \in S^{-1}P \quad \text{o} \quad \frac{b}{t} \in S^{-1}P e quindi  $S^{-1}P$  primo.

**Osservazione 2.80 (Equivalenza delle condizioni)** — Osserviamo che le tre condizioni date sono equivalenti, infatti, per quanto riguarda (i) e (iii) si ha:

$$a | a' \iff (a') \subseteq (a) \quad \text{e} \quad a' | a \iff (a) \subseteq (a')$$

dunque se sono vere entrambe le condizioni (i) e (iii) sono equivalenti. Dobbiamo da verificare che (i)  $\implies$  (ii), dalle due divisibilità segue che:

$$a' = xa \quad \text{e} \quad a = ya' \implies a = yxa \implies a(1 - xy) = 0$$

poiché  $a \neq 0$ , ed  $A$  dominio per ipotesi si ha che  $xy = 1 \implies y \in A^*$ , ovvero la (ii). Viceversa, assumiamo (ii) e deduciamo (iii):<sup>a</sup>

$$a = ua' \implies a \in (a') \implies (a') \subseteq (a)$$

con  $u \in A^*$ , pertanto  $\exists v \in A^*$  tale che  $uv = vu = 1$ , moltiplicando la prima relazione per  $v$  si ottiene:

$$a' = va \implies a' \in (a) \implies (a) \subseteq (a')$$

e si conclude  $(a) \subseteq (a')$ .

<sup>a</sup>A questo punto sappiamo che già che (i) e (iii) sono equivalenti, quindi non è necessario fare verifiche distinte.

## punteggiatura, spazi, tipo vari

dunque se sono vere entrambe le condizioni, (i) e (iii) sono equivalenti.  
Dobbiamo verificare che (i)  $\iff$  (ii), dalle due divisibilità segue che:

$$\begin{aligned} & \forall [ a^{\prime\prime} = xa \quad \text{e} \quad a = y a^{\prime\prime} \implies a = yxa \\ & \implies a(1-xy) = 0 \end{aligned}$$

$$\begin{aligned} & \forall [ a = ua^{\prime\prime} \implies a \in (a^{\prime\prime}) \implies (a) \subseteq (a^{\prime\prime}) \\ & (a^{\prime\prime}) \end{aligned}$$

$$\begin{aligned} & \forall [ a^{\prime\prime} = va \implies a^{\prime\prime} \in (a) \implies (a^{\prime\prime}) \subseteq (a) \\ & ] \\ & \text{e si conclude } a = (a^{\prime\prime}). \end{aligned}$$

rr. 3161-3170; p. 81

da cui, sfruttando il fatto che  $A$  è un dominio segue:

$$d = u d' = u v d \implies d(1 - uv) = 0 \implies uv = 1 \implies u, v \in A^*$$

e quindi  $d \sim d'$  per definizione.  $\square$

**Definizione 2.83.** Dato un dominio  $A$  e  $x \in A$ , con  $x \notin A^* \cup \{0\}$ ,  $x$  si dice **primo** se  $\forall a, b \in A$ :

$$x \mid ab \implies x \mid a \vee x \mid b$$

aggiunta (è stata dimostrata solo una freccia)

e quindi  $d \sim d'$  per definizione.

Viceversa, se  $d$  è un massimo comune divisore di  $a$  e  $b$  e  $d \sim d'$ , allora:

$$\begin{aligned} & \exists d \mid d' \quad \text{e} \quad d \mid d' \\ & \end{aligned}$$

quindi

$$\begin{aligned} & \exists d \mid d \mid d' \mid a \quad \text{e} \quad d \mid d' \mid b \\ & \end{aligned}$$

inoltre  $\forall x \in A$  tale che  $x \mid a$  o  $x \mid b$

$$\begin{aligned} & \exists x \mid d \mid d' \mid x \\ & \end{aligned}$$

cioè anche  $d'$  è un massimo comune divisore di  $a$  e  $b$ .

\end{proof}

Come conseguenza l'M.C.D è definito a meno di associati.

\begin{definition}

rr. 3197, 3199; p. 81

essendo  $x$  primo, allora  $x \mid a$  o  $x \mid b$ , assumiamo (WLOG) che  $x \mid a$ , allora:

$$a = xc \implies x = bcx \implies x(1 - bc) = 0$$

poiché  $A$  è un dominio, e poiché  $x \neq 0$  per ipotesi segue che:

$$bc = 1 \implies b, c \in A^*$$

aggiunte

$$\begin{aligned} & \exists a = xc \implies ab = xcb \implies x = bcx \implies x(1 - bc) = 0 \\ & \end{aligned}$$

poiché  $A$  è un dominio, e poiché  $x \neq 0$  per ipotesi ( $x$  primo) segue che:

(1) Sia  $(x)$  un ideale primo, ovvero:

$$ab \in (x) \iff a \in (x) \vee b \in (x)$$

ciò è equivalente al richiedere che  $x | a$  o  $x | b$ , ovvero che  $x$  sia primo in  $A$ .

(2) Dimostriamo separatamente le due implicazioni. Sia  $x$  irriducibile e supponiamo che sia  $(x) \subseteq (y) \subsetneq A$ , dunque  $\exists z \in A$  tale che  $x = yz$ , sappiamo che  $y \notin A^*$  (altrimenti sarebbe l'ideale conterebbe l'identità e avremmo  $(y) = A$ ), poiché  $x$  deve essere irriducibile segue necessariamente che  $z \in A^*$  e quindi  $x \sim y$ , cioè:

riscrittura (è stata fatta solo una freccia), rimozione (typo)

```
\item Sia $x \in A$, allora:  
  $[ x \mid ab \iff ab \in (x)  
   ]$  
  $[ x \mid a \vee x \mid b \iff a \in (x) \vee b \in (x)  
   ]$  
da ciò si deduce la tesi.
```

Sia  $x \in A$ , allora:

$$x \mid ab \iff ab \in (x)$$

$$x \mid a \vee x \mid b \iff a \in (x) \vee b \in (x)$$

da ciò si deduce la tesi.

(magari separa le righe con una congiunzione, tipo “e inoltre”)

```
dunque $\exists z \in A$ tale che $x = yz$, sappiamo che $y \not\in A^*$ (altrimenti l'ideale conterebbe l'identità
```

r. 3316; p. 84

Come si osserva  $\alpha$  cade in un quadrato (compreso il bordo) e del quale  $q\beta$  è il multiplo di  $\beta$  più vicino ad  $\alpha$ , pertanto, scelto  $q\beta$  abbiamo:

$$r = \alpha - q\beta$$

## rimozione (typo)

Come si osserva  $\alpha$  cade in un quadrato (compreso il bordo) del quale  $q\beta$  è il multiplo di  $\beta$  più vicino ad  $\alpha$ , pertanto, scelto  $q\beta$  abbiamo:

---

rr. 3382, 3390-3393; p. 86

### Proposizione 2.93 (Ideali di un dominio euclideo)

Dato un dominio euclideo  $A$ , tutti gli ideali di  $A$  sono principali<sup>a</sup> e generati da un elemento di grado minimo.

<sup>a</sup>Quindi ogni dominio euclideo è un PID.

*Dimostrazione.* Sia  $I \subset A$  un ideale, se  $I = \{0\}$ , allora è principale, altrimenti, preso  $I \neq \{0\}$ , vogliamo mostrare che  $I$  è generato da un singolo elemento di grado minimo. Sia  $x \in I$  un elemento di grado minimo (esiste perché  $d(I) \subset \mathbb{N}$  e non vuoto), allora è ovvio che  $(x) \subseteq I$ , viceversa, si ha che  $\forall a \in A$  si può fare la divisione euclidea per  $x$ :

$$a = qx + r \quad d(r) < d(x) \vee r = 0$$

da cui segue che  $r = a - qx \in I$  da cui  $d(x) \leq d(r) \implies r = 0$ , ovvero:

$$a = qx \in (a) \implies I \subseteq (a)$$

## aggiunte varie

Dato un dominio euclideo  $A$ , tutti gli ideali di  $A$  sono principali<sup>a</sup> e generati da un elemento di grado minimo (nell'ideale).

da cui segue che, se  $a \in I$ ,  $r = a - qx \in I$  da cui  $d(x) \leq d(r)$   $\implies r = 0$ , ovvero:  
[  $a = qx \in (a) \implies I \subseteq (a)$   $\forall a \in I \implies I \subseteq (a)$  ]  
Quindi  $I = (a)$ .

**Osservazione 2.96 (M.C.D. nei PID)** — Se  $A$  è un PID e  $x, y \in A$ , non entrambi nulli, osserviamo che l'ideale generato da  $x$  e  $y$  deve essere tale che:

$$(x, y) = (d)$$

con  $d$  un M.C.D.<sup>a</sup> di  $x$  e  $y$ . Infatti:

$$x \in (d) \quad \text{e} \quad y \in (d)$$

dunque  $d \mid x$  e  $d \mid y$ , inoltre, se  $c \mid x$  e  $c \mid y$ , allora  $x, y \in (c)$ , da cui:

$$(d) = (x, y) \subseteq (c) \implies d \in (c) \implies c \mid d$$

dunque  $d$  è un M.C.D. tra  $x$  ed  $y$ .

---

<sup>a</sup>M.C.D. a meno di prodotto per elementi di  $A^*$ .

## riscrittura, aggiunte, typo

con  $d$  un M.C.D. a meno di associati. di  $x$  e  $y$ . Infatti se  $(x, y) = (d)$ , allora:  
 $\forall x \in (d) \quad \text{e} \quad \forall y \in (d) \implies d \mid x \quad \text{e} \quad d \mid y$   
 $\exists c \in A^* \text{ tale che } x = cd \text{ e } y = cd$   
Inoltre, se  $c \mid x$  e  $c \mid y$ , allora  $x, y \in (c)$ , da cui:

## §2.10 Domini a fattorizzazione unica (UFD)

**Definizione 2.97.** Dato  $A$  un dominio, esso si dice **a fattorizzazione unica** (UFD) se  $\forall x \in A, x \notin A^* \setminus \{0\}$  si scrive in modo unico, a meno dell'ordine di fattori e di moltiplicazione per elementi invertibili, come prodotto di elementi irriducibili.

## typo

$$\backslash \rightarrow \cup$$

Dato  $A$  un dominio, esso si dice a fattorizzazione unica (UFD) se  $\forall x \in A, x \notin A^* \setminus \{0\}$ , si scrive in modo

rr. 3473, 3476, 3492; p. 89

è tale che  $\text{M.C.D.}(2, x) = 1$ , ma  $1 \notin (2, x)$ , perché se non fosse così avremmo:

$$1 = 2a(x) + xb(x)$$

che per  $x = 0$  porta a:

$$1 = 2a(0) + 0 \implies 2 \mid 1$$

che è assurdo.

### Teorema 2.101 (Caratterizzazione degli UFD)

Dato un dominio  $A$ , sono fatti equivalenti:

- (1)  $A$  è un UFD.
- (2) Valgono le due condizioni seguenti:
  - (i) Ogni elemento irriducibile è primo.
  - (ii) Ogni catena discendente di divisibilità è stazionaria, ovvero se  $\{a_i\} \subset A$ , con:

$$a_{i+1} \mid a_i \quad \forall i \geq 0$$

allora  $\exists n_0$  tale che  $a_i \sim a_{n_0}$ ,  $\forall i \geq n_0$ .

typo/riscrittura

è tale che  $\text{M.C.D.}(2, x) = 1$ , ma  $1 \not\in (2, x)$ , perché altrimenti avremmo:

che valutata in  $x = 0$  porta a:

\item Ogni catena discendente di divisibilità è stazionaria, ovvero se  $\{a_i\} \subset A$ , con:

rr. 3507-3508; p. 89

**Osservazione 2.103** — Osserviamo che la condizione (ii) può essere riformulata equivalentemente come: ogni catena ascendente di ideali principali è stazionaria, ovvero, considerata  $\{(a_i)\}_{i \geq 0}$ , catena ascendente di ideali di  $A$ :

riscrittura

Osserviamo che la condizione (ii) può essere riformulata equivalentemente come: ogni catena ascendente di ideali principali è stazionaria, ovvero  
data  $\{(a_i)\}_{i \geq 0}$ , catena ascendente di ideali di  $A$ :

---

r. 3521; p. 90

*Dimostrazione.* Per dimostrare il corollario ci basta verificare che per ogni PID valgono le condizioni (i) e (ii) del Teorema 2.101, e ciò è equivalente al dire che ogni PID è un UFD. Sia  $A$  un PID, e sia  $x \in A$  un elemento irriducibile, per quanto visto nella Proposizione 2.95 l'ideale  $(x)$  è massimale in  $A$ , ma dalla (3) del Corollario 2.57, sappiamo quindi che  $(x)$  è primo, e poiché siamo in un dominio vale la (1) della Proposizione 2.86 che ci assicura che  $x$  è primo, dunque vale la (i).

Consideriamo ora una catena ascendente di ideali (principali):

typo/riscrittura

Sia  $A$  un PID, e sia  $x \in A$  un elemento irriducibile, allora dalla (2) della Proposizione 2.86 l'ideale  $(x)$  è massimale in  $A$ , ma dalla (3) del Corollario 2.57, sappiamo quindi che

---

r. 3599; p. 92

- (1) Siano  $f(x), g(x) \in A[x] \setminus \{0\}$ , e  $\deg f(x) = n \geq 0$ ,  $\deg g(x) = m \geq 0$ , essendo  $a_n, b_m \neq 0$ , segue che  $a_n b_m \neq 0$  poiché per ipotesi  $A$  un dominio di integrità, pertanto  $f(x) \cdot g(x) \neq 0$  se  $f(x), g(x) \neq 0 \implies A[x]$  è un dominio d'integrità.

rimozione (stiamo già supponendo  $f(x), g(x) \neq 0$ )

$a_{nb\_m} \neq 0$  poiché per ipotesi  $A$  un dominio di integrità, pertanto  $f(x) \cdot g(x) \neq 0 \implies A[x]$  è un dominio d'integrità.

---

Per verificare la condizione (i) dobbiamo prima caratterizzare gli irriducibili di  $A[x]$ , e fare ciò abbiamo bisogno del Lemma di Gauss.

**Definizione 2.113.** Dato  $A$  un UFD e  $f(x) \in A[x]$ , con  $f(x) = \sum_{i=0}^n a_i x^i$ , si dice **contenuto** di  $f(x)$  l'M.C.D. dei suoi coefficienti:

$$c(f(x)) = (a_0, \dots, a_n)$$

**Osservazione 2.114 —** Il contenuto di un polinomio a coefficienti in un UFD è definito a meno di associati.

**Definizione 2.115.** Dato  $A$  un UFD e  $f(x) \in A[x]$ ,  $f(x)$  si dice **primitivo** se  $c(f(x)) \sim 1$ .

**Osservazione 2.116 —** Ovviamente dato  $f(x) \in A[x]$  si ha che:

$$f(x) = c(f(x)) f'(x) \quad c(f'(x)) = 1$$

dove  $f'(x) \in A[x]$  e:

$$f'(x) = \sum_{i=0}^n \frac{a_i}{d} x^i \quad \frac{a_i}{d} \in A, \left( \frac{a_0}{d}, \dots, \frac{a_n}{d} \right) = 1$$

## aggiunte e riscritture varie

Per verificare la condizione (i) dobbiamo prima caratterizzare gli irriducibili di  $A[x]$ , e per fare ciò abbiamo bisogno del Lemma di Gauss.

```
\[ c(f(x)) = (a_0, \dots, a_n) \in A
```

Il contenuto di un polinomio a coefficienti in un UFD è definito a meno di associati (perché l'M.C.D. lo è).

Dato  $A$  un UFD e  $f(x) \in A[x]$ ,  $f(x)$  si dice **primitivo** se  $c(f(x)) = 1$ .

Dato  $f(x) \in A[x]$  si può scrivere come:

```
\[ f(x) = c(f(x)) f'(\prime)(x) \quad c(f'(\prime)(x)) = 1
```

dove  $f'(\prime)(x) \in A[x]$  primitivo e, detto  $d$  un M.C.D. dei coefficienti di  $f$ :

- Se  $c(f(x)) = c(g(x)) = 1$ , dunque  $f(x)$  e  $g(x)$  sono primitivi, vogliamo verificare che  $c(f(x)g(x)) = 1$ ; se  $f(x)g(x)$  non fosse primitivo (ovvero associato ad 1) allora  $c(f(x)g(x))$  non sarebbe invertibile (gli elementi invertibili sono associati ad 1),

ovvero esisterebbe  $p$  primo tale che  $p \mid c(f(x)g(x))$ , consideriamo la proiezione modulo  $(p)$ :

$$\pi_{(p)} : A[x] \longrightarrow \frac{A}{(p)}[x] : f(x) \longmapsto \overline{f(x)}$$

con  $\overline{f(x)} \neq 0$  in quanto  $p \nmid c(f(x))$ , analogamente  $\pi_{(p)}(g(x)) = \overline{g(x)} \neq 0$ , poiché  $p \nmid c(g(x))$ , ma  $\pi_{(p)}(f(x)g(x)) = \overline{f(x)g(x)} = 0$ , perché avevamo supposto che  $p \mid c(f(x)g(x))$ , ma questo è assurdo in quanto  $\frac{A}{(p)}$  è un dominio e quindi, per quanto detto,  $A$  dominio  $\implies A[x]$  dominio, ovvero  $\frac{A}{(p)}[x]$  è un dominio, da cui  $c(f(x)g(x)) = 1$ .

## riscrittura

\item Dati  $f(x)$  e  $g(x)$  primitivi, vogliamo verificare che  $f(x)g(x)$  è primitivo;

se così non fosse, ovvero  $c(f(x)g(x)) \neq 1$ , esisterebbe  $p$  primo tale che  $p \mid c(f(x)g(x))$

\footnote{Stiamo usando il fatto che  $A$  è UFD: basta prendere un fattore irriducibile della fattorizzazione di  $c(f(x)g(x))$  (che esiste unica) ed, essendo  $A$  UFD, questo è anche un primo.}.

Consideriamo la proiezione modulo  $(p)$ :

con  $\pi_{(p)}(f(x)) = \overline{f(x)} \neq 0$  in quanto  $p \nmid c(f(x)) = 1$ , analogamente  $\overline{g(x)} \neq 0$ , ma  $\pi_{(p)}(f(x)g(x)) = \overline{f(x)g(x)} = 0$ , perché avevamo supposto che  $p \mid c(f(x)g(x))$ .

Ma questo è assurdo in quanto  $\frac{A}{(p)}$  è un dominio, quindi  $c(f(x)g(x)) = 1$ .

- Consideriamo ora il caso generale, sia  $f(x) = c(f(x))f'(x)$ , con  $f'(x)$  primitivo, e analogamente  $g(x) = c(g(x))g'(x)$ , con  $g'(x)$  primitivo, abbiamo che:

$$h(x) = f(x)g(x) = c(f(x))c(g(x))\cancel{g'(x)}\cancel{f'(x)}$$

dove  $h'(x) = \cancel{g'(x)}\cancel{f'(x)}$  è primitivo perché prodotto di polinomi primitivi, dunque:

$$h(x) = c(h(x))h'(x)$$

e uguagliando i contenuti si ha:

$$\begin{aligned} c(h(x)) \underbrace{c(h'(x))}_{=1} &= c(f(x))c(g(x)) \underbrace{c(\cancel{g'(x)}\cancel{f'(x)})}_{=1} \implies \\ c(h(x)) &= c(f(x)g(x)) = c(f(x))c(g(x)) \end{aligned}$$

## correzioni minori

$$\boxed{h(x) = f(x)g(x) = c(f(x))c(g(x))f^{\prime}(x)g^{\prime}(x)}$$

dove  $h^{\prime}(x) = f^{\prime}(x)g^{\prime}(x)$  è primitivo perché prodotto di polinomi primitivi, dunque:

$$\begin{aligned} c(h(x))\underbrace{c(h^{\prime}(x))}_{=1} &= \\ c(f(x))c(g(x))\underbrace{c(f^{\prime}(x)g^{\prime}(x))}_{=1} \implies & \\ c(f(x)g(x)) &= c(h(x)) = c(f(x))c(g(x)) \end{aligned}$$


---

**Corollario 2.118**

Siano  $f(x), g(x) \in A[x]$ , con  $c(f(x)) = 1$  e  $f(x) \mid g(x)$  in  $K[x]$ , (con  $K$  campo dei quozienti di  $A$ , allora  $f(x) \mid g(x)$  in  $A[x]$ ).

*Dimostrazione.* Per ipotesi sappiamo che  $f(x) \mid g(x)$  in  $K[x]$ , ovvero  $\exists h(x) \in K[x]$  tale che  $g(x) = f(x)h(x)$ , allora  $\exists d \in A$  tale che:

$$h_1(x) = dh(x) \in A[x]$$

(stiamo "cancellando" il denominatore), dunque:

$$dg(x) = f(x)h_1(x) \in A[x]$$

da cui per il [Lemma di Gauss](#):

$$dc(g(x)) = c(f(x)h_1(x)) = c(f(x))c(h_1(x)) = c(h_1(x)) \implies d \mid c(h_1(x))$$

dove abbiamo usato nell'ultimo passaggio il fatto che  $c(f(x)) = 1$ , dunque abbiamo  $\frac{h_1(x)}{d} = h(x) \in A[x]$  e quindi la divisibilità iniziale era anche in  $A[x]$ .  $\square$

## aggiunta, riscritture varie

Nelle prossime proposizioni indicheremo con  $K$  il campo dei quozienti di  $A$ .

```
\begin{corollary}
\label{2.118}
Siano $f(x), g(x) \in A[x]$, con $f$ primitivo e $f(x) \mid g(x)$ in $K[x]$,
allora $f(x) \mid g(x)$ in $A[x]$.
\end{corollary}
```

Per ipotesi sappiamo che  $f(x) \mid g(x)$  in  $K[x]$ , ovvero  $\exists h(x) \in K[x]$  tale che  $g(x) = f(x)h(x)$ .

Possiamo "cancellare" i denominatori moltiplicando per un loro m.c.m., quindi  $\exists d \in A$  tale che:

e dunque:

dove abbiamo usato nell'ultimo passaggio il fatto che  $c(f(x)) = 1$ , dunque abbiamo  $h(x) = \frac{h_1(x)}{d} \in A[x]$

**Corollario 2.119**

Sia  $f(x) \in A[x]$  e  $f(x) = g(x)h(x)$  in  $K[x]$  (con  $K$  campo dei quozienti di  $A$ ), con  $\deg f(x), \deg g(x) \geq 1$ , allora esiste  $\delta \in K^*$  tale che  $g_1(x) = \delta g(x) \in A[x]$ ,  $h_1(x) = \delta^{-1}h(x) \in A[x]$  e  $f(x) = g_1(x)h_1(x)$ .

*Dimostrazione.* Analogamente a quanto fatto per il corollario precedente, sappiamo che  $\exists d \in A$  tale che  $g_1(x) = dg(x) \in A[x]$  (stiamo di nuovo "eliminando" i denominatori, ad esempio moltiplicando per l'm.c.m.), dunque:

$$f(x) = dg(x)d^{-1}h(x) = g_1(x)(d^{-1}h(x)) = c(g_1(x))g'_1(x)(d^{-1}h(x))$$

con  $g'_1(x) \in A[x]$  primitivo (dividendo per il contenuto, che è un invertibile di  $A$ , siamo rimasti in  $A[x]$ ), pertanto abbiamo:

$$f(x) = g'_1(x) \underbrace{(c(g_1(x))d^{-1}h(x))}_{\in K[x]}$$

ovvero  $g'_1(x) \mid f(x)$  in  $K[x]$ , ma allora per il Corollario 2.118 segue che  $g'_1(x) \mid f(x)$  in  $A[x]$ , dunque:

$$h_1(x) = \frac{c(g_1(x))}{d} h(x)$$

$\underbrace{d}_{=\delta^{-1}}$

abbiamo quindi determinato  $\delta$  e  $\delta^{-1}$  richiesti dalla tesi. □

## aggiunte, tipo, riscritture varie, rimozione

Sia  $f(x) \in A[x]$  e  $f(x) = g(x)h(x)$  in  $K[x]$ , con  $\deg f(x), \deg g(x) \geq 1$ , allora esiste  $\delta \in K^*$  tale che  $g_0(x) = \delta g(x) \in A[x]$ ,  $h_0(x) = \delta^{-1}h(x) \in A[x]$  e  $f(x) = g_0(x)h_0(x)$  (in  $A[x]$ ).

\[ f(x) = dg(x)d^{-1}h(x) = g\_1(x)(d^{-1}h(x)) = c(g\_1(x))g\_1'(x)(d^{-1}h(x)) \] \footnote{Non possiamo usare  $g_1(x) = dg(x)$  e  $h_1(x) = d^{-1}h(x)$  perché in generale  $d^{-1} \notin A^*$ , quindi  $h_1(x) \notin A[x]$ .} \\ \]

\[ g\_0(x) = g\_1'(x) = \underbrace{\frac{d}{c(g\_1(x))}}\_{= \delta} g(x) \] \[ h\_0(x) = \underbrace{\frac{c(g\_1(x))}{d}}\_{= \delta^{-1}} h(x) \] \\ \end{proof}

rr. 3727, 3729-3730; p. 94

**Teorema 2.122 (Caratterizzazione degli irriducibili di  $A[x]$ )**

Dato  $A$  UFD, gli elementi irriducibili di  $A[x]$  sono tutti e soli quelli che soddisfano una tra le seguenti:

- (1)  $f(x) \in A$  irriducibile in  $A$ .
- (2)  $f(x) \in A[x]$ , con  $\deg f(x) \geq 1$ ,  $c(f(x)) = 1$  e  $f(x)$  irriducibile in  $K[x]$  (anello dei polinomi a coefficienti nel campo dei quozienti di  $A$ ).

rimozione, riscrittura

Dato  $A$  UFD, gli elementi irriducibili di  $A[x]$  sono tutti e soli:

\item le costanti irriducibili in  $A$ ;  
\item i polinomi non costanti, primitivi, irriducibili in  $K[x]$ .

rr. 3737, 3740-3741; p. 95

1. Se  $f(x) \in A$ , dunque è costante, allora, come già osservato in precedenza, si ha:

$$f(x) = g(x)h(x) \implies \deg g(x) + \deg h(x) = \deg f(x) = 0$$

dove l'implicazione è data dal fatto che siamo in un dominio, dunque segue che  $\deg g(x) = \deg h(x) = 0$ , pertanto  $g(x), h(x) \in A$ , per cui  $f(x)$  è irriducibile in  $A[x]$  se e solo se  $f(x)$  è irriducibile in  $A$  (che è la stessa cosa che avevamo già osservato dicendo che  $(A[x])^* = A^*$ ).

riscrittura, rimozione, typo

\item Se  $f(x)$  è costante,  $f(x) \in A$ , allora, come già osservato in precedenza, si ha:

$$\begin{aligned} & [ f(x) = g(x)h(x) \implies \deg g(x) + \deg h(x) = \deg f(x) = 0 \\ & ] \end{aligned}$$

dunque segue che  $\deg g(x) = \deg h(x) = 0$ , pertanto anche  $g(x)$  e  $h(x)$  sono costanti,  $g(x), h(x) \in A$ ,

per cui  $f(x)$  è irriducibile in  $A[x]$  se e solo se  $f(x)$  è irriducibile in  $A$  (che è la stessa cosa che avevamo già osservato dicendo che  $(A[x])^* = A^*$ ).

2. Sia  $f(x)$  con  $\deg f(x) \geq 1$ . Supponiamo che  $f(x)$  sia irriducibile in  $A[x]$ , abbiamo che:

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

con  $c(f(x))$  invertibile in  $A[x]$ ,  $c(f(x)) \in (A[x])^* = A^*$  (per quanto detto al punto (1)), d'altra parte, sia  $f(x) = g(x)h(x)$  in  $K[x]$ , allora per il Corollario 2.119, possiamo scriverlo come prodotto di polinomi dello stesso grado in  $A[x]$ :

$$f(x) = g_1(x)h_1(x) \quad \text{con} \quad \deg g_1(x) = \deg g(x), \deg h_1(x) = \deg h(x)$$

poiché  $f(x)$  è irriducibile in  $A[x]$  deve essere che  $g_1(x)$  o  $h_1(x)$  sono invertibili. Abbiamo quindi che  $\deg g_1(x) = 0$  o  $\deg h_1(x) = 0$ , da cui  $\deg g(x) = 0$  o  $\deg h(x) = 0$ , ovvero  $g(x) \in (K[x])^*$  o  $h(x) \in (K[x])^*$ , dunque  $f(x)$  è irriducibile in  $K[x]$ . Verifichiamo il viceversa, sia  $f(x)$  primitivo ed irriducibile in  $K[x]$ , e sia  $f(x) = g(x)h(x)$  in  $A[x]$  (e anche in  $K[x]$ ), poiché  $f(x)$  è irriducibile in  $K[x]$   $g(x)$  o  $h(x)$  sono invertibili in  $K[x]$  e quindi costanti, supponiamo quindi ad esempio che sia  $g(x) \in A$ , da ciò segue che:

$$1 = c(f(x)) = c(g(x)h(x)) = c(g(x))c(h(x)) = gc(h(x))$$

dove nell'ultima uguaglianza abbiamo usato il fatto che, essendo  $g(x)$  costante, allora è uguale al suo contenuto, dunque  $g \in A^* (= (A[x])^*)$ , pertanto  $f(x)$  è irriducibile in  $A[x]$ .

riscritture varie (inoltre ho preferito prima mostrare che i polinomi primitivi irriducibili in  $K[x]$  sono irriducibili in  $A[x]$  e poi mostrare che non ce ne sono altri)

[continua ...]

\item Sia  $f(x) \in A[x]$  non costante,  $\deg f(x) \geq 1$ . \\ Supponiamo  $f(x)$  primitivo e irriducibile in  $K[x]$  e sia  $f(x) = g(x)h(x)$  in  $A[x]$  (e quindi anche in  $K[x]$ ). Poiché  $f(x)$  è irriducibile in  $K[x]$ , o  $g(x)$  o  $h(x)$  è invertibile in  $K[x]$  e quindi costante; supponiamo (WLOG) che sia  $g(x) = g \in A$ , da ciò segue che:

$$\begin{aligned} 1 &= c(f(x)) = c(g(x)h(x)) = c(g(x))c(h(x)) = g \cdot c(h(x)) \\ &\quad \end{aligned}$$

dove nell'ultima uguaglianza abbiamo usato il fatto che, essendo  $g(x)$  costante, è uguale al suo contenuto, dunque  $g(x) = g \in A^* = (A[x])^*$  (osservazione 2.112), pertanto  $f(x)$  è irriducibile in  $A[x]$ . \\ Viceversa, supponiamo  $f(x)$  irriducibile in  $A[x]$  e sia  $f(x) = g(x)h(x)$  in  $K[x]$ . Allora per il \hyperref[2.119]{Corollario 2.119}, possiamo scriverlo come prodotto di polinomi dello stesso grado in  $A[x]$ :

$$\begin{aligned} f(x) &= g_1(x)h_1(x) \quad \text{\texttt{quad}} \quad \text{\texttt{text\{con\}}} \sim \deg g_1(x) = \deg g(x), \sim \deg h_1(x) = \deg h(x) \\ &\quad \end{aligned}$$

Poiché  $f(x)$  è irriducibile in  $A[x]$  deve essere che o  $g_1(x)$  o  $h_1(x)$  è invertibile in  $A[x]$ , cioè appartiene a  $(A[x])^* = A^*$  (osservazione 2.112). In particolare  $\deg g_1(x) = 0$  o  $\deg h_1(x) = 0$ , da cui  $\deg g(x) = 0$  o  $\deg h(x) = 0$ , cioè sono costanti in  $K[x]$ . Ma dato che  $K \setminus \{0\} = K^*$  e sia  $g(x)$  che  $h(x)$  non sono nulli (perché altrimenti anche  $f(x)$  sarebbe nullo), allora o  $g(x)$  o  $h(x)$  è invertibile in  $K$ , cioè appartiene a  $K^* = (K[x])^*$  (osservazione 2.112). Dunque  $f(x)$  è irriducibile in  $K[x]$ .

---

rr. 3770-3779; p. 95-96

- Se  $\deg f(x) = 0$ , ovvero  $f(x) = f \in A$ , dunque se  $f$  è irriducibile in  $A$ , essendo  $A$  UFD, allora  $f$  è primo in  $A$ ; infatti abbiamo che:

$$f | gh \implies f = c(f) | c(gh) = c(g)c(h) \implies f | c(g) = g \quad \text{o} \quad f | c(h) = h$$

dunque  $f$  primo.

- Sia  $f(x)$  primitivo e irriducibile in  $K[x]$ , con  $\deg f(x) \geq 1$ , si osserva che  $K[x]$  è euclideo, dunque  $f(x)$  è primo in  $K[x]$  (poiché avevamo detto che ED  $\subset$  UFD), dunque se:

$$f(x) | g(x)h(x) \quad \text{in } A[x]$$

allora  $f(x) | g(x)$  o  $f(x) | h(x)$  in  $K[x]$ . Avendo supposto che  $f(x)$  è primitivo, allora per il Corollario 2.118:

$$f(x) | g(x)h(x) \quad \text{in } A[x]$$

## correzioni e riscritture varie

```
\begin{itemize}
    \item Sia $f$ costante, ovvero $f(x) = f \in A$. Allora, per la caratterizzazione precedente, $f$ irriducibile in $A[x]$ implica $f$ irriducibile in $A$, quindi $f$ è primo in $A$, dato che $A$ è UFD. Passando ai contenuti e applicando il \hyperref[gauss]{Lemma di Gauss} abbiamo che
        \begin{multiline*}
            f \mid g(x)h(x) \implies f = c(f) \mid c(g(x)h(x)) = c(g(x))c(h(x)) \\
            \implies f \mid c(g(x)) \mid g(x) \quad \text{quad text o quad} \quad f \mid c(h(x)) \\
            \mid h(x)
        \end{multiline*}
        dunque $f$ è primo anche in $A[x]$.
    \item Sia $f(x)$ primitivo e irriducibile in $K[x]$, con $\deg f(x) \geq 1$.
        Si osserva che $K[x]$ è euclideo, quindi $f(x)$ è primo in $K[x]$ (poiché ED $\implies$ UFD).
        Dunque se $f(x) \mid g(x)h(x)$ in $A[x]$ (e quindi in $K[x]$), allora $f(x) \mid g(x)$ o $f(x) \mid h(x)$ in $K[x]$.
        Avendo supposto $f(x)$ primitivo, per il \hyperref[2.118]{Corollario 2.118}
        $f(x) \mid g(x)$ o $f(x) \mid h(x)$ in $A[x]$.
\end{itemize}
```

*Dimostrazione.* Si osserva che per il Lemma di Gauss si ha che:

$$f(x) \mid g(x) \implies c(f(x)) \mid c(g(x)) \quad \text{e} \quad f'(x) \mid g'(x)$$

infatti, se  $g(x) = f(x)h(x) \implies c(g(x))g'(x) = c(f(x))f'(x)c(h(x))c'(x)$ , ma per quanto detto  $c(g(x)) = c(f(x)h(x)) = c(f(x))c(h(x))$ , da cui  $f'(x) \mid g'(x)$ . Alla successione  $\{f_i(x)\}$  possiamo quindi associare le successioni  $\{c(f_i(x))\}$  e  $\{f'_i(x)\}$ , per quanto abbiamo detto si ha:

$$c(f_{i+1}(x)) \mid c(f_i(x)) \quad \text{e} \quad f'_{i+1}(x) \mid f'_i(x) \quad \forall i \geq 0$$

dove la successione  $\{c(f_i(x))\}$  è stazionaria, in quanto è una catena descendente di divisibilità dell'UFD  $A$ , dunque:

$$\exists m_0 : c(f_i(x)) \sim c(f_{m_0}(x)) \quad \forall i \geq m_0$$

spazi, tipo vari

*descendete*  $\rightarrow$  *descendente*

$$\begin{aligned} & \forall [ f(x) \mid g(x) \implies c(f(x)) \mid c(g(x)) \quad \text{e} \quad \\ & f^{\prime(\prime)}(x) \mid g^{\prime(\prime)}(x) \end{aligned}$$

infatti, se  $g(x) = f(x)h(x) \implies c(g(x))g^{\prime(\prime)}(x) = c(f(x))f^{\prime(\prime)}(x)c(h(x))h^{\prime(\prime)}(x)$ ,  
ma per quanto detto  $c(g(x)) = c(f(x)h(x)) = c(f(x))c(h(x))$ , da cui  
 $f^{\prime(\prime)}(x) \mid g^{\prime(\prime)}(x)$ .

dove la successione  $\{c(f_i(x))\}$  è stazionaria, in quanto è una catena descendente di divisibilità dell'UFD  $A$ , dunque:

rr. 3806, 3808, 3816; p. 96

$$\exists d_0 : \deg f'_i(x) \leq \deg f'_{d_0}(x) \quad \forall i \geq d_0$$

pertanto  $\forall i \geq d_0$  abbiamo che  $f'_i(x)$  e  $\deg f'_{i+1}(x)$  hanno lo stesso grado e  $f'_i(x) \mid f'_{d_0}(x)$ , cioè differiscono per una costante, ma essendo entrambi primitivi la costante deve essere un'unità, per cui:

$$f'_i(x) \sim f'_{d_0}(x) \quad \forall i \geq d_0$$

dunque, detto  $n_0 = \max\{m_0, d_0\}$ ,  $\forall i \geq n_0$  vale contemporaneamente che:

$$c(f_i(x)) \sim c(f_{m_0}(x)) \quad \text{e} \quad f'_i(x) \sim f'_{d_0}(x)$$

da cui la tesi:

$$f_i(x) = c(f_i(x))f'_i(x) \sim c(f_{n_0}(x))f'_{d_0}(x) \quad \forall i \geq n_0$$

typo, aggiunta

$$\leq \rightarrow =$$

$$\deg f'_{i+1}(x) \rightarrow f'_{d_0}(x)$$

$$\begin{aligned} & \forall [ \exists d_0 : \deg f_i(x) = \deg f_{d_0}(x) ] \\ & \forall i \geq d_0 \end{aligned}$$

$$\begin{aligned} & \text{pertanto } \forall i \geq d_0 \text{ abbiamo che } f_i(x) \text{ e} \\ & f_{d_0}(x) \text{ hanno lo stesso grado e } f_i(x) \mid f_{d_0}(x), \end{aligned}$$

$$\begin{aligned} & \forall i \geq d_0 : f_i(x) = c(f_i(x))f'_{d_0}(x) \sim c(f_{d_0}(x))f'_{d_0}(x) = \\ & f_{d_0}(x) \end{aligned}$$

---

r. 3820; p. 96

Con la dimostrazione di quest'ultima proposizione abbiamo concluso la dimostrazione del Teorema di Caratterizzazione degli UFD.

rimozione, typo

Con quest'ultima proposizione abbiamo concluso la dimostrazione del fatto che  $A[x]$  è UFD.

---

**Osservazione 2.125 —** Osserviamo che in generale se  $A$  è un PID, allora non è sempre vero che  $A[x]$  sia un PID, ad esempio nel caso di  $\mathbb{Z}$  sappiamo che  $\mathbb{Z}[x]$  non è un PID, in quanto, ad esempio, l'ideale  $I = (2, x)$  non è principale. Analogamente, in generale se  $A$  è un ED, allora non è sempre vero che  $A[x]$  sia un ED, anche qui come controsenso possiamo considerare il caso di  $\mathbb{Z}$  e  $\mathbb{Z}[x]$ .

**Osservazione 2.126 —** Se  $K$  è un campo, allora abbiamo che  $K[x]$  è euclideo, mentre  $K[x, y]$  è un UFD (poiché vale sempre il Teorema di Caratterizzazione degli UFD, e  $K[x]$  è un UFD), ma  $K[x, y]$  non è un PID, in quanto ad esempio  $I = (x, y)$  non è principale.

## punteggiatura e altre correzioni minori

Osserviamo che, in generale, se  $A$  è un PID non è sempre vero che  $A[x]$  è un PID.

Nel caso di  $\mathbb{Z}$  sappiamo che  $\mathbb{Z}[x]$  non è un PID, in quanto, ad esempio, l'ideale  $I = (2, x)$  non è principale.

Analogamente, in generale se  $A$  è un ED non è sempre vero che  $A[x]$  è un ED, (anche qui come controsenso possiamo considerare il caso di  $\mathbb{Z}$  e  $\mathbb{Z}[x]$ ).

Se  $K$  è un campo abbiamo che  $K[x]$  è ED, mentre  $K[x, y]$  è solo UFD (poiché  $K[x]$  ED  $\implies K[x]$  UFD  $\implies K[x, y] = K[x][y]$  UFD),

infatti  $K[x, y]$  non è un PID, in quanto ad esempio  $I = (x, y)$  non è principale.

rr. 3909, 3916; p. 98

## §2.11 Terne pitagoriche

**Definizione 2.129.** Si definiscono **terne pitagoriche** le terne di soluzioni intere dell'equazione:

$$x^2 + y^2 = z^2 \quad x, y, z \in \mathbb{Z}$$

con  $(x, y, z) = 1$ .

Osserviamo che possiamo riformulare il problema negli interi di Gauss nel modo che segue:

$$x^2 + y^2 = (x + iy)(x - iy) = z^2$$

dunque determinare le terne pitagoriche significa risolvere questo problema moltiplicativo in  $\mathbb{Z}[i]$ .

rimozione, aggiunta

Ci limiteremo a studiare le cosiddette terne primitive, dove  $(x, y, z) = 1$  (le altre si ottengono moltiplicando i tre termini per un fattore comune).

r. 3926; p. 98

**Osservazione 2.131 —** Abbiamo che  $x \not\equiv y \pmod{2}$ , infatti, studiando l'equazione modulo 4:

$$x^2 + y^2 \equiv z^2 \pmod{4}$$

dove essendo un quadrato modulo 4 abbiamo che  $z^2 \in \{0, 1\}$ , dunque  $x^2, y^2 \in \{0, 1\}$ , ma non possono essere contemporaneamente pari, altrimenti avremmo che  $(x, y) \neq 1$ , e neppure contemporaneamente dispari, altrimenti la somma dei loro quadrati modulo 4 sarebbe 2, pertanto  $x$  ed  $y$  sono uno pari e l'altro dispari.

riscrittura

dove essendo quadrati modulo 4 abbiamo che  $x^2, y^2, z^2 \in \{0, 1\}$ , ma  $x$  e  $y$  non possono essere contemporaneamente pari,

**Osservazione 2.132 —** Consideriamo l'ideale  $I = (x + iy, x - iy)$ , verifichiamo che  $I = (1)$ , o equivalentemente che  $x + iy$  e  $x - iy$  sono coprimi (abbiamo visto che in un ED l'ideale generato da due elementi è quello generato dal loro M.C.D.). Osserviamo che:

$$2x = (x + iy) + (x - iy) \in I$$

Analogamente, considerando la differenza si ha  $2y \in I$  e, considerando il prodotto,  $x^2 + y^2 \in I$ ; poiché  $x$  ed  $y$  hanno diversa parità,  $x^2 + y^2$  è dispari, mentre  $2x$  è pari, dunque si ha che:

$$1 \in (2x, 2y, x^2 + y^2) \subset \mathbb{Z} \subset \mathbb{Z}[i]$$

infatti, se non ci fosse 1,  $\exists p$  tale che  $p \mid 2x$ ,  $p \mid 2y$ , da cui  $p = 2$  (in quanto  $(x, y) = 1$ ), ma  $2 = p \mid x^2 + y^2$ , che però è dispari, dunque:

$$I = (1)$$

o equivalentemente  $x + iy$  e  $x - iy$  sono coprimi e quindi entrambi dei quadrati a meno di unità.

riscritture e aggiunte varie

[continua ...]

```

\begin{remark}
    Consideriamo l'ideale  $I = (x+iy, x-iy)$ , verifichiamo che  $I = (1)$ , o
    equivalentemente che  $x+iy$  e  $x-iy$  sono coprimi
    (abbiamo visto che in un ED l'ideale generato da due elementi è quello generato
    dal loro M.C.D.). Osserviamo che:
    \begin{align*}
        2x &= (x+iy) + (x-iy) \in I \\
        2yi &= (x+iy) - (x-iy) \in I \\
        a^2 + b^2 &= (x+iy)(x-iy) \in I
    \end{align*}
    Mostriamo che:
    \begin{bmatrix} 1 \in (2x, 2yi, x^2+y^2) \subset \underbrace{\{(x+iy, x-iy)\}}_I \subset \mathbb{Z}[i] \\
    \end{bmatrix}
    infatti, se non ci fosse 1,  $\exists p$  primo tale che  $(p) \supseteq (2x, 2yi, x^2+y^2)$ ,
    \footnote{Perché ogni ideale proprio (cioè che non contiene 1) è contenuto in
    un ideale massimale (proposizione 2.55), ma massimale implica primo (corollario
    2.57) e gli ideali primi sono generati da elementi primi (proposizione 2.86).}
    quindi  $p \mid 2x$  e  $p \mid 2yi \implies p \mid 2y$ ,
    \footnote{Come vedremo nella prossima osservazione,  $i$  è invertibile in
     $\mathbb{Z}[i]$ , quindi  $p$  non può dividere  $i$  altrimenti sarebbe anch'esso invertibile
    (infatti sarebbe associato a un elemento invertibile), che è assurdo per
    definizione di elemento primo. \\
    [In realtà si poteva considerare direttamente l'ideale  $(2x, 2y, x^2+y^2)$  in
    quanto  $2y = (2yi)i^3 \in I$  perché  $2yi \in I$ ]}
    da cui  $p \mid 2$  (in quanto  $(x,y) = 1$ ).
    In  $\mathbb{Z}[i]$  la fattorizzazione in irriducibili di  $2$  è  $2 = -i(1+i)^2$ , quindi
     $p = 1+i$  (a meno di associati);
    ma  $1+i \mid a+bi \implies N(a+bi) = a^2+b^2$  è pari [in realtà vale "se e solo
    se" ma non ho voglia di scrivere l'altra freccia]
    e  $x^2+y^2$  è dispari (perché  $x$  e  $y$  hanno diversa parità), assurdo.
    Dunque  $I = (1)$  o equivalentemente  $x+iy$  e  $x-iy$  sono coprimi.
    Ciò significa che  $x+iy$  e  $x-iy$  sono dei quadrati (a meno di unità):
    infatti se fattorizziamo  $z$  in irriducibili (ricordiamo che  $\mathbb{Z}[i]$  è UFD),
    un suo fattore primo non può appartenere sia a  $x+iy$  che  $x-iy$  (per
    coprimalità);
    dato che  $(x+iy)(x-iy) = z^2$ , nel membro destro questi fattori primi compaiono
    come potenze con esponente pari
    e ognuna di queste, per quanto detto, sta o in  $x+iy$  o in  $x-iy$ , che quindi
    sono quadrati.
\end{remark}

```

Consideriamo l'ideale  $I = (x + iy, x - iy)$ , verifichiamo che  $I = (1)$ , o equivalentemente che  $x + iy$  e  $x - iy$  sono coprimi (abbiamo visto che in un ED l'ideale generato da due elementi è quello generato dal loro M.C.D.). Osserviamo che:

$$\begin{aligned} 2x &= (x + iy) + (x - iy) \in I \\ 2yi &= (x + iy) - (x - iy) \in I \\ a^2 + b^2 &= (x + iy)(x - iy) \in I \end{aligned}$$

Mostriamo che:

$$1 \in (2x, 2yi, x^2 + y^2) \subset \underbrace{(x + iy, x - iy)}_I \subset [i]$$

infatti, se non ci fosse 1,  $\exists p$  primo tale che  $(p) \supseteq (2x, 2yi, x^2 + y^2)$ , <sup>1</sup> quindi  $p \mid 2x$  e  $p \mid 2yi \implies p \mid 2y$ , <sup>2</sup> da cui  $p \mid 2$  (in quanto  $(x, y) = 1$ ). In  $[i]$  la fattorizzazione in irriducibili di 2 è  $2 = -i(1+i)^2$ , quindi  $p = 1+i$  (a meno di associati); ma  $1+i \mid a+bi \implies N(a+bi) = a^2 + b^2$  è pari [in realtà vale "se e solo se" ma non ho voglia di scrivere l'altra freccia] e  $x^2 + y^2$  è dispari (perché  $x$  e  $y$  hanno diversa parità), assurdo. Dunque  $I = (1)$  o equivalentemente  $x + iy$  e  $x - iy$  sono coprimi. Ciò significa che  $x + iy$  e  $x - iy$  sono dei quadrati (a meno di unità): infatti se fattorizziamo  $z$  in irriducibili (ricordiamo che  $[i]$  è UFD), un suo fattore primo non può appartenere sia a  $x + iy$  che  $x - iy$  (per coprimalità); dato che  $(x+iy)(x-iy) = z^2$ , nel membro destro questi fattori primi compaiono come potenze con esponente pari e ognuna di queste, per quanto detto, sta o in  $x + iy$  o in  $x - iy$ , che quindi sono quadrati.

**Osservazione 2.133 (Invertibili di  $\mathbb{Z}[i]$ )** — Osserviamo che gli elementi di  $(\mathbb{Z}[i])^*$  sono gli  $u \in \mathbb{Z}[i]$  tali per cui  $\exists v \in \mathbb{Z}[i]$ :

$$uv = 1^{\text{a}} \implies v = \bar{u} \implies u\bar{u} = 1$$

ovvero  $u = \varepsilon + i\delta \in \mathbb{Z}[i]$  dove:

$$u\bar{u} = \varepsilon^2 + \delta^2 = 1$$

che ha per soluzioni:

$$\begin{cases} \varepsilon = \pm 1 \\ \delta = 0 \end{cases} \quad \text{e} \quad \begin{cases} \varepsilon = 0 \\ \delta = \pm 1 \end{cases}$$

dunque  $(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$ .

<sup>a</sup>Stiamo usando il fatto che nei complessi il prodotto fa 1 se è tra elementi coniugati.

Detto così è falso, infatti  $2 \cdot \frac{1}{2} = 1$  ma 2 e  $\frac{1}{2}$  non sono coniugati; potrebbe andare bene sapendo che  $N(u) = N(v) = 1$ , ma a questo punto si fa prima direttamente con le norme (come ha fatto Lombardo).

---

Allora, per quanto detto sappiamo che:

$$x + iy = u\alpha^2 \quad \alpha \in \mathbb{Z}[i], u \in \{\pm 1, \pm i\}$$

e analogamente:

$$x - iy = \bar{u}\bar{\alpha}^2 \quad \bar{\alpha} \in \mathbb{Z}[i], \bar{u} \in \{\pm 1, \pm i\}$$

Considerando  $\alpha = a + ib$  si ottiene:

$$x + iy = u(a^2 - b^2 - 2iab)$$

distinguiamo ora due casi:

- Se  $u = \pm 1$ , allora si ottiene:

$$\begin{cases} x = \pm(a^2 - b^2) \\ y = \mp 2ab \\ z = \pm(a^2 + b^2) \end{cases}$$

- Se  $u = \pm i$ , allora si ottiene:

$$\begin{cases} x = \mp 2ab \\ z = \pm(a^2 - b^2 - 2) \\ y = \pm(a^2 + b^2) \end{cases}$$

che forniscono la parametrizzazione delle terne pitagoriche e rispondono al problema iniziale di determinarle.

typo, riscritture e aggiunte varie

[continua ...]

Allora, per quanto detto sappiamo che:

```
\[ x + iy = u\alpha^2 \quad \text{where } \alpha \in \mathbb{Z}[i], \quad u \in \{\pm 1, \pm i\}
```

e analogamente:

```

    \[ x - iy = \overline{x + iy} = \overline{u}, \overline{\alpha^2} \quad \text{quad}
\overline{\alpha} \in \mathbb{Z}[i], \overline{u} \in \{\pm 1, \pm i\}
\]

```

Considerando  $\alpha = a+ib$  si ottiene:

```
\begin{align*}
```

$$\begin{aligned} x + iy &= u(a^2 - b^2 + 2abi) \\ x - iy &= \overline{u}(a^2 - b^2 - 2abi) \end{aligned}$$

```
\end{align*}
```

inoltre

```

    \[ z^2 = (x + iy)(x - iy) = (\overline{u})(\overline{\alpha}\overline{\alpha})^2 =
N(u)(N(\alpha))^2 = 1 \cdot (a^2 + b^2)^2
\]

```

Distinguiamo ora due casi:

```
\begin{itemize}
```

\item Se  $u = \pm 1$ , allora si ottiene:

```
\[ \begin{cases}
```

$x = \sqrt{pm(a^2 - b^2)}$

$$v = \sqrt{2ab}$$

```
\end{cases}
```

1

\item Se  $u \equiv pm$  i\$, allora si ottiene:

```
\[ \begin{cases}
```

$x \equiv \text{mp} 2ab \backslash \backslash$

$$v = \sqrt{a^2 - b^2}$$

```
\end{cases}
```

1

```
\end{itemize}
```

montno

\[ z = \sqrt{a^2 + b^2}

1

indipendentemente da  $\$u\$$  (il segno viene dall'estrazione di radice). //

Queste formule forniscono la parametrizzazione delle terne pitagoriche e rispondono al problema iniziale di determinarle.

Allora, per quanto detto sappiamo che:

$$x + iy = u\alpha^2 \quad \alpha \in [i], u \in \{\pm 1, \pm i\}$$

e analogamente:

$$x - iy = \overline{x + iy} = \bar{u}\bar{\alpha}^2 \quad \bar{\alpha} \in [i], \bar{u} \in \{\pm 1, \pm i\}$$

Considerando  $\alpha = a + ib$  si ottiene:

$$\begin{aligned} x + iy &= u(a^2 - b^2 + 2abi) \\ x - iy &= \bar{u}(a^2 - b^2 - 2abi) \end{aligned}$$

inoltre

$$z^2 = (x + iy)(x - iy) = (u\bar{u})(\alpha\bar{\alpha})^2 = N(u)(N(\alpha))^2 = 1 \cdot (a^2 + b^2)^2$$

Distinguiamo ora due casi:

- Se  $u = \pm 1$ , allora si ottiene:

$$\begin{cases} x = \pm(a^2 - b^2) \\ y = \mp 2ab \end{cases}$$

- Se  $u = \pm i$ , allora si ottiene:

$$\begin{cases} x = \mp 2ab \\ y = \pm(a^2 - b^2) \end{cases}$$

mentre

$$z = \pm(a^2 + b^2)$$

indipendentemente da  $u$  (il segno viene dall'estrazione di radice).

Queste formule forniscono la parametrizzazione delle terne pitagoriche e rispondono al problema iniziale di determinarle.

r. 4050; p. 101

**Definizione 3.2.** Dato un campo  $K$  ed una sua estensione  $L$ ,  $\alpha \in L$  si dice **trascendente** su  $K$  se non è algebrico, ovvero:

$$\nexists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$$

aggiustare il “non esiste” (vedi

<https://tex.stackexchange.com/questions/117070/how-to-write-a-pretty-not-varepsilon>)

---

r. 4088; p. 101

**Osservazione 3.5 —** Poiché  $K[x]$  è un PID, si ha che  $\ker \varphi_\alpha = (\mu_\alpha(x))$ , con  $\mu_\alpha(x) \in \ker \varphi_\alpha$ , ed essendo un ideale massimale  $\mu_\alpha(x)$  è irriducibile in  $K[x]$  (Proposizione 2.86). Inoltre, scegliamo  $\mu_\alpha(x)$  come l'unico generatore monico, infatti essendo  $K[x]$  anche un ED, per la Proposizione 2.93 sappiamo che i suoi ideali sono generati da elementi di grado minimo, e tali elementi differiscono per un elemento di  $K \setminus \{0\}$ .

correzione minore

Possiamo scegliere  $\mu_\alpha(x)$  come l'unico generatore monico, infatti essendo  $K[x]$  anche un ED, per la Proposizione 2.93 sappiamo che i suoi ideali sono generati da elementi di grado minimo, e tali elementi differiscono per un elemento di  $K \setminus \{0\}$ .

---

**Proposizione 3.8** (Proprietà delle torri di estensioni)

Data una torre di estensioni  $K \subset F \subset L$ ,  $F/K$  è finita se e solo se  $F/L$  e  $L/K$  sono finite e inoltre:

$$[F : K] = [F : L][L : K]$$

*Dimostrazione.* La dimostrazione è identica a quella già vista in [Aritmetica](#). Siano  $[F : K] = n$  e  $[L : F] = m$ , verifichiamo che  $[L : K] = nm$ ; per definizione sappiamo che  $[F : K] = n$  ovvero  $F$  è un  $K$ -spazio vettoriale con  $\dim_K F = n$ , e ugualmente,  $[L : F] = m$  ovvero  $L$  è un  $F$ -spazio vettoriale con  $\dim_F L = m$ , possiamo considerare allora una  $K$ -base di  $F$ ,  $\{v_1, \dots, v_n\}$ , ed una  $F$ -base di  $L$ ,  $\{w_1, \dots, w_m\}$ , per dimostrare la tesi, dobbiamo dimostrare che  $\dim_K L = nm$ , ovvero  $L$  ammette una  $K$ -base di cardinalità  $nm$ . Consideriamo l'insieme  $\{v_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$ , come si osserva facilmente, esso ha cardinalità  $nm$ , dimostriamo quindi che tale insieme è una  $K$ -base di  $L$ , per fare ciò verifichiamo separatamente che gli elementi di  $\{v_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$  generano tutti gli elementi di  $L$  e che sono tra loro linearmente indipendenti:

**typo, punteggiatura**

Data una torre di estensioni  $K \subset F \subset L$ , allora  $\text{\faktor}{L}{K}$  è finita se e solo se  $\text{\faktor}{L}{F}$  e  $\text{\faktor}{F}{K}$  sono finite e inoltre:

$$\begin{aligned} & [L : K] = [L : F][F : K] \\ & \end{aligned}$$

e ugualmente,  $[L : F] = m$  ovvero  $L$  è un  $F$ -spazio vettoriale con  $\dim_F L = m$ .

Possiamo considerare allora una  $K$ -base di  $F$ ,  $\{v_1, \dots, v_n\}$ , ed una  $F$ -base di  $L$ ,  $\{w_1, \dots, w_m\}$ ;

rr 4147, 4167; p. 103

- Sia  $\alpha \in L$ , poiché  $L$  è per ipotesi un  $F$ -spazio vettoriale, quindi  $L = \langle w_1, \dots, w_m \rangle_F$ , si ha che:

$$\alpha = \sum_{j=1}^m \lambda_j w_j \quad \lambda_j \in F$$

d'altra parte, poiché  $F$  è un  $K$ -spazio vettoriale, quindi  $F = \langle w_1, \dots, w_m \rangle_K$ , si ha che:

$$\lambda_j = \sum_{i=1}^n a_{j_i} v_i \quad a_{j_i} \in K$$

essendo  $\{v_1, \dots, v_n\}$  una  $K$ -base di  $F$ , le singole somme  $\sum_{i=1}^n a_{j_i} v_i$  sono nulle se e solo se  $a_{j_i} = 0$ ,  $\forall i \in \{1, \dots, n\}$ , quindi la somma iniziale è nulla se e solo se  $a_{j_i} = 0$ ,  $\forall i \in \{1, \dots, n\}$ ,  $\forall j \in \{1, \dots, m\}$ , quindi gli elementi di  $\{v_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$  sono linearmente indipendenti.  $\square$

typo, aggiunta

d'altra parte, poiché  $F$  è un  $K$ -spazio vettoriale, quindi  $F = \langle v_1, \dots, v_n \rangle_K$ , si ha che:

ossia  $\forall i \in \{1, \dots, n\}$ ,  $\forall j \in \{1, \dots, m\}$ , quindi gli elementi di  $\{v_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$  sono linearmente indipendenti.

**Proposizione 3.12** (Campo delle estensioni algebriche)

Data un'estensione  $L/K$ , sia  $A = \{\alpha \in L \mid \alpha \text{ è algebrico su } K\}$ , allora  $A$  è un campo (ed ovviamente è un'estensione algebrica di  $K$ ).

*Dimostrazione.* Verifichiamo che  $A$  sia un campo; siano  $\alpha, \beta \in A$ , allora  $[K(\alpha) : K] < +\infty$  e  $[K(\beta) : K] < +\infty$ , consideriamo la torre:

$$K \subseteq K(\alpha) \subseteq K(\alpha)(\beta) = K(\alpha, \beta)$$

la prima estensione è finita per ipotesi, mentre la seconda è finita per la [Proposizione 3.9](#) in quanto estensione composta da  $K(\alpha)$  e  $K(\beta)$  (entrambe semplici e quindi finite perché algebriche, per la [Proposizione 3.7](#)). Essendo dunque  $K \subseteq K(\alpha, \beta)$  un'estensione finita, per la [Proposizione 3.11](#) è algebrica, quindi tutti gli elementi  $\alpha \pm \beta$ ,  $\alpha\beta$  e  $\frac{1}{\beta}$  sono algebrici su  $K$ , pertanto  $A$  è un campo.  $\square$

punteggiatura, riscritture, aggiunte

[Si chiama “campo delle estensioni algebriche”? forse “campo degli elementi algebrici”]

(perché algebriche e semplici quindi finite per la [Proposizione 3.7](#)). Consideriamo la torre:

la seconda estensione è finita per la [Proposizione 3.9](#), in quanto estensione composta da  $K(\alpha)$  e  $K(\beta)$  entrambe finite.

Essendo dunque anche  $K(\alpha, \beta)$  un'estensione finita (per [Torri](#)), per la [Proposizione 3.11](#) è algebrica, quindi gli elementi  $\alpha \pm \beta$ ,  $\alpha\beta$  e  $\frac{1}{\beta}$  sono algebrici su  $K$  in quanto elementi di  $K(\alpha, \beta)$ .

\footnote{Stiamo usando il fatto che  $K(\alpha, \beta)$  è un campo.}, pertanto  $A$  è un campo.

**Osservazione 3.15** — Ricordiamo che avevamo definito un'estensione **finitamente generata** una scrittura del tipo  $L = K(\alpha_1, \dots, \alpha_n)$  che può essere definita equivalentemente come:

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1) \dots (\alpha_n) = \{p(\alpha_1, \dots, \alpha_n) \mid p(x_1, \dots, x_n) \in K[x_1, \dots, x_n]\}$$

usare `\mid`

```
\[ K(\alpha_1, \dots, \alpha_n) = K(\alpha_1) \dots (\alpha_n) =  
 \{ p(\alpha_1, \dots, \alpha_n) \mid p(x_1, \dots, x_n) \in K[x_1, \dots, x_n] \}  
\]
```

---

- (1) La prima implicazione segue quasi immediatamente, infatti, se  $F/K$  è algebrica, allora  $\forall \alpha \in F$ ,  $\alpha$  è algebrico su  $K$ , dunque tutti gli  $\alpha \in L \subset F$  sono algebrici su  $K$  perché elementi anche di  $F$ , pertanto  $L$  è algebrico su  $K$ , inoltre,  $F$  è algebrico su  $L$  perché contiene  $K$ , dunque tutti gli elementi di  $F$  sono già algebrici su  $K$  e quindi lo saranno anche in un campo più grande.  
Viceversa sia  $\alpha \in F$ , per ipotesi sappiamo che  $F/L$  e  $L/K$  sono algebriche, quindi  $\alpha$  è algebrico su  $L$ , dunque:

$$\exists f(x) \in L[x] \setminus \{0\} : f(\alpha) = 0 \quad \text{con} \quad f(x) = \sum_{i=0}^n a_i x^i$$

dove la prima estensione è finitamente generata ed algebrica (perché  $\forall a_i \in L$ ,  $a_i$  è algebrico su  $K$ ), pertanto è finita per la [Proposizione 3.16](#), inoltre la seconda estensione è a sua volta finita perché algebrica ([quindi vale la Proposizione 3.11](#)), di conseguenza, per il [Teorema delle torri](#), la torre di estensione è finita,  $[L_0(\alpha) : K] < +\infty$ , dunque, sempre per la [Proposizione 3.11](#)  $L_0(\alpha)/K$  è algebrica. Abbiamo quindi dimostrato che  $\alpha \in F$  è algebrico su  $K$ ,  $\forall \alpha \in F$ , dunque  $F/K$  è algebrica.

- (2) Sia  $LM/K$  algebrica e sia  $\alpha \in M \subset LM$ , allora è algebrico su  $K$ , in quanto tutti gli elementi di  $LM$  già lo erano, dunque non stiamo facendo altro che prendere una sottoestensione di un'estensione algebrica, che quindi sarà a sua volta algebrica, ovvero  $M/K$  algebrica; in maniera identica  $L/K$  è anch'essa algebrica.  
Supponiamo ora che  $L/K$  e  $M/K$  siano algebriche, consideriamo  $\alpha \in LM = L(M)$ , ovvero  $\alpha = \sum_{i=1}^n \lambda_i m_i$ , con  $\lambda_i \in L$  e  $m_i \in M$ , dunque:

punteggiatura, tipo, aggiunte

dunque tutti gli  $\alpha \in L \subset F$  sono algebrici su  $K$  perché elementi anche di  $F$ , pertanto  $L$  è algebrico su  $K$ ;  
inoltre,  $F$  è algebrico su  $L$  perché contiene  $K$ , dunque tutti gli elementi di  $F$  sono già algebrici su  $K$  e quindi lo saranno anche in un campo più grande.\

```
\[ \exists f(x) \in L[x] \setminus \{0\} : f(\alpha) = 0 \quad \text{con} \quad f(x) = \sum_{i=0}^n a_i x^i
```

dove la prima estensione è finitamente generata ed algebrica (perché  $\forall a_i \in L$ ,  $a_i$  è algebrico su  $K$ ), pertanto è finita per la [Proposizione 3.16](#),

inoltre la seconda estensione è a sua volta finita perché algebrica e semplice ([Proposizione 3.7](#)).

Di conseguenza, per il [Teorema delle torri](#), la torre di estensione  $L_0(\alpha) : K$  è finita,

dunque, per la [Proposizione 3.11](#)  $\text{faktor}\{L_0(\alpha)\}{K}$  è algebrica, e in particolare  $\alpha$  è algebrico su  $K$ .

Abbiamo quindi dimostrato che  $\alpha \in F$  è algebrico su  $K$ ,  $\forall \alpha \in F$ ,

dunque  $\text{faktor}\{F\}{K}$  è algebrica.

sarà a sua volta algebrica, \footnote{Volendo per il punto (1).} ovvero  $\text{faktor}\{M\}{K}$  algebrica; in maniera identica  $\text{faktor}\{L\}{K}$  è anch'essa algebrica.\

**Teorema 3.25** (Esistenza e unicità della chiusura algebrica)

Sia  $K$  un campo, allora esiste sempre una sua chiusura algebrica. Inoltre due qualsiasi chiusure algebriche su  $K$  sono isomorfe.<sup>a</sup>

<sup>a</sup>Nel senso che gli isomorfismi tra le varie chiusure algebriche fissano  $K$ .

**Esempio 3.26**

Consideriamo  $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$ , tale insieme è un campo, per quanto asserito nella [Proposizione 3.12](#), ed è per [una chiusura algebrica di  \$\mathbb{Q}\$](#) , infatti  $\overline{\mathbb{Q}}/\mathbb{Q}$  è un'estensione algebrica per definizione. Verifichiamo che  $\overline{\mathbb{Q}}$  è algebricamente chiuso; sia  $f(x) \in \overline{\mathbb{Q}}[x]$  non costante, allora  $f(x)$  ammette almeno una radice  $\alpha \in \mathbb{C}$ , poiché  $f(x) \in \overline{\mathbb{Q}}[x] \subset \mathbb{C}[x]$  e  $\mathbb{C}$  è algebricamente chiuso. Per mostrare che  $\alpha \in \overline{\mathbb{Q}}$ , bisogna dimostrare che  $\alpha$  è algebrico su  $\mathbb{Q}$ , consideriamo la torre:

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}(\alpha)$$

la prima estensione è algebrica per quanto già discusso, la seconda è algebrica perché semplice ([Proposizione 3.7](#)), dunque per [torri](#)  $\alpha$  è algebrico su  $\mathbb{Q}$ , inoltre  $\alpha \in \mathbb{C}$ , per cui  $\alpha \in \overline{\mathbb{Q}}$  che quindi è algebricamente chiuso, perché quanto detto vale per qualunque polinomio in  $\overline{\mathbb{Q}}[x]$ .

aggiunte, usare \mid, riscrittura, punteggiatura, correzioni varie

il link per “torri” è sbagliato (non ci interessa il grado, ma l’essere algebrico)

[continua ...]

Sia  $K$  un campo, allora esiste sempre una sua chiusura algebrica. Inoltre due qualsiasi chiusure algebriche su  $K$  sono isomorfe su  $K$ .

\footnote{Nel senso che gli isomorfismi tra le varie chiusure algebriche fissano  $K$ .}

Consideriamo  $\overline{Q} = \{\alpha \in C \mid \text{$\alpha$ è algebrico su $\overline{Q}$}\}$ , tale insieme è un campo, per quanto asserito nella

\hyperref[3.12]{Proposizione 3.12}, e inoltre è una chiusura algebrica di  $\overline{Q}$ .

Infatti  $\faktor{\overline{Q}}{\overline{Q}}$  è un'estensione algebrica per definizione.

Verifichiamo che  $\overline{Q}$  è algebricamente chiuso; sia  $f(x) \in \overline{Q}[x]$  non costante,

allora  $f(x)$  ammette almeno una radice  $\alpha \in C$ , poiché  $f(x) \in \overline{Q}[x] \subset C[x]$  e  $C$  è algebricamente chiuso.

Per mostrare che  $\alpha \in \overline{Q}$ , bisogna

la prima estensione è algebrica per quanto già discusso,

la seconda è algebrica perché  $\alpha$  è algebrico su  $\overline{Q}$  (è radice di  $f(x) \in \overline{Q}[x]$ ),

dunque per torri (osservazione 3.18)  $\alpha$  è algebrico su  $\overline{Q}$ , ossia  $\alpha \in \overline{Q}$ .

Quindi  $\overline{Q}$  è algebricamente chiuso perché quanto detto vale per qualunque polinomio in  $\overline{Q}[x]$ .

---

con  $\Omega$  algebricamente chiuso, definendo  $\overline{K} = \{\alpha \in \Omega \mid \alpha \text{ è algebrico su } K\}$ , da cui  $\overline{K}$  chiusura algebrica di  $K$  (infatti  $\overline{K}$  è un'estensione algebrica di  $K$  per definizione, ed iterando il ragionamento precedente si mostra come sia anche algebricamente chiuso).

**Definizione 3.28.** Sia  $f(x) \in K[x]$ , con  $\deg f(x) \geq 1$ , e siano  $\alpha_1, \dots, \alpha_n \in \overline{K}$  le radici di  $f(x)$ , si definisce **campo di spezzamento** di  $f(x)$  su  $K$  il sottocampo di  $\overline{K}$ :

$$K(\alpha_1, \dots, \alpha_n)$$

**Osservazione 3.29 —** La definizione di campo di spezzamento può essere estesa ad una famiglia di polinomi  $\mathcal{F} = \{f_i(x) \mid i \in I\} \subset K[x]$ , infatti, dato l'insieme delle radici di un polinomio  $f_i(x)$  della famiglia,  $\{\alpha_{ij}\}_{j=1, \dots, n_i}^{i \in I}$ , il campo di spezzamento di  $\mathcal{F}$  su  $K$  è dato da:

$$K(\{\alpha_{ij}\}_{j=1, \dots, n_i} \mid i \in I)$$

usare `\mid`, `typo`, aggiunta

con  $\Omega$  algebricamente chiuso, definendo  $\overline{K} = \{\alpha \in \Omega \mid \alpha \text{ è algebrico su } K\}$ , da cui  $\overline{K}$  chiusura algebrica di  $K$  (infatti  $\overline{K}$  è un'estensione algebrica

Sia  $f(x) \in K[x]$ , con  $\deg f(x) \geq 1$ , e, detta  $\overline{K}$  una chiusura algebrica di  $K$ , siano  $\alpha_1, \dots, \alpha_n \in \overline{K}$  le radici di  $f(x)$ , si definisce **campo di spezzamento** di  $f(x)$  su  $K$  il sottocampo di  $\overline{K}$ :

La definizione di campo di spezzamento può essere estesa ad una famiglia di polinomi  $\mathcal{F} = \{f_i(x) \mid i \in I\} \subset K[x]$ , infatti, dato l'insieme delle radici di un polinomio  $f_i(x)$  della famiglia,

$$\bigcup_{i \in I} K(\{\alpha_{ij}\}_{j=1, \dots, n_i} \mid i \in I)$$

rr. 4423-4426; p. 109

Ci poniamo ora il seguente problema: dato un campo  $K$ , la sua chiusura algebrica  $\overline{K}$  e  $\alpha \in \overline{K}$  (algebrico su  $K$ ), vogliamo sapere in quanti modi si può immerge  $K(\alpha)$  in  $\overline{K}$  con:

$$\varphi : K(\alpha) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K$$

aggiunta

forse è il caso di fare un nuovo capitolo qui (tipo “estensioni di omomorfismi”)

Ci poniamo ora il seguente problema: dato un campo  $K$ , la sua chiusura algebrica  $\overline{K}$  e  $\alpha \in \overline{K}$  (algebrico su  $K$ ), vogliamo sapere in quanti modi si può immerge  $K(\alpha)$  in  $\overline{K}$  fissando  $K$ :

---

**Proposizione 3.33** (Numero di estensioni via identità di  $K(\alpha)$  a  $\overline{K}$ )

Dato un campo  $K$  ed  $\alpha \in \overline{K}$ , con  $\overline{K}$  chiusura algebrica di  $K$ , detto  $k$  il numero di radici distinte di  $\mu_\alpha(x)$  in  $\overline{K}$ , allora:

$$\exists \varphi_1, \dots, \varphi_k : K(\alpha) \longrightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = id_K$$

ovvero esistono esattamente  $k$  estensioni distinte da  $K(\alpha)$  a  $\overline{K}$ .

*Dimostrazione.* Per quanto detto sull'omomorfismo di valutazione sappiamo che  $K(\alpha) \cong \frac{K[x]}{(\mu_\alpha(x))}$ , dunque, determinando un omomorfismo da  $K[x]$  ad  $\overline{K}$  possiamo applicare il **Primo Teorema di Omomorfismo**. Sia dunque:

$$\tilde{\varphi} : K[x] \longrightarrow \overline{K} : x \longmapsto \beta, p(x) \longmapsto p(\beta) \quad \forall \beta \in \overline{K}$$

per tale omomorfismo abbiamo che  $(\mu_\alpha(x)) \subset \ker \tilde{\varphi} \iff \mu_\alpha(x) \in \ker \tilde{\varphi}$  (per le proprietà degli ideali), quindi se e solo se  $\mu_\alpha(\beta) = 0$ , quindi per tutte le radici di  $\mu_\alpha(x)$  in  $\overline{K}$  si ha che:

correzioni minori, aggiunta

```
\begin{proposition}[Numero di estensioni di $K(\alpha)$ a $\overline{K}$ via identità]
```

```
\[ \exists \varphi_1, \dots, \varphi_k : K(\alpha) \varlonghookrightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = id_K
```

Per quanto detto sull'omomorfismo di valutazione sappiamo che  $K(\alpha) \cong \frac{K[x]}{(\mu_\alpha(x))}$ , dunque, determinato un omomorfismo da  $K[x]$  ad  $\overline{K}$  possiamo applicare il **Primo Teorema di Omomorfismo**. Sia dunque:

```
\[ \tilde{\varphi} : K[x] \longrightarrow \overline{K} : x \longmapsto \beta, p(x) \longmapsto p(\beta) \quad \beta \in \overline{K}
```

Si verifica che  $\tilde{\varphi}|_K = id$  (infatti valutare una costante restituisce sé stessa). \\

Per l'omomorfismo  $\tilde{\varphi}$  abbiamo che  $(\mu_\alpha(x)) \subset \ker \tilde{\varphi} \iff \mu_\alpha(x) \in \ker \tilde{\varphi}$  (per le proprietà degli ideali), quindi se e solo se  $\mu_\alpha(\beta) = 0$ .

Dunque per tutte le radici di  $\mu_\alpha(x)$  in  $\overline{K}$  si ha che:

Dalla proposizione appena dimostrata ci poniamo un secondo problema, quello di contare il numero di radici di  $\mu_\alpha(x)$  in  $\overline{K}$ , essendo  $\overline{K}$  algebricamente chiuso, allora il numero delle radici del polinomio, ciascuna contata con la propria molteplicità, è dato da  $\deg \mu_\alpha(x) = n$ , a questo punto, per determinare se  $\mu_\alpha(x)$  abbia o meno radici multiple possiamo fare uso del criterio che segue.

## aggiunta, punteggiatura

Osservazione importante:

Le  $\varphi_i$  che abbiamo trovato mandano  $\alpha$  in una radice di  $\mu_\alpha(x)$ .

Ragionando in modo analogo per le altri radici e sfruttando l'iniettività di  $\varphi_i$  possiamo concludere che le  $\varphi_i$  agiscono sull'insieme delle radici di  $\mu_\alpha(x)$  permutandole. \\

Dalla proposizione appena dimostrata ci poniamo un secondo problema: quello di contare il numero di radici di  $\mu_\alpha(x)$  in  $\overline{K}$ .

Essendo  $\overline{K}$  algebricamente chiuso, il numero delle radici del polinomio, ciascuna contata con la propria molteplicità, è dato da  $\deg \mu_\alpha(x) = n$ ; a questo punto, per determinare se  $\mu_\alpha(x)$  abbia o meno radici multiple possiamo fare uso del criterio che segue.

---

**Teorema 3.34** (Criterio della Derivata)

Sia  $f(x) \in K[x]$ , allora  $f(x)$  ha radici multiple in  $\overline{K}$  se e solo se  $(f(x), f'(x)) \neq 1$ . Inoltre se  $f(x)$  è irriducibile in  $K[x]$ , allora  $f(x)$  ha radici multiple se e solo se  $f'(x) = 0$ .

*Dimostrazione.* Il primo fatto è stato trattato in [Aritmetica](#), quindi non ne forniremo qui una dimostrazione. Per il secondo fatto si può osservare che  $f(x) \in K[x] \implies f'(x) \in K[x]$ , da cui  $(f(x), f'(x)) \in K[x]$  (perché si ottiene mediante l'Algoritmo di Euclide), e se  $f(x)$  è irriducibile in  $K[x]$  l'M.C.D. fa 1 oppure  $f(x)$ ; dove il secondo caso si realizza se e solo se  $f'(x) = 0$  (dato che  $\deg f'(x) < \deg f(x)$ ).  $\square$

Dunque se in  $K[x]$  i polinomi irriducibili non hanno derivata nulla, allora il numero delle loro radici distinte coincide con il loro grado.

**Definizione 3.35.** Un campo  $K$  tale per cui tutti i polinomi irriducibili in  $K[x]$  hanno derivata non nulla prende il nome di **campo perfetto**.

Sia  $f(x) \in K[x]$ , allora  $f(x)$  ha radici multiple in  $\overline{K}$  se e solo se  $(f(x), f'(\prime)(x)) \neq 1$ .

Inoltre se  $f(x)$  è irriducibile in  $K[x]$ , allora  $f(x)$  ha radici multiple se e solo se  $f'(\prime)(x) = 0$ .

da cui  $(f(x), f'(\prime)(x)) \in K[x]$  (perché si ottiene mediante l'Algoritmo di Euclide), e se  $f(x)$  è irriducibile in  $K[x]$ , l'M.C.D. fa 1 oppure  $f(x)$ ; il secondo caso si realizza se e solo se  $f'(\prime)(x) = 0$  (dato che  $\deg f'(\prime)(x) < \deg f(x)$ ).

Dunque se in  $K[x]$  i polinomi irriducibili non hanno derivata nulla, allora il numero delle loro radici distinte in  $\overline{K}$  coincide con il loro grado.

Un campo  $K$  tale che tutti i polinomi irriducibili in  $K[x]$  hanno derivata non nulla prende il nome di **campo perfetto**.

- Al contrario possiamo vedere che per campi con caratteristica diversa da 0 esistono polinomi irriducibili con derivata nulla, sia  $K = \mathbb{F}_p(t)$  e  $f(x) = x^p - t \in K[x]$ , abbiamo che  $f'(x) = px^{p-1} = 0$ , possiamo verificare che  $f(x)$  è irriducibile in  $K[x]$ . Osserviamo che:

$$f(x) \in \mathbb{F}_p[t][x] := A[x]$$

dove  $A$  UFD (essendo un ED), dunque per il [Lemma di Gauss](#) verificare che  $f(x)$  è irriducibile in  $K[x] = \mathbb{F}_p(t)[x]$  è equivalente a verificare che sia irriducibile in  $A[x] = \mathbb{F}_p[t][x]$ . In  $A[x]$ , essendo UFD, vale il [Criterio di Eisenstein](#), dunque  $f(x)$  è irriducibile rispetto all'ideale  $P = (t)$ , che è primo in quanto massimale, infatti  $\frac{A}{(t)} \cong \mathbb{F}_p$ . Inoltre se  $\alpha \in \overline{K}$  è una radice di  $f(x)$ , abbiamo che  $f(\alpha) = \alpha^p - t = \alpha^p - \alpha^p = 0$ , da cui:

$$f(x) = x^p - \alpha^p = (x - \alpha)^p$$

dove nell'ultima uguaglianza abbiamo usato il lemma del Binomio Ingenuo, pertanto in realtà  $f(x)$  ha un'unica radice in  $\overline{K}$ .

## punteggiatura, aggiunte, riscrittura

\item Al contrario possiamo vedere che per campi con caratteristica diversa da 0 esistono polinomi irriducibili con derivata nulla:

sia  $K = \mathbb{F}_p(t)$  e  $f(x) = x^p - t \in K[x]$ , abbiamo che  $f'(x) = px^{p-1} = 0$ ,

In  $A[x]$ , essendo UFD (perché  $A$  lo è) vale il [\hyperref\[eisenstein\]{Criterio di Eisenstein}](#):

$t$  è un elemento primo, perché l'ideale  $(t)$  è massimale ( $\frac{A}{(t)} \cong \mathbb{F}_p$  campo) e quindi primo; possiamo concludere che  $f(x)$  è irriducibile.

\item La chiusura algebrica di un campo perfetto è un campo perfetto: infatti i polinomi irriducibili a coefficienti in una chiusura algebrica sono solo quelli di primo grado, quindi la loro derivata non si annulla mai.

rr. 4520, 4526; p. 111-112

**Proposizione 3.37** (Numero di estensioni di  $K(\alpha)$  a  $\overline{K}$ )

Dato  $\alpha \in \overline{K}$ , con  $[K(\alpha) : K] = n$ , si ha che  $\forall \varphi : K \hookrightarrow \overline{K}$  immersione, esistono esattamente  $n$  estensioni a  $K(\alpha)$ , cioè:

$$\exists \varphi_1, \dots, \varphi_n : K(\alpha) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi$$

**Osservazione 3.38** — Abbiamo già visto che ciò è vero se  $\varphi = id_K$ , nella [Proposizione 3.33](#), la nuova proposizione ci permette di contare il numero di estensioni di un omomorfismo da  $K$  in  $\overline{K}$  ad uno da  $K(\alpha)$  in  $\overline{K}$ . Ad esempio, dato  $K = \mathbb{Q}(\sqrt[3]{2})$  e l'omomorfismo:

$$\varphi : K \hookrightarrow \overline{K} : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$$

ci chiediamo quanti sono gli omomorfismi:

$$\varphi_i : K(\zeta_3) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi$$

cioè che quando ristretti a  $K$  si comportano come  $\varphi$ .

spazi, aggiunta

```
\[ \exists \varphi_1, \dots, \varphi_n : K(\alpha) \rightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi
```

la nuova proposizione ci permette di contare il numero di estensioni di un omomorfismo qualsiasi da  $K$  in  $\overline{K}$  ad uno da  $K(\alpha)$  in  $\overline{K}$ .

```
\[ \exists \varphi_i : K(\zeta_3) \rightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi
```

*Dimostrazione.* In analogia con quanto fatto nella dimostrazione della [Proposizione 3.33](#), consideriamo:

$$\tilde{\varphi} : K[x] \longrightarrow \overline{K} : x \longmapsto \beta : p(x) \longmapsto p(\beta) \quad \text{con} \quad \varphi_{i|K} = \varphi$$

per tale omomorfismo abbiamo che  $(\mu_\alpha(x)) \subseteq \ker \tilde{\varphi} \iff \tilde{\varphi}(\mu_\alpha(x)) = 0 \iff \varphi(\mu_\alpha(x))(\beta) = 0$ , dunque applichiamo  $\varphi$  ai coefficienti di  $\mu_\alpha(x)$  (prima venivano lasciati fissi perché usavamo l'identità) e poi valutiamo il nuovo polinomio in  $\beta$ , pertanto  $\beta$  deve essere una radice di  $\varphi(\mu_\alpha(x))$ , dunque le estensioni di  $\varphi$  a  $K(\alpha)$  sono tante quante le radici distinte di  $\varphi(\mu_\alpha(x))$  in  $\overline{K}$ .

Poiché  $\mu_\alpha(x)$  è irriducibile per definizione, allora  $\varphi(\mu_\alpha(x))$  è irriducibile, inoltre,  $\deg \mu_\alpha(x) = \deg \varphi(\mu_\alpha(x))$  (poiché l'omomorfismo è iniettivo), pertanto, essendo il campo perfetto il numero di radici distinte di  $\varphi(\mu_\alpha(x))$  è uguale al suo grado, e quindi a quello di  $\mu_\alpha(x)$ .  $\square$

typo, riscritture e aggiunte varie

[continua ...]

```

\begin{proof}
    Per prima cosa estendiamo  $\varphi$  a un omomorfismo sui polinomi:
    
$$\begin{aligned} \varphi : K[x] &\xrightarrow{\quad} \overline{K}[x] : p(x) \xrightarrow{\quad} \\ \varphi(p(x)) &= (\varphi \circ p)(x) \end{aligned}$$

    dove, se  $p(x) = \sum a_i x^i$ ,
    
$$\begin{aligned} (\varphi \circ p)(x) &= \sum \varphi(a_i) x^i \end{aligned}$$

    In analogia con quanto fatto nella dimostrazione della
    \hyperref[3.33]{Proposizione 3.33}, consideriamo:
    
$$\begin{aligned} \widetilde{\varphi} : K[x] &\xrightarrow{\quad} \overline{K} : p(x) \xrightarrow{\quad} \\ (\varphi \circ p)(\beta) & \end{aligned}$$

    cioè applichiamo  $\varphi$  ai coefficienti di  $\mu_\alpha(x)$  (prima venivano lasciati fissi perché usavamo l'identità) e poi valutiamo il nuovo polinomio in  $\beta$ . Si verifica che  $\widetilde{\varphi}|_{\overline{K}} = id$ .
    Per l'omomorfismo  $\widetilde{\varphi}$  abbiamo che  $(\mu_\alpha(x)) \subsetneq \ker \widetilde{\varphi} \iff \widetilde{\varphi}(\mu_\alpha(x)) = 0 \iff (\varphi \circ \mu_\alpha)(\beta) = 0$ , cioè  $\beta$  deve essere una radice di  $(\varphi \circ \mu_\alpha)(x)$ .
    Dunque le estensioni di  $\varphi$  a  $K(\alpha)$  sono tante quante le radici distinte di  $(\varphi \circ \mu_\alpha)(x)$  in  $\overline{K}$ .
    Poiché  $\mu_\alpha(x)$  è irriducibile in  $K[x]$  (per definizione), allora  $(\varphi \circ \mu_\alpha)(x)$  è irriducibile in  $\varphi(K)[x]$ .
    \footnote{Mostriamo la contronominale. Sia  $(\varphi \circ f)(x)$  riducibile in  $\varphi(K)[x]$ , allora si spezza in due polinomi non costanti  $(\varphi \circ f)(x) = g(x)h(x)$  con  $g(x), h(x) \in \varphi(K)[x]$ . Ma allora si può scrivere  $f(x) = (\varphi^{-1} \circ g)(x) \cdot (\varphi^{-1} \circ h)(x)$  con  $(\varphi^{-1} \circ g)(x), (\varphi^{-1} \circ h)(x) \in K[x]$  (notare che per iniettività di  $\varphi$  è tutto ben definito), quindi anche  $f(x)$  è riducibile.}
    ed essendo  $\varphi(K)$  perfetto, il numero di radici distinte di  $(\varphi \circ \mu_\alpha)(x)$  coincide con  $\deg(\varphi \circ \mu_\alpha) = \deg \mu_\alpha = n$ .
    \footnote{$\varphi$ è iniettiva, ossia  $\ker \varphi = \{0\}$ , quindi non può mandare il coefficiente direttore in 0.}
\end{proof}

```

Per prima cosa estendiamo  $\varphi$  a un omomorfismo sui polinomi:

$$\varphi : K[x] \longrightarrow \overline{K}[x] : p(x) \longmapsto \varphi(p(x)) = (\varphi \circ p)(x)$$

dove, se  $p(x) = \sum a_i x^i$ ,

$$(\varphi \circ p)(x) = \sum \varphi(a_i)x^i$$

In analogia con quanto fatto nella dimostrazione della Proposizione 3.33, consideriamo:

$$\tilde{\varphi} : K[x] \longrightarrow \overline{K} : p(x) \longmapsto (\varphi \circ p)(\beta)$$

cioè applichiamo  $\varphi$  ai coefficienti di  $\mu_\alpha(x)$  (prima venivano lasciati fissi perché usavamo l'identità) e poi valutiamo il nuovo polinomio in  $\beta$ . Si verifica che  $\tilde{\varphi}|_K = id$ .

Per l'omomorfismo  $\tilde{\varphi}$  abbiamo che  $(\mu_\alpha(x)) \subseteq \ker \tilde{\varphi} \iff \tilde{\varphi}(\mu_\alpha(x)) = 0 \iff (\varphi \circ \mu_\alpha)(\beta) = 0$ , cioè  $\beta$  deve essere una radice di  $(\varphi \circ \mu_\alpha)(x)$ . Dunque le estensioni di  $\varphi$  a  $K(\alpha)$  sono tante quante le radici distinte di  $(\varphi \circ \mu_\alpha)(x)$  in  $\overline{K}$ .

Poiché  $\mu_\alpha(x)$  è irriducibile in  $K[x]$  (per definizione), allora  $(\varphi \circ \mu_\alpha)(x)$  è irriducibile in  $\varphi(K)[x]$ <sup>1</sup> ed essendo  $\varphi(K) \cong K$  perfetto, il numero di radici distinte di  $(\varphi \circ \mu_\alpha)(x)$  coincide con  $\deg(\varphi \circ \mu_\alpha)(x) = \deg \mu_\alpha(x) = n$ .<sup>2</sup>

---

<sup>1</sup> Mostriamo la contronominale. Sia  $(\varphi \circ f)(x)$  riducibile in  $\varphi(K)[x]$ , allora si spezza in due polinomi non costanti  $(\varphi \circ f)(x) = g(x)h(x)$  con  $g(x), h(x) \in \varphi(K)[x]$ . Ma allora si può scrivere  $f(x) = (\varphi^{-1} \circ g)(x) \cdot (\varphi^{-1} \circ h)(x)$  con  $(\varphi^{-1} \circ g)(x), (\varphi^{-1} \circ h)(x) \in K[x]$  (notare che per iniettività di  $\varphi$  è tutto ben definito), quindi anche  $f(x)$  è riducibile.

<sup>2</sup>  $\varphi$  è iniettiva, ossia  $\text{Ker } \varphi = \{0\}$ , quindi non può mandare il coefficiente direttore in 0.

**Corollario 3.39** (Numero di estensioni a  $\overline{K}$  di un'estensione qualsiasi)

Sia  $E/K$  un'estensione, con  $[E : K] = n$ , allora  $\forall \varphi : K \hookrightarrow \overline{K}$  immersione, esistono  $n$  immersioni:

$$\varphi_1, \dots, \varphi_n : E \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi$$

*Dimostrazione.* La dimostrazione segue facilmente per induzione, infatti per  $n = 1$  abbiamo che l'estensione è semplice e quindi vale la [Proposizione 3.37](#); per  $n > 1$  consideriamo  $\alpha \in E \setminus K$  per il quale si ha la torre di estensioni:

$$K \subset K(\alpha) \subset E$$

con  $[K(\alpha) : K] = m$  e  $[E : K(\alpha)] = d$ . Se  $m = n$ , allora  $E = K(\alpha)$  e siamo ancora nel caso precedente; se  $1 < m < n \implies d < n$ , essendo  $n = md$  (in pratica stiamo supponendo di aver già messo nell'estensione almeno un nuovo elemento), dunque per la [Proposizione 3.37](#)  $\varphi$  si estende in  $m$  modi a  $K(\alpha)$ :

$$\varphi_1, \dots, \varphi_m : K(\alpha) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi$$

Ogni  $\varphi_i : K(\alpha) \hookrightarrow \overline{K}$  si estende a sua volta per ipotesi induttiva:

$$\varphi_{i1}, \dots, \varphi_{id} : E \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_{ij|K(\alpha)} = \varphi_i$$

spazi, typo

Proposizione  $\rightarrow$  Proposizione

$$1d \rightarrow id$$

```
\[ \varphi_1, \dots, \varphi_n : E \rightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi
```

essendo  $n = md$  (in pratica stiamo supponendo di aver già messo nell'estensione almeno un nuovo elemento), dunque per la [Proposizione 3.37](#)  $\varphi$  si estende in  $m$  modi a  $K(\alpha)$ :

```
\[ \varphi_1, \dots, \varphi_m : K(\alpha) \rightarrow \overline{K} \quad \text{con} \quad \varphi_{i|K} = \varphi
```

```
\[ \varphi_{i1}, \dots, \varphi_{id} : E \rightarrow \overline{K} \quad \text{con} \quad \varphi_{ij|K(\alpha)} = \varphi_i
```

### §3.3 Estensioni normali

**Definizione 3.40.** Dato  $\alpha \in \overline{K}$ , diciamo che i **coniugati** di  $\alpha$  su  $K$  sono le radici del polinomio minimo di  $\alpha$  su  $K$ .

**Definizione 3.41.** Data un'estensione algebrica  $K \subset L$ , essa si dice **separabile** se il polinomio minimo di ogni elemento è un **polinomio separabile**, ovvero se ha radici tutte distinte in un suo campo di spezzamento.<sup>43</sup>

Nella trattazione di teoria di campi di queste dispense considereremo soltanto estensioni separabili.

<sup>43</sup>Questa definizione è stata aggiunta per completezza al materiale della professoressa, infatti verrà citata successivamente qualche volta, pertanto, sebbene non vi sarà una trattazione ulteriore a riguardo, ho ritenuto opportuno aggiungerla qui.

## aggiunte varie, punteggiatura

```
\begin{definition}
    Dato  $\alpha \in \overline{K}$ , diciamo che i \vocab{coniugati} di  $\alpha$  su  $K$  sono le radici in  $\overline{K}$  del polinomio minimo di  $\alpha$  su  $K$ .
\end{definition}

\begin{definition}
    Data un'estensione algebrica  $K \subset L$ , essa si dice \vocab{separabile} se il polinomio minimo di ogni elemento di  $L$  è un \vocab{polinomio separabile}, ovvero ha radici tutte distinte nel suo campo di spezzamento (o equivalentemente in una chiusura algebrica di  $K$ ).
    \footnote{Questa definizione è stata aggiunta per completezza al materiale della professoressa, infatti verrà citata successivamente qualche volta; pertanto, sebbene non vi sarà una trattazione ulteriore a riguardo, ho ritenuto opportuno aggiungerla qui.}
\end{definition}
```

Nella trattazione di teoria di campi di queste dispense considereremo soltanto estensioni separabili.

\footnote{Abbiamo visto che su un campo perfetto ogni polinomio irriducibile è separabile.}

Questo implica che le estensioni algebriche di un campo perfetto sono separabili, dato che i polinomi minimi sono polinomi irriducibili.

Quindi limitandoci ai campi perfetti effettivamente abbiamo a che fare solo con estensioni separabili.}

r. 4599; p. 113

### Esempio 3.42

Sia  $f(x) = x^3 - 2$ , tale polinomio coincide con  $\mu_{\sqrt[3]{2}/\mathbb{Q}}(x)$ , ovvero il polinomio minimo di  $\alpha = \sqrt[3]{2}$  su  $\mathbb{Q}$ , vogliamo studiare le immersioni di  $\mathbb{Q}(\alpha)$  in  $\overline{\mathbb{Q}}$ :

$$\varphi : \mathbb{Q}(\alpha) \longrightarrow \overline{\mathbb{Q}} \quad \text{con} \quad \varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}$$

spazi, tipo

```
\[ \varphi : \mathbb{Q}(\alpha) \rightarrow \overline{\mathbb{Q}} \quad \text{con} \quad \varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}
```

---

rr. 4622-4624, 4628; p. 114

### Esempio 3.43

Sia  $p$  un primo e consideriamo il campo ciclotomico  $p$ -esimo  $\mathbb{Q}(\zeta_p)$ ; per tale campo abbiamo che:

$$\mu_{\zeta_p/\mathbb{Q}}(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x + 1$$

il quale è irriducibile perché è traslato di un  $p$ -Eisenstein, pertanto i coniugati di  $\zeta_p$  sono  $\zeta_p^i$ , con  $1 \leq i < p$  (ovvero sono  $p - 1$ ), da cui:

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \phi(p) = p - 1$$

Le immersioni di  $\mathbb{Q}(\zeta_p)/\mathbb{Q}$  sono del tipo:

$$\varphi_i : \mathbb{Q}(\zeta_p) \longrightarrow \overline{\mathbb{Q}} : \zeta_p \longmapsto \zeta_p^i \quad \text{con} \quad \varphi_i|_{\mathbb{Q}} = id_{\mathbb{Q}}$$

aggiunta, spazi

il quale è irriducibile perché è traslato di un  $p$ -Eisenstein,  
Cioè  $\mu(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{x^p}{x} = x^{p-1}$

```
\[ \varphi_i : \mathbb{Q}(\zeta_p) \rightarrow \overline{\mathbb{Q}} : \zeta_p \longmapsto \zeta_p^i \quad \text{con} \quad \varphi_i|_{\mathbb{Q}} = id_{\mathbb{Q}}
```

**Definizione 3.44.** Un'estensione algebrica  $F/K$  si dice **normale** se:

$$\forall \varphi : F \hookrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K$$

si ha che  $\varphi(F) = F$ , ovvero l'estensione viene fissata da ogni immersione del campo di partenza nella sua chiusura algebrica.

- Detto  $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ , allora l'estensione  $F/\mathbb{Q}$  è normale, infatti data:

$$\varphi : F \hookrightarrow \overline{\mathbb{Q}} \quad \text{con} \quad \varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}$$

con:

$$\varphi(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) = \mathbb{Q}(\varphi(\sqrt[3]{2}), \varphi(\zeta_3)) = \mathbb{Q}(\sqrt[3]{2}\zeta_3^i, \zeta_3^j) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

spazi

```
\[ \forall \varphi : F \rightarrow \overline{K} \quad \text{con} \quad
\varphi|_K = id_K
\]
```

```
\[ \forall \varphi : F \rightarrow \overline{\mathbb{Q}} \quad \text{con} \quad
\varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}
\]
abbiamo che:
\[ \varphi(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}\zeta_3^i, \zeta_3^j) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)
\]
```

- (1)  $\implies$  (2): sia  $f(x) \in K[x]$  e siano  $\alpha_1, \dots, \alpha_n \in \overline{K}$  le radici di  $F$ , per ipotesi sappiamo che  $f(x)$  ha almeno una radice in  $F$ , supponiamo sia  $\alpha_1$ , allora  $K(\alpha_1) \subset F$ , dunque  $\forall i \in \{1, \dots, n\}$  consideriamo le immersioni:

$$\varphi_i : K(\alpha_1) \hookrightarrow K(\alpha_i) \subseteq \overline{K} : \alpha_1 \mapsto \alpha_i \quad \text{con } \varphi_{i|K} = id_K$$

esse esistono sempre per la [Proposizione 3.33](#), inoltre,  $\forall i \in \{1, \dots, n\}$  sia  $\tilde{\varphi}_i$  un'estensione di  $\varphi_i$  a  $F$ , cioè ogni immersione di  $K(\alpha_i)$  si estende ad  $F$  in tanti modi quanti il grado  $[F : K(\alpha_1)]$ , pertanto, fissata un'estensione di  $\varphi_i$ :

$$\tilde{\varphi}_i : (K(\alpha_i) \subset)F \longrightarrow \overline{K} \quad \text{con } \tilde{\varphi}_{i|K(\alpha_1)} = \varphi_i \implies \tilde{\varphi}_{i|K} = id_K$$

cioè  $\tilde{\varphi}_i$  si restringe a  $K$  proprio come  $\varphi_i$ , da cui, essendo  $F/K$  normale, si ha che  $\tilde{\varphi}_i(F) = F$ , ma in particolare ciò significa che dalla radice  $\alpha_1$  di  $f(x)$ , che va nei suoi coniugati mediante  $\tilde{\varphi}_i$ , otteniamo tutte le altre radici dentro  $F$ :

$$\tilde{\varphi}_i(\alpha_1) = \varphi_i(\alpha_1) = \alpha_i \in F \quad \forall i \in \{1, \dots, n\}$$

che prova la tesi.

## typo, spazi, riscrittura

$$F \rightarrow f(x)$$

```
\item \underline{\textbf{(1)} \implies (2)}: sia $f(x) \in K[x]$ e siano $\alpha_1, \dots, \alpha_n \in \overline{K}$ le radici di $f(x)$, per ipotesi sappiamo che $f(x)$ ha almeno una radice in $F$, supponiamo sia $\alpha_1$, allora $K(\alpha_1) \subset F$, dunque
```

```
\[ \varphi_i : K(\alpha_1) \xrightarrow{\text{con}} K(\alpha_i) \subseteq \overline{K} : \alpha_1 \mapsto \alpha_i \quad \text{con } \varphi_{i|K} = id_K \]
```

```
\[ \tilde{\varphi}_i : (K(\alpha_i) \subset)F \xrightarrow{\text{con}} \overline{K} : \alpha_i \mapsto \tilde{\varphi}_i(\alpha_i) \quad \text{con } \tilde{\varphi}_{i|K(\alpha_1)} = \varphi_i \implies \tilde{\varphi}_{i|K} = id_K \]
```

```
\[ \alpha_i = \tilde{\varphi}_i(\alpha_1) \in F \quad \forall i \in \{1, \dots, n\} \]
```

- (2)  $\implies$  (3): Consideriamo  $F_0$  il campo di spezzamento su  $K$  della famiglia di polinomi:

$$\mathcal{F} = \{\mu_\alpha(x) \mid \alpha \in F, \mu_\alpha(x) \text{ polinomio minimo di } \alpha \text{ su } K\}$$

abbiamo che  $F \subseteq F_0$ , poiché abbiamo aggiunto tutte le radici di tutti i polinomi minimi di tutti gli elementi di  $F$ , dunque  $F_0$  contiene almeno  $F$ . D'altra parte:

$$F_0 = K(\beta \mid \beta \text{ radice di } \mu_\alpha(x) \in \mathcal{F})$$

dove  $\mu_\alpha(x)$  è irriducibile su  $K[x]$  e  $\alpha$  è una sua radice in  $F$ , dunque per ipotesi  $F$  contiene tutte le radici  $\beta$  di  $\mu_\alpha(x)$ ,  $\forall \mu_\alpha(x) \in \mathcal{F}$ , ovvero  $F_0 \subseteq F$ , quindi  $F = F_0$ , per cui  $F$  è proprio il campo di spezzamento dei polinomi della famiglia  $\mathcal{F}$ .

- (3)  $\implies$  (1): Consideriamo:

$$\varphi : F \longrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K$$

usare `\mid`, riscrittura, spazi

```
\[ \mathcal{F} = \{ \mu_\alpha(x) \mid \alpha \in F, \text{ ``} \mu_\alpha(x) \text{ polinomio minimo di } \alpha \text{ su } K \} \]
```

abbiamo che  $F \subseteq F_0$ , poiché abbiamo aggiunto tutte le radici del polinomio minimo di ogni elemento di  $F$ , dunque  $F_0$  contiene  $F$ .

```
\[ F_0 = K(\beta \mid \text{``} \beta \text{ radice di } \mu_\alpha(x) \in \mathcal{F} \text{''}) \]
```

```
\[ \varphi : F \varlonghookrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K \]
```

---

rr. 4702, 4707; p. 116

per cui  $\{\alpha_{ij}\}_{j=1,\dots,n_i}$  sono le radici di  $f_i(x)$ , dunque possiamo riscrivere  $F$  come:

$$F = K(\{\alpha_{ij}\} \mid i = 1, \dots, k, j = 1, \dots, n_i)^{44}$$

Sappiamo che per ogni  $i$  e  $j$ , poiché  $\varphi$  è un'immersione deve mandare le radici in loro coniugati, dunque  $\varphi(\alpha_{ij}) = \alpha_{ij'}$  (ovvero un'altra radice dello stesso polinomio  $f_i(x) \in K[x]$ , con  $\mu_{\alpha_{ij}}(x) \mid f_i(x)$ ), da cui abbiamo che:

$$\begin{aligned} \varphi(F) &= \varphi(K(\{\alpha_{ij}\} \mid i = 1, \dots, k, j = 1, \dots, n_i)) = \\ &= K(\varphi(\alpha_{ij}) \mid i = 1, \dots, k, j = 1, \dots, n_i) \subset F \end{aligned}$$

dove il contenimento segue dal fatto che abbiamo soltanto permutato gli elementi  $\{\alpha_{ij}\}$ , per cui  $K \subset \varphi(F) \subset F$ , ma poiché  $F$  e  $\varphi(F)$  hanno lo stesso grado finito su  $K$ , allora  $\varphi(F) = F$ .

usare `\mid`

```
\[ F = K(\{\alpha_{ij}\} \mid i = 1, \dots, k, j = 1, \dots, n_i)
\footnote{Potremmo anche considerare il campo di spezzamento del polinomio prodotto dei precedenti, ma le radici sarebbero sempre le stesse.}
\]
```

```
\begin{multiline*}
\varphi(F) = \varphi(K(\{\alpha_{ij}\} \mid i = 1, \dots, k, j = 1, \dots, n_i)) = \\
= K(\varphi(\alpha_{ij}) \mid i = 1, \dots, k, j = 1, \dots, n_i)
\subset F
\end{multiline*}
```

**Esempio 3.47** (Ogni estensione di grado 2 è normale)

Sia  $F/K$  un'estensione, supponiamo di essere in caratteristica diversa da  $2^a$ , con  $[F : K] = 2$  e sia  $\alpha \in F \setminus K \implies F = K(\alpha)$  abbiamo che quindi il polinomio minimo è della forma:

$$\mu_\alpha(x) = x^2 + bx + c \in K[x]$$

typo

$$x \rightarrow c$$

```
\[ \mu_\alpha(x) = x^2 + bx + c \in K[x]
```

essendo  $K \subset F$ , allora  $\text{id}_F$  include già  $\text{id}_K$ , quindi  $\varphi|_F = \text{id}_F \implies \varphi|_K = \text{id}_K$ , dato che  $L/K$  è normale, abbiamo  $\varphi(L) = L$  per tutte le immersioni  $\varphi$  di  $L$  che fissano  $K$ , ma abbiamo visto che le immersioni che fissano  $F$  fissano  $K$  dunque  $\varphi(L) = L$  anche in questo caso, pertanto  $L/F$  è normale.

*Dimostrazione alternativa.*<sup>47</sup>  $L/K$  normale significa che è campo di spezzamento di una famiglia di polinomi in  $K[x] \subseteq F[x]$ , quindi  $L$  è il campo di spezzamento della stessa famiglia vista come polinomi in  $F$ .  $\square$

punteggiatura, typo, aggiunte, riscrittura

```
essendo $K \subset F$, allora $id_F$ include già $id_K$, quindi $\varphi_{|F} = id_F \implies \varphi_{|K} = id_K$.
Dato che $\faktor{L}{K}$ è normale, abbiamo $\varphi(L)=L$ per tutte le immersioni $\varphi$ di $L$ che fissano $K$,
ma abbiamo visto che le immersioni che fissano $F$ fissano anche $K$ dunque
$\varphi(L) = L$ per tutte le immersioni di $L$ che fissano $F$,
ovvero $\faktor{L}{F}$ è normale. \\
```

### §3.4 Gruppo di Galois

**Definizione 3.53.** Un'estensione  $E/K$  si dice **estensione di Galois** se è normale e separabile.

In queste dispense tratteremo soltanto il caso di estensioni di Galois finite. Poiché  $E/K$  è normale possiamo considerare l'insieme:

$$\{\varphi : E \hookrightarrow \overline{K} \mid \varphi|_K = id_K\}$$

considerando ora lo stesso insieme, poiché l'estensione è normale, dunque  $\varphi(E) = E$  per ogni  $\varphi$ , possiamo restringere l'insieme di arrivo degli omomorfismi ottenendo:

$$\text{Aut}_K E = \{\varphi : E \xrightarrow{\sim} E \mid \varphi|_K = id_K\}$$

i  $K$ -automorfismi di  $E$ , cioè gli automorfismi dell'estensione che fissano  $K$ , tale insieme con l'operazione di composizione forma il **gruppo di Galois**:

$$\text{Gal}(E/K) := \text{Aut}_K(E)$$

con:

$$|\text{Gal}(E/K)| = [E : K]$$

riscritture e aggiunte varie, usare  $\mid$

Un'estensione  $\mathbf{\faktor{E}{K}}$  si dice **estensione di Galois** se è normale e separabile.

\footnote{Dato che in queste dispense consideriamo solo estensioni separabili, per noi "estensione di Galois" è equivalente a "estensione normale".}

In queste dispense tratteremo soltanto il caso di estensioni di Galois finite.

\\\

Consideriamo l'insieme:

```
\[ \{ \varphi : E \xrightarrow{\sim} \overline{K} \mid \varphi|_K = id_K \}
```

Poiché  $\mathbf{\faktor{E}{K}}$  è normale, dunque  $\varphi(E) = E$  per ogni  $\varphi$ , possiamo restringere il codominio ottenendo:

```
\[ \text{Aut}_K E = \{ \varphi : E \xrightarrow{\sim} E \mid \varphi|_K = id_K \}
```

\footnote{\varphi è iniettiva perché omomorfismo da un campo e surgettiva (dopo aver ristretto il codominio) grazie all'ipotesi di normalità, quindi è un automorfismo di  $E$ .}

\]

e per il corollario 3.39 (ricordiamo che come sempre  $E$  è perfetto)

r. 4815; p. 119

### Proposizione 3.54

Il gruppo di Galois dell'estensione di Galois  $E/K$ ,  $\text{Gal}(E/K)$  è un gruppo.

*Dimostrazione.* Essendo un sottoinsieme del gruppo degli automorfismi di un campo, è sufficiente mostrare che è un suo sottogruppo, dunque date  $\varphi, \psi \in \text{Gal}(E/K)$ , allora si verifica che  $\varphi \circ \psi \in \text{Gal}(E/K)$ , inoltre, essendo automorfismi sono invertibili e i loro inversi sono ancora automorfismi, dunque:

Essendo un sottoinsieme del gruppo degli automorfismi di un campo, è sufficiente mostrare che è un suo sottogruppo, dunque date  $\varphi, \psi \in \text{Gal}(E/K)$ , allora

---

r. 4831; p. 119

*Dimostrazione.* Dette  $\alpha_1, \dots, \alpha_n$  le radici di  $f(x)$  in  $\overline{K}$ , allora  $F = K(\alpha_1, \dots, \alpha_n)$ , da cui si ha la torre:

$$K \subseteq K(\alpha_1) \subseteq F \implies n = [K(\alpha_1) : K] \mid [F : K] = |\text{Gal}(F/K)|$$

usare  $\Big|$  per maggiore leggibilità

$$\begin{aligned} & \forall K \subseteq K(\alpha_1) \subseteq F \implies n = [K(\alpha_1) : K] \mid [F : K] \\ & [F : K] = |\text{Gal}(F/K)| \end{aligned}$$

---

- $\phi$  è ben definita: poiché  $\forall \varphi \in \text{Gal}(F/K)$ ,  $\varphi$  permuta le radici di  $f(x)$  poiché manda ciascuna in un suo coniugato.

- $\phi$  è un omomorfismo: si verifica direttamente che:

$$\phi(\varphi \circ \psi) = (\varphi \circ \psi)|_{\{\alpha_1, \dots, \alpha_n\}} = \varphi(\psi|_{\{\alpha_1, \dots, \alpha_n\}}) = \varphi|_{\{\alpha_1, \dots, \alpha_n\}} \circ \psi|_{\{\alpha_1, \dots, \alpha_n\}}$$

$\forall \phi, \psi \in \text{Gal}(F/K)$ , in questo caso stiamo restringendo  $\varphi$  alle radici perché  $\psi$  sulle radici ha immagine nelle radici, per quanto detto sopra.

dove l'ultima uguaglianza è data dal fatto che se  $\varphi$  fissa tutti i generatori di  $F/K$ , l'unica possibilità è che sia l'identità (banalmente perché stiamo considerando funzioni che permutano delle radici, dunque ce n'è una sola che le lascia tutte fisse ed è l'identità). In alternativa si poteva anche osservare che  $\varphi$  è in particolare  $K$  lineare e le radici formano una base su  $K$  di  $F$ , dunque dato che  $\varphi$  coincide con l'identità su queste essa è l'identità.

## riscrittura, punteggiatura

```
\item \underline{\textbf{$\phi$ è un omomorfismo}}: si verifica direttamente che $\forall \varphi, \psi \in \text{Gal}(F/K)$:
```

$$\begin{aligned} \phi(\varphi \circ \psi) &= (\varphi \circ \psi)|_{\{\alpha_1, \dots, \alpha_n\}} \\ \varphi|_{\{\alpha_1, \dots, \alpha_n\}} \circ \psi|_{\{\alpha_1, \dots, \alpha_n\}} &= \\ \varphi|_{\{\alpha_1, \dots, \alpha_n\}} \circ \psi|_{\{\alpha_1, \dots, \alpha_n\}} &= \end{aligned}$$

in questo caso stiamo restringendo  $\varphi$  alle radici perché

$\psi$  sulle radici ha immagine nelle radici, per quanto detto sopra.

con l'identità su queste, essa è l'identità.

**Osservazione 3.56 —** Con la dimostrazione precedente abbiamo anche visto che il gruppo di Galois agisce fedelmente su  $\{\alpha_1, \dots, \alpha_n\}$ . Inoltre tale azione è transitiva perché ha un'unica orbita:

$$\text{Orb}(\alpha_1) = \left\{ \varphi(\alpha_1) \mid \varphi \in \text{Gal}(F/K) \right\} = \{\alpha_1, \dots, \alpha_n\}$$

infatti, essendo  $[K(\alpha_1) : K] = n$ , allora ho esattamente  $n$  immersioni che permutano i coniugati (ognuna delle quali si può estendere ad  $F$ ):

$$\forall i \in \{1, \dots, n\}, \exists \psi_i : K(\alpha_1) \longrightarrow K(\alpha_i) \subset \overline{K} : \alpha_1 \longmapsto \alpha_i$$

e per tali immersioni abbiamo appunto che l'unica orbita è quella vista sopra.

## spazi, riscrittura

```
\[ \text{Orb}(\alpha_1) = \left\{ \varphi(\alpha_1) \mid \varphi \in \text{Gal}(F/K) \right\} = \{\alpha_1, \dots, \alpha_n\}
```

```
\[ \exists \psi_i : K(\alpha_1) \longrightarrow K(\alpha_i) \subset \overline{K} : \alpha_1 \longmapsto \alpha_i \quad \forall i \in \{1, \dots, n\}
```

---

rr. 4866, 4869-4875; p. 121

- Se  $\deg f(x) = 2$ , allora  $[F : K] = 2$ , per la Proposizione 3.55, dunque  $\text{Gal}\left(\frac{F}{K}\right) \cong \mathbb{Z}/2\mathbb{Z}$ , pertanto  $\text{Gal}\left(\frac{F}{K}\right) = \{\text{id}, \varphi\}$ , dove, essendo  $F = K(\sqrt{\Delta})$  abbiamo che:

$$id : a + b\sqrt{\Delta} \mapsto a + b\sqrt{\Delta} \quad \text{and} \quad \varphi : a + b\sqrt{\Delta} \mapsto a - b\sqrt{\Delta}$$

o analogamente, se fosse  $f(x) = (x - \alpha_1)(x - \alpha_2)$  le applicazioni sarebbero state tali che  $\text{id} : \alpha_1 \mapsto \alpha_1$  e  $\varphi : \alpha_1 \mapsto \alpha_2$ .

- Se  $\deg f(x) = 3$ , allora  $[F : K] \leq 6$ , per la [Proposizione 3.55](#) sappiamo che  $\text{Gal}\left(\frac{F}{K}\right) \leq S_3$  pertanto:

### riscritture varie

(nel primo caso non serve la Prop. 3.55, sappiamo già che

$$|Gal(F/K)| = [F:K]$$

\item Se  $\deg f(x) = 2$ , allora  $[F : K] = 2$ , dunque  
 $\left(\frac{F}{K}\right) \cong \mathbb{Z}_2$ , pertanto  
 $\left(\frac{F}{K}\right) = \{\text{id}, \varphi\}$ , dove, essendo  $F = K(\sqrt{\Delta})$  abbiamo che:

o analogamente, se fosse  $f(x) = (x - \alpha_1)(x - \alpha_2)$  le applicazioni sarebbero state tali che

```
\begin{align*}
    id : \alpha_1 \longmapsto \alpha_1, \alpha_2 \longmapsto \alpha_2 \\
    \varphi : \alpha_1 \longmapsto \alpha_2, \alpha_2 \longmapsto \alpha_1
\end{align*}
```

\item Se  $\deg f(x) = 3$ , allora per la \hyperref[3.55]{Proposizione 3.55} vale  

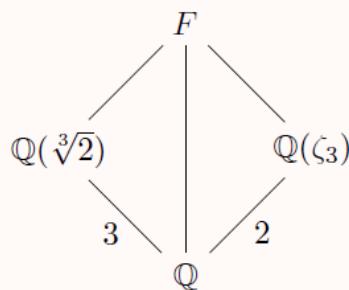
$$3 \mid F : K \mid 6 \text{ e } \left( \frac{F}{K} \right) \leqslant S_3$$
 pertanto:

**Esempio 3.58**

Se fosse  $f(x) = x^3 - 2$ , con  $K = \mathbb{Q}$  e  $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \implies [F : K] = 6$  e quindi  $\text{Gal}(F/K) \cong S_3$ ; per quanto detto sulle immersioni sappiamo che qualsiasi automorfismo del gruppo di Galois deve mandare un elemento nei suoi coniugati, quindi abbiamo in totale appunto 6 possibili immersioni al variare di  $\varphi$ :

$$\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3^i \quad \text{e} \quad \varphi(\zeta_3) = \zeta_3^j \quad \text{con } i \in \{0, 1, 2\}, j \in \{0, 1\}$$

Necessariamente  $\varphi$  deve verificare le relazioni sopra<sup>a</sup> che danno al più 6 possibili  $\varphi$ . Poiché il grado è 6, tutte e 6 funzionano cioè si estendono ad  $F$ , ciò perché:



ovvero  $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 6$ .

<sup>a</sup>E per la precisione, affinché il discorso fatto sopra funzioni gli elementi devono essere algebricamente indipendenti.

riscritture e aggiunte varie

[continua ...]

Se fosse  $f(x) = x^3 - 2$ , con  $K = \mathbb{Q}(\sqrt[3]{2})$  e  $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$   
 $\text{implies } [F : K] = 6$  e quindi  $\text{Gal}(F/K)$  (ricordiamo che questa estensione è normale, quindi di Galois). \\

Infatti, per quanto detto sulle immersioni sappiamo che qualsiasi automorfismo del gruppo di Galois

deve mandare le radici di  $f(x)$  nei suoi coniugati, quindi abbiamo 6 possibili immersioni:

```
\[ \varphi(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3^i \quad \text{e} \quad \varphi(\zeta_3) = \zeta_3^j \quad \text{con } i \in \{0,1,2\}, j \in \{1,2\}
```

Necessariamente  $\varphi$  deve verificare le relazioni sopra che danno al più 6 possibilità.

\footnote{Definire gli omomorfismi sui generatori ci dà un upper bound perché in generale ci potrebbero essere delle relazioni ulteriori tra questi generatori; quindi non tutte le immersioni  $\varphi$  potrebbero andar bene.}

Se i generatori sono algebricamente indipendenti (cioè non sussistono relazioni di tipo polinomiale tra loro),

allora tutte le  $\varphi$  funzionano e possiamo contare in modo combinatorio contando le scelte per ogni generatore. \\

Detto questo non è facile mostrare che due elementi sono indipendenti (bisognerebbe mostrare che ogni possibile relazione polinomiale non è verificata), quindi nella pratica si preferisce ricorrere ad argomenti più generali (per esempio il corollario 3.39).}

Ma dalla teoria sappiamo che ci devono essere esattamente 6 estensioni:

ovvero  $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 6$ . \\

Quindi effettivamente tutte le  $\varphi$  che avevamo trovato funzionano.

---

**Esempio 3.59** (Vi sconsiglio caldamente di leggere quest'esempio prima che l'abbia riscritto)

<sup>a</sup> Consideriamo  $f(x) = x^3 + x^2 - 2x - 1$ , ovvero il polinomio minimo di  $\zeta_7 + \zeta_7^{-1}$  su  $\mathbb{Q}$  e  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ , che è normale, quindi di Galois<sup>b</sup>, abbiamo quindi che:

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}\right) \cong \mathcal{A}_3$$

verifichiamo quanto appena detto. Abbiamo che  $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \phi(7) = 6$ , pertanto:

$$\text{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right) = \{\varphi : \zeta_7 \mapsto \zeta_7^i \mid (i, 7) = 1\}$$

Osserviamo che il polinomio scritto sopra è proprio il polinomio minimo di  $\alpha = \zeta_7 + \zeta_7^{-1} \in \mathbb{Q}(\zeta_7)$ , infatti per l'appartenenza appena citata sappiamo che tutte le radici di  $\mu_{\zeta_7+\zeta_7^{-1}}(x)$  stanno in  $\mathbb{Q}(\zeta_7)$ , ed esse sono:

$$\left\{ \varphi(\alpha) \mid \varphi \in \text{Gal} \left( \mathbb{Q}(\zeta_7)/\mathbb{Q} \right) \right\}$$

typo, punteggiatura, spazi

[comunque questo esercizio l'ha fatto meglio Lombardo]

Consideriamo  $f(x) = x^3 + x^2 - 2x - 1$ , ovvero il polinomio minimo di  $\zeta_7 + \zeta_7^{-1}$  su  $Q$  e  $\text{faktor}(Q(\zeta_7 + \zeta_7^{-1}))Q$ , che è normale (quindi di Galois) e dunque abbiamo che:

Verifichiamo quanto appena detto. Abbiamo che  $\zeta_7$  è un numero complesso di quinto grado, quindi  $\phi(7) = 6$ , pertanto:

```
\[ \left( \operatorname{\faktor}{\zeta_7}{\zeta_7^i} \mid i,7 = 1 \right) \]

```

```
\[ \left\{ \varphi(\alpha) \sim \Big| \varphi \in \right.
\\ \left. \text{Gal} \left( \text{faktor} \{ \text{QQ}(\zeta_7) \} \{ \text{QQ} \} \right) \right\}
\\ \right]
```

### §3.5 Gruppo di Galois di $\mathbb{F}_{q^d}/\mathbb{F}_q$

**Proposizione 3.60** (L'estensione  $\mathbb{F}_{q^d}/\mathbb{F}_q$ )

Data l'estensione  $\mathbb{F}_{q^d}/\mathbb{F}_q$ , con  $q = p^r$ , allora è normale.

usare \faktor, tipo

(nella dimostrazione viene usato  $\mathbb{F}_{p^n}$ , il caso generale viene discusso nell'osservazione successiva)

```
\subsection{Gruppo di Galois di $\faktor{\mathbb{F}{q^d}}{\mathbb{F}{q}}$}
```

```
\begin{proposition}[$\faktor{\mathbb{F}{p^n}}{\mathbb{F}{p}}$]
    L'estensione $\faktor{\mathbb{F}{p^n}}{\mathbb{F}{p}}$ è normale.

```

---

**Osservazione 3.61** — Osserviamo che tutte le estensioni di campi finiti sono normali, infatti, considerando la torre:

$$\begin{array}{c} \mathbb{F}_{p^n} = \mathbb{F}_{q^d} \\ \text{NOR.} \quad \left( \begin{array}{c} \mathbb{F}_q = \mathbb{F}_{p^r} \\ \mathbb{F}_p \end{array} \right) \quad \text{NOR.} \end{array}$$

dove per quanto detto  $\mathbb{F}_{p^n}/\mathbb{F}_p$  è normale, dunque per la Proposizione 3.50 tutte le estensioni di campi finiti sono normali.

## riscrittura varie

```
\begin{remark}
```

Osserviamo che tutte le estensioni di campi finiti sono normali. Infatti, considerando la torre:

```
\begin{tikzpicture}
    \node (Q1) at (0,-1.5) {$\mathbb{F}_p$};
    \node (Q3) at (0,0) {$\mathbb{F}_q = \mathbb{F}_{p^r}$};
    \node (Q4) at (0,1.5) {$\mathbb{F}_{p^n} = \mathbb{F}_{q^d}$};
    \draw (Q4)--(Q3) node [right, yshift=-0.75cm] {NORM.};
    \draw (Q1)--(Q3) node [right, yshift=0.75cm] {NORM.};
    \draw (Q4) to [bend right=45] (Q1) node[left, yshift=1.20cm, xshift=-0.5cm]
{NORM.};
\end{tikzpicture}
```

dove per quanto detto  $\mathbb{F}_{p^n}/\mathbb{F}_p$  e  $\mathbb{F}_{p^n}/\mathbb{F}_p$  sono normali,

dunque per la [Proposizione 3.50](#) anche  $\mathbb{F}_{q^d}/\mathbb{F}_q$  è normale.

```
\end{remark}
```

rr. 4984, 4993; p. 123

**Definizione 3.62.** Si dice **automorfismo di Frobenius** l'automorfismo:

$$\phi : \mathbb{F}_{q^d} \xrightarrow{\sim} \mathbb{F}_{q^d} : x \longmapsto x^q$$

**Teorema 3.63** (Gruppo di Galois di estensioni di campi finiti)

Il gruppo di Galois  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ , con  $q = p^r$ , è generato dall'automorfismo di Frobenius  $\phi$  di  $\mathbb{F}_{q^d}$ :

$$\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \phi \rangle$$

con  $\phi$  automorfismo di Frobenius del campo  $\mathbb{F}_{q^d}$ :

$$\phi : \mathbb{F}_{q^d} \xrightarrow{\sim} \mathbb{F}_{q^d} : x \longmapsto x^q$$

correzioni minori

$$\begin{aligned} & \begin{bmatrix} \phi : \mathbb{F}_{q^d} \xrightarrow{\sim} \mathbb{F}_{q^d} : x \mapsto x^q \\ \end{bmatrix} \end{aligned}$$

$$\begin{aligned} & \begin{bmatrix} \phi : \mathbb{F}_{q^d} \xrightarrow{\sim} \mathbb{F}_{q^d} : x \mapsto x^q \\ \end{bmatrix} \end{aligned}$$

Si verifica facilmente inoltre che è iniettivo e surgettivo.  $\forall \alpha \in \mathbb{F}_q$  si ha che  $\phi(\alpha) = \alpha^q = \alpha$  (perché stiamo considerando elementi di  $\mathbb{F}_q$ ), dunque  $\phi$  è un automorfismo di  $\mathbb{F}_{q^d}$  che lascia fisso  $\mathbb{F}_q$ , pertanto  $\phi \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ , per definizione. Osserviamo che per ipotesi  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  è un gruppo di ordine  $d$  e quindi ovviamente  $\text{ord } \phi = k \mid d$ ; d'altra parte se  $\phi^k = id$ ,  $\forall \alpha \in \mathbb{F}_{q^d}$  si ha che:

$$\phi^k(\alpha) = \alpha^{q^k} = \alpha$$

## correzioni minori

Si verifica facilmente inoltre che è iniettivo e surgettivo.

Dato  $\alpha \in \mathbb{F}_q$  si ha che  $\phi(\alpha) = \alpha^q = \alpha$  (perché stiamo considerando elementi di  $\mathbb{F}_q$ ),

dunque  $\phi$  è un automorfismo di  $\mathbb{F}_{q^d}$  che lascia fisso  $\mathbb{F}_q$ , pertanto  $\phi \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ , per definizione. \\

Osserviamo che per ipotesi  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  è un gruppo di ordine  $d$  e quindi

ovviamente  $k = \text{ord } \phi \mid d$ ; d'altra parte se  $\phi^k = id$ ,  $\forall \alpha \in \mathbb{F}_{q^d}$  si ha che:

con  $\varphi_i(E) = E$ ,  $\forall i = 1, \dots, 4$ . Il gruppo di Galois è dato da  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , poiché ha ordine 4, e tutti gli elementi, esclusa l'identità, hanno ordine 2. Si verifica facilmente via contenimenti che  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ , tuttavia possiamo anche osservare a questo punto che, data la torre:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq E$$

di grado 4, abbiamo che:

$$\varphi_1(\sqrt{2} + \sqrt{3}) = \sqrt{2} + \sqrt{3} \quad \varphi_2(\sqrt{2} + \sqrt{3}) = -\sqrt{2} + \sqrt{3}$$

$$\varphi_3(\sqrt{2} + \sqrt{3}) = \sqrt{2} - \sqrt{3} \quad \varphi_4(\sqrt{2} + \sqrt{3}) = -\sqrt{2} - \sqrt{3}$$

$\gamma = \sqrt{2} + \sqrt{3}$  ha quattro immagini distinte<sup>a</sup> attraverso le immersioni del gruppo di Galois, e mediante questo  $\gamma$  viene mandato in suoi coniugati su  $\mathbb{Q}$ ; dunque il polinomio minimo di  $\gamma$  su  $\mathbb{Q}$  ha almeno grado 4, ma per la torre precedente ciò significa che  $\mathbb{Q}(\gamma) = E$ .

<sup>a</sup>Per essere precisi ciò significa che, data la base  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$  di  $E$ , per mezzo di questa si verifica che tutte e quattro quelle immagini hanno scrittura unica e distinta.

## riscritture e aggiunte varie

con  $\varphi_i(E) = E$ ,  $\forall i = 1, \dots, 4$ . Il gruppo di Galois è dato da  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , poiché ha ordine 4, e tutti gli elementi, esclusa l'identità, hanno ordine 2. \\

Si verifica facilmente via contenimenti che  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . In alternativa possiamo osservare che, data la torre:  

$$[\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = E]$$

dove  $\faktor{E}{\mathbb{Q}}$  è di grado 4, abbiamo che:

$\begin{aligned} \varphi_1(\sqrt{2} + \sqrt{3}) &= \sqrt{2} + \sqrt{3} \\ \varphi_2(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} + \sqrt{3} \\ \varphi_3(\sqrt{2} + \sqrt{3}) &= \sqrt{2} - \sqrt{3} \\ \varphi_4(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} - \sqrt{3} \end{aligned}$

$\end{aligned}$

l'elemento  $\gamma = \sqrt{2} + \sqrt{3}$  ha quattro immagini distinte

$\footnote{Infatti E è uno spazio vettoriale su \mathbb{Q} e le immagini di \gamma nella base \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} hanno tutte scritture distinte.}$

attraverso gli elementi del gruppo di Galois, e sono coniugati di  $\gamma$  su  $\mathbb{Q}$ ;  
dunque il polinomio minimo di  $\gamma$  su  $\mathbb{Q}$  ha almeno grado 4, ma per la torre precedente ciò significa che  $\mathbb{Q}(\gamma) = E$ .

**Osservazione 3.65 —** In questo caso abbiamo assunto direttamente che  $\deg \mu_\gamma(x) = 4$ , perché  $\deg \mu_\gamma = \#\{\psi : \mathbb{Q}(\gamma) \hookrightarrow \overline{\mathbb{Q}}\}$  e ogni  $\psi$  si estende ad  $E$ , via:

$$\varphi_i : E \hookrightarrow \overline{\mathbb{Q}}$$

pertanto  $\{\varphi_i(\gamma)\}$  è l'insieme dei coniugati di  $\gamma$  su  $\mathbb{Q}$ .

aggiunte

```
\[ \varphi_i : E \xrightarrow{\text{con}} \overline{\mathbb{Q}} \quad \varphi_i(\gamma) = \text{id}_{\overline{\mathbb{Q}}}(\gamma) \]
pertanto  $\{\varphi_i(\gamma)\} = \{\psi(\gamma)\}$  è l'insieme dei coniugati di  $\gamma$  su  $\overline{\mathbb{Q}}$ .
```

- **$K$  campo infinito:** Per ipotesi abbiamo che  $E/K$  è finita, dunque per la [Proposizione 3.16](#), ciò è equivalente al dire che  $E$  è finitamente generata da elementi algebrici,  $E = K(\alpha_1, \dots, \alpha_n)$ , dimostriamo per induzione che  $E/K$  è semplice. Per  $n = 2$  (trattiamo solo di questo caso in quanto una volta dimostrata la tesi per  $n = 2$ , basterà come al solito aggiungere un altro alla volta e procedere per induzione usando il caso  $n = 2$  come fatto che rende vero il passo induttivo<sup>48</sup>) abbiamo  $E = K(\alpha, \beta)$ , sia  $[E : K] = n$ , allora per il [Corollario 3.35](#):

$$\exists \varphi_1, \dots, \varphi_n : E \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_i|_K = \text{id}_K$$

sia  $x$  un'indeterminata, consideriamo i polinomi  $\alpha + \beta x$ , possiamo definire il polinomio:

$$F(x) = \prod_{i < j} (\varphi_i(\alpha) + x\varphi_i(\beta) - \varphi_j(\alpha) - x\varphi_j(\beta)) \in \overline{K}[x]$$

con  $\deg F(x) \leq \binom{n}{2}$  e  $F(x) \neq 0$  in quanto se un fattore fosse 0, quindi  $\varphi_i(\alpha) + x\varphi_i(\beta) = \varphi_j(\alpha) + x\varphi_j(\beta)$ , da cui  $x(\varphi_i(\beta) - \varphi_j(\beta)) + \varphi_i(\alpha) - \varphi_j(\alpha) = 0$ , per il principio di identità dei polinomi avremmo:

$$\begin{cases} \varphi_i(\beta) - \varphi_j(\beta) = 0 \\ \varphi_i(\alpha) - \varphi_j(\alpha) = 0 \end{cases} \iff \begin{cases} \varphi_i(\beta) = \varphi_j(\beta) \\ \varphi_i(\alpha) = \varphi_j(\alpha) \end{cases}$$

da cui  $\varphi_i \equiv \varphi_j$  perché  $E = K(\alpha, \beta)$  (infatti due immersioni in cui i generatori coincidono sono la stessa immersione), ma ciò è assurdo, in quanto avevamo assunto  $i < j$ . Dunque il polinomio è non nullo ed ha grado limitato, sappiamo quindi che  $F(x)$  ha al più  $\deg F(x)$  radici in  $\overline{K}$  e poiché  $K$  è un campo infinito, allora  $\exists t \in K$  tale che  $F(t) \neq 0$ , dunque:

$$F(t) = \prod_{i < j} (\underbrace{\varphi_i(\alpha) + t\varphi_i(\beta)}_{=\varphi_i(\alpha+x\beta)} - \underbrace{\varphi_j(\alpha) - t\varphi_j(\beta)}_{=-\varphi_j(\alpha+x\beta)}) \neq 0$$

da ciò abbiamo che:

$$\varphi_i(\alpha + t\beta) \neq \varphi_j(\alpha + t\beta) \quad \forall i \neq j$$

quindi  $\gamma = \alpha + t\beta$  ha  $n$  coniugati, pertanto  $[K(\gamma) : K] = n \implies E = K(\gamma)$  (ovvero le due estensioni dello stesso campo hanno lo stesso grado e quindi coincidono).

<sup>48</sup> Andrebbe dimostrato anche il caso  $n = 1$ , ma è banale.

<sup>49</sup> È come se applicassimo  $\varphi_i$  al polinomio  $\alpha + \beta x$  e poi vi sottraessimo  $\varphi_j$  applicata allo stesso.

- **$K$  campo finito:** Se  $E/K$  è finita, allora  $E$  è finito, da cui, per la nota proprietà sui sottogruppi moltiplicativi di un campo finito, sia che  $E^*$  è un sottogruppo moltiplicativo finito di  $E$  ed è ciclico,  $E^* = \langle \gamma \rangle$ , ma per un altro teorema noto da Aritmetica, si ha che  $E = K(\gamma)$ .

## riscrittura e aggiunte varie

```
\begin{proof}
Distinguiamo due casi:
\begin{itemize}
\item \underline{\textbf{$K$ campo infinito}}:
Per ipotesi abbiamo che $\faktor{E}{K}$ è finita, dunque per l'osservazione 3.17, ciò è equivalente a dire che $E$ è finitamente generata da elementi algebrici, $E = K(\alpha_1, \dots, \alpha_s)$. Dimostriamo per induzione che $\faktor{E}{K}$ è semplice. \\

Basta mostrare il caso $s = 2$, infatti per $s = 1$ la tesi è ovvia e per $s$ generico possiamo scrivere
\begin{array}{l}
[ K(\alpha_1, \dots, \alpha_s) = K(\alpha_1, \alpha_2)(\alpha_3, \dots, \alpha_s) \\
\quad ]
\end{array}
ma per ipotesi induttiva $K(\alpha_1, \alpha_2)$ è semplice quindi
\begin{array}{l}
[ K(\alpha_1, \dots, \alpha_s) = K(\gamma)(\alpha_3, \dots, \alpha_s) = \\
\quad K(\gamma, \alpha_3)(\alpha_4, \dots, \alpha_s) \\
\quad ]
\end{array}
e così via, spostando un elemento per volta e utilizzando ripetutamente l'ipotesi induttiva per $s = 2$. \\

Sia $s = 2$ e $n = [E : K]$, allora abbiamo $E = K(\alpha, \beta)$ e per il \hyperref[3.39]{Corollario 3.39}:

```

$\begin{aligned} & \exists \varphi_1, \dots, \varphi_n : E \rightarrow K \quad \text{e} \\ & \forall \text{ con } \varphi_i|K = id_K \\ & ] \end{aligned}$   
 Sia  $x$  un'indeterminata e consideriamo i polinomi  $\alpha + \beta x$ . Possiamo definire il polinomio:  
 $F(x) = \prod_{i < j} (\varphi_i(\alpha) + x \varphi_i(\beta) - \varphi_j(\alpha) - x \varphi_j(\beta)) \in K[x]$   
\footnote{È come se applicassimo  $\varphi_i$  al polinomio  $\alpha + \beta x$  e poi vi sottraessimo  $\varphi_j$  applicata allo stesso.}  
 $] \quad$   
 con  $\deg F(x) \leq \binom{n}{2}$  e  $F(x) \neq 0$  in quanto se un fattore fosse 0, quindi  
 $\begin{aligned} & \begin{aligned} & \varphi_i(\alpha) + x \varphi_i(\beta) = \varphi_j(\alpha) + x \varphi_j(\beta) \\ & \text{implies } \\ & x(\varphi_i(\beta) - \varphi_j(\beta)) + \varphi_i(\alpha) - \varphi_j(\alpha) = 0 \end{aligned} \\ & \end{aligned}$   
 $\end{aligned}$   
 per il principio di identità dei polinomi avremmo:  
 $\begin{aligned} & \begin{aligned} & \begin{aligned} & \varphi_i(\beta) - \varphi_j(\beta) = 0 \\ & \varphi_i(\alpha) - \varphi_j(\alpha) = 0 \end{aligned} \\ & \end{aligned} \\ & \text{iff } \begin{aligned} & \begin{aligned} & \varphi_i(\beta) = \varphi_j(\beta) \\ & \varphi_i(\alpha) = \varphi_j(\alpha) \end{aligned} \\ & \end{aligned} \\ & \end{aligned}$   
 $] \quad$   
 da cui  $\varphi_i \equiv \varphi_j$  perché  $E = K(\alpha, \beta)$  (se coincidono sui generatori coincidono dappertutto);  
 ma ciò è assurdo, in quanto avevamo assunto  $i < j$  (ricordiamo che le  $\varphi_i$  sono distinte). Dunque il polinomio è non nullo e ha grado limitato.  
 $\newpage$   
 Sappiamo quindi che  $F(x)$  ha un numero finito di radici in  $K$  (al più  $\deg F(x)$ ) e poiché  $K$  è un campo infinito,  
 allora  $\exists t \in K$  tale che  $F(t) \neq 0$ , dunque:  
 $\begin{aligned} & \begin{aligned} & \begin{aligned} & F(t) = \prod_{i < j} (\underbrace{\varphi_i(\alpha) + t \varphi_i(\beta)}_{\varphi_i(\alpha + t \beta)} - \underbrace{\varphi_j(\alpha) - t \varphi_j(\beta)}_{\varphi_j(\alpha + t \beta)}) \neq 0 \\ & \end{aligned} \\ & \end{aligned}$   
 $] \quad$   
 da ciò abbiamo che:  
 $\begin{aligned} & \begin{aligned} & \varphi_i(\alpha + t \beta) \neq \varphi_j(\alpha + t \beta) \quad \text{quindi } \gamma = \alpha + t \beta \text{ ha } n \text{ coniugati, pertanto } [K(\gamma) : K] \\ & = n = [E : K]. \end{aligned} \\ & \end{aligned}$   
 Inoltre  $\gamma \in K(\alpha, \beta) = E$ , quindi  $E = K(\gamma)$ .  
 $\item \underline{\textbf{\$K\$ campo finito}}$

Se  $\faktor{E}{K}$  è finita, allora  $E$  è finito. Essendo  $E^*$  un sottogruppo moltiplicativo finito di  $E$ , è ciclico  
 (per un risultato di [\textcolor{purple}{Aritmetica}](https://github.com/diego-unipi/Appunti-Aritmetica)),  
 ossia  $E^* = \left<\gamma\right> \implies E = K(\gamma).$   
 $\end{itemize}$   
 $\end{proof}$

rr. 5153, 5155, 5158-5160; p. 129

$$L^H = \text{Fix}(H) := \{\alpha \in L \mid \varphi(\alpha) = \alpha, \forall \alpha \in H\} \subseteq L$$

ovvero il sottocampo<sup>50</sup> di  $L$  di tutti gli elementi fissati da tutti i  $K$ -automorfismi del sottogruppo  $H$ . Si osserva che per tale sottocampo si ha che:

$$K \subseteq L^H \subseteq L$$

la seconda inclusione segue immediatamente dalla definizione, la prima deriva dal fatto che essendo i  $K$ -automorfismi in particolare delle immersioni di  $L$  in  $\overline{K}$  via identità (per come è definito il gruppo di Galois), allora almeno tutti gli elementi del campo  $K$  devono essere fissati per definizione.

<sup>50</sup> Andrebbe verificato che è un campo.

usare `\mid`, `typo`, correzioni minori

```
\[ L^H = \text{Fix}(H) := \{ \alpha \in L \mid \varphi(\alpha) = \alpha, \forall \varphi \in H \} \subseteq L
\]
ovvero il sottocampo\footnote{Il fatto che  $L^H$  sia un campo deriva dalle proprietà di omomorfismo di  $\varphi$  di  $L$  degli elementi fissati da tutti i  $K$ -automorfismi del sottogruppo  $H$ . Si osserva che per tale sottocampo si ha che:
\[ K \subseteq L^H \subseteq L
\]
la seconda inclusione segue immediatamente dalla definizione, la prima deriva dal fatto che essendo i  $K$ -automorfismi in particolare delle immersioni di  $L$  in  $K$  via identità (per come è definito il gruppo di Galois), allora gli elementi del campo  $K$  vengono fissati per definizione.}
```

**Lemma 3.67** (Il campo fissato è quello base  $\iff$  fissiamo rispetto a tutto il gruppo di Galois)

Sia  $L/M$  un'estensione di Galois e  $H < \text{Gal}(L/M)$ , allora:

$$M = L^H \iff H = \text{Gal}(L/M)$$

*Dimostrazione.* Dimostriamo separatamente le due implicazioni:

- Supponiamo che  $G = \text{Gal}(L/M)$  e dimostriamo che  $L^G = M$ . Se  $M \subsetneq L^G$ , allora  $[L^G : M] > 1$ , quindi:

$$\exists \varphi : L^G \longrightarrow \overline{M} \quad \text{con} \quad \varphi|_M = id_M$$

con  $\varphi \neq id$  in quanto il grado è maggiore di 1, per cui non c'è solo l'identità tra le immersioni; a questo punto sappiamo dalla [Proposizione 3.39](#) che l'immersione si può estendere ad un campo più grande, dunque sia:

$$\tilde{\varphi} : L \longrightarrow \overline{M} \quad \text{con} \quad \tilde{\varphi}|_{L^G} = \varphi$$

## riscritture e aggiunte varie

```
\begin{lemma}[Il campo fissato è quello base$\iff$fissiamo rispetto a tutto il gruppo di Galois]
```

```
\label{3.67}
```

```
Sia $faktor{L}{M}$ un'estensione di Galois e $H <
```

```
\text{Gal}\left(faktor{L}{M}\right)$, allora:
```

```
\[ M = L^H \iff H = \text{Gal}\left(faktor{L}{M}\right)
```

```
\]
```

```
o equivalentemente
```

```
\[ L^{faktor{L}{M}} = M \quad \text{e} \quad
```

```
\text{Gal}\left(L^{faktor{L}{H}}\right) = H
```

```
\]
```

```
\end{lemma}
```

```
\begin{proof}
```

Sia  $G = \text{Gal}(L/M)$ . Dimostriamo separatamente le due implicazioni:

```
\begin{itemize}
```

\item Dimostriamo che  $L^G = M$ . Se  $M \subsetneq L^G$ , allora  $[L^G : M] > 1$ , quindi:

```
\[ \exists \varphi : L^G \longrightarrow M \quad \text{con} \quad \varphi|_M = id_M
```

con  $\varphi$  in quanto il grado è maggiore di 1, per cui non c'è solo l'identità tra le immersioni;

a questo punto sappiamo dalla [Proposizione 3.39](#) che l'immersione si può estendere ad un campo più grande, dunque sia:

$$\begin{aligned} \exists \tilde{\varphi} : L &\rightarrow M \quad \text{con} \\ \tilde{\varphi}|_{L^G} &= \varphi \end{aligned}$$

rr. 5182-5191, 5194, 5197-5201; p. 129-130

dove  $\tilde{\varphi}|_M = \varphi|_M = id$ . D'altra parte abbiamo per ipotesi che  $L/M$  è normale, dunque  $\tilde{\varphi}(L) = L$ , quindi:  $\tilde{\varphi} \in \text{Gal}(L/M)$  (perché è un automorfismo che fissa puntualmente  $L$  e si restringe all'identità su  $M$ ), da ciò abbiamo che  $\tilde{\varphi}$  fissa puntualmente  $L^G$ , che è assurdo perché avevamo supposto il grado dell'estensione maggiore di 1 (quindi con un elemento non fissato da  $\tilde{\varphi}$ ).

- Essendo  $L/M$  un'estensione finita, per il [Teorema dell'elemento primitivo](#)  $L = M(\alpha)$ , sia  $H \leq G$  e consideriamo:

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \quad \text{con} \quad \deg f(x) = |H|$$

si ha  $f(x) \in L^H[x]$ , poiché, se consideriamo  $\rho \in H$ , allora si ha:

$$\rho f(x) = \prod_{\sigma \in H} (x - \rho(\sigma(\alpha))) = \prod_{\sigma \in H} (x - \sigma(\alpha)) = f(x)$$

dove l'ultima uguaglianza deriva dal fatto che anche  $\rho$  è un elemento di  $H$ , e dunque l'unica cosa che fa è permutare gli elementi dell'insieme stesso. Se  $H = G$  abbiamo  $|G| = [L : M] = [M(\alpha) : M] = \deg \mu_{\alpha/M}(x) \geq \deg f(x) = |H|$ , in quanto  $f(x) \in L^M[x] = M[x]$  per ipotesi e  $f(\alpha) = 0$ , da cui  $\mu_{\alpha/M}(x) \mid f(x)$  e quindi la tesi  $H = G$ .

riscritture e aggiunte varie

[continua ...]

dove  $\widetilde{\varphi}_M = \varphi_M = id_M$ . D'altra parte abbiamo per ipotesi che  $\text{faktor}(L|M)$  è normale,

dunque  $\widetilde{\varphi}(L) = L$ , quindi  $\widetilde{\varphi} \in \text{Gal}(\text{faktor}(L|M)) = G$

(perché è un automorfismo che manda  $L$  in sé stesso e si restringe all'identità su  $M$ ). \\

Da ciò abbiamo che  $\widetilde{\varphi}$  fissa puntualmente  $L^G$  (per definizione di  $\text{Fix}(G)$ ),

che è assurdo perché avevamo supposto il grado dell'estensione maggiore di 1 (quindi con almeno un elemento non fissato da  $\widetilde{\varphi}$ ).

\item Sia  $M = L^H$  e dimostriamo  $H = G = \text{Gal}(\text{faktor}(L|M))$ .

Essendo  $\text{faktor}(L|M)$  un'estensione finita,  $\text{faktor}(L|M)$  è di Galois ma noi consideriamo solo estensioni di Galois finite.}

per il \hyperref[prim]{Teorema dell'elemento primitivo}  $L = M(\alpha)$ .

Consideriamo:

\[ f(x) = \prod\_{\sigma \in H} (x - \sigma(\alpha)) \quad \text{con} \quad \deg f(x) = |H| \]

Si ha che  $f(x) \in L^H[x]$ , poiché, se consideriamo  $\rho \in H$ , allora si ha:

\[ \rho f(x) = \prod\_{\sigma \in H} (x - \rho(\sigma(\alpha))) = \prod\_{\sigma \in H} (x - \sigma(\alpha)) = f(x) \]

dove l'uguaglianza deriva dal fatto che anche  $\rho$  è un elemento di  $H$ , e dunque l'unica cosa che fa è permutare gli elementi dell'insieme stesso.

Dato che  $f(x) \in L^H[x] = M[x]$  (per ipotesi) e  $f(\alpha) = 0$ , si ha che  $\mu_\alpha(x) \mid f(x)$ , da cui:

\[ |\text{faktor}(L|M)| = [L : M] = [M(\alpha) : M] = \deg \mu\_\alpha(x) \leq \deg f(x) = |H| \]

e dato che per ipotesi  $H < G$ , si ha la tesi.

\end{itemize}  
\end{proof}

---

**Lemma 3.68**

Data l'estensione  $L/K$  di Galois  $H < \text{Gal}(L/K)$ , sia  $\sigma \in \text{Gal}(L/K)$ , allora:

$$L^{\sigma H \sigma^{-1}} = \sigma(L^H)$$

*Dimostrazione.* Ricordando che  $L^H = \{\alpha \in L \mid \varphi(\alpha) = \alpha, \forall \varphi \in H\}$ , abbiamo che:

$$\sigma(L^H) = \{\sigma(\alpha) \mid \alpha \in L^H\} = \underbrace{\{\sigma(\alpha) \mid}_{=\beta} \varphi(\alpha) = \alpha, \forall \varphi \in H\}$$

da cui:

$$\begin{aligned} \sigma(L^H) &= \{\beta \in L \mid (\varphi \circ \sigma^{-1})(\beta) = \sigma^{-1}(\beta), \forall \varphi \in H\} = \\ &= \{\beta \in L \mid (\sigma \circ \varphi \circ \sigma^{-1})(\beta) = \beta, \forall \varphi \in H\} = L^{\sigma H \sigma^{-1}} \end{aligned}$$

correzioni minori, usare  $\mid$

Data l'estensione  $L/K$  di Galois siano  $H < \text{Gal}(L/K)$  e  $\sigma \in \text{Gal}(L/K)$ , allora:

```
\begin{proof}
Ricordando che  $L^H = \{\alpha \in L \mid \varphi(\alpha) = \alpha, \forall \varphi \in H\}$ , abbiamo che:

$$\sigma(L^H) = \{\sigma(\alpha) \mid \alpha \in L^H\} =$$


$$\{\underbrace{\sigma(\alpha)}_{=\beta} \mid \varphi(\alpha) = \alpha, \forall \varphi \in H\}$$

da cui:
\begin{multline*}
\sigma(L^H) = \{\beta \in L \mid (\varphi \circ \sigma^{-1})(\beta) = \sigma^{-1}(\beta), \forall \varphi \in H\} = \\
= \{\beta \in L \mid (\sigma \circ \varphi \circ \sigma^{-1})(\beta) = \beta, \forall \varphi \in H\} = L^{\sigma H \sigma^{-1}}
\end{multline*}
\end{proof}
```

**Teorema 3.70 (Teorema di Corrispondenza di Galois)**

Data l'estensione di Galois (finita)  $L/K$  c'è una corrispondenza biunivoca tra l'insieme delle sottoestensioni di  $L/K$  e l'insieme dei sottogruppi di  $\text{Gal}(L/K)$ . Inoltre  $H \triangleleft G$  se e solo se  $L^H/K$  è normale, ed in tal caso abbiamo:

$$\text{Gal}(L^H/K) \cong \frac{\text{Gal}(L/K)}{\text{Gal}(L/L^H)} = G/H$$

*Dimostrazione.* Detto  $\mathcal{E}_{L/K} = \{F | K \subseteq F \subseteq L\}$  l'insieme delle sottoestensioni di  $L/K$  e  $\mathcal{G}_{L/K} = \{H < \text{Gal}(L/K)\}$  l'insieme dei sottogruppi del gruppo di Galois dell'estensione, allora essi sono in bigezione:

$$\mathcal{E}_{L/K} \longleftrightarrow \mathcal{G}_{L/K}$$

mediante le applicazioni:

$$\alpha : \mathcal{E}_{L/K} \longrightarrow \mathcal{G}_{L/K} : F \longmapsto \text{Gal}(L/F)^{51}$$

---

<sup>51</sup>Per la precisione, avendo assunto che estensione normale e di Galois siano la stessa cosa e che  $L/K$  sia di Galois, allora  $L/F$  è di Galois, mentre non è detto che  $F/K$  lo sia, per la [Proposizione 3.50](#), ed essendo di Galois ciò ci permette di usare la corrispondenza scritta sopra.

**riscrittura e aggiunte varie**

```
\begin{theorem}
    [Teorema di Corrispondenza di Galois]
    \label{corrG}

    Data l'estensione di Galois (finita) $\faktor{L}{K}$ c'è una corrispondenza
    biunivoca tra l'insieme delle sottoestensioni di $\faktor{L}{K}$ e l'insieme dei
    sottogruppi di $G = \text{Gal}(\faktor{L}{K})$. \\

    Inoltre $H \triangleleft G$ se e solo se $\faktor{L^H}{K}$ è normale, ed in tal
    caso abbiamo:
    \[ \text{Gal}(\faktor{L^H}{K}) \cong \faktor{G}{H} \]

\end{theorem}

\begin{proof}
    Detto $\mathcal{E}_{L/K} = \{F \mid K \subseteq F \subseteq L\}$ l'insieme
    delle sottoestensioni di $\faktor{L}{K}$ e
    $\mathcal{G}_{L/K} = \left\{ H < \text{Gal}(\faktor{L}{K}) \right\}$ l'insieme dei sottogruppi del gruppo di
    Galois dell'estensione,
```

```

allora essi sono in biogezione:
\begin{array}{l}
\mathcal{E}_{L/K} \longrightarrow \mathcal{G}_{L/K} \\
\end{array}
mediante le applicazioni:
\begin{array}{l}
\alpha : \mathcal{E}_{L/K} \longmapsto \mathcal{G}_{L/K} : F \longmapsto \\
\text{\footnotesize Gal}(\mathcal{F}) \\
\end{array}
\text{Per la precisione, avendo assunto che estensione normale e di Galois siano la stessa cosa e che } \mathcal{F} \text{ sia di Galois,} \\
\text{allora } \mathcal{F} \text{ è di Galois (mentre non è detto che } \mathcal{G} \text{ lo sia) per la \hyperref[3.50]{Proposizione 3.50},} \\
\text{quindi è ben definito } \text{\footnotesize Gal}(\mathcal{F}). \\
\end{array}

```

---

rr. 5264-5265, 5268-5269, 5272, 5275-5276; p. 131

Si osserva che essendo  $L^H$  un campo e  $K \subseteq L^H \subseteq L$  per definizione, allora  $\beta$  è ben definita; osserviamo anche che si ha:

$$\text{Gal}\left(L/F\right) < \text{Gal}\left(L/K\right)$$

perché un automorfismo di  $F$  che fissa puntualmente  $F$ , ovviamente fissa puntualmente anche il suo sottoinsieme  $K$ , dunque l'immagine via  $\alpha$  di  $F$  sta in  $\mathcal{G}$ , pertanto  $\alpha$  è ben definita. Verifichiamo ora che  $\alpha$  e  $\beta$  descrivono una biogezone tra  $\mathcal{E}_{L/K}$  e  $\mathcal{G}_{L/K}$ , mostriamo che sono una l'inversa dell'altra:

$$\beta \circ \alpha(F) = \beta\left(\text{Gal}\left(L/F\right)\right) = L^{\text{Gal}(L/F)} = F \quad \forall F \in \mathcal{E}_{F/K}$$

dove l'ultima uguaglianza è garantita dal Lemma 3.67, in quanto stiamo considerando il campo fissato da tutto il gruppo di Galois  $\text{Gal}\left(L/F\right)$ . Viceversa:

$$\alpha \circ \beta(H) = \alpha(L^H) = \text{Gal}\left(L/L^H\right) = H \quad \forall H \in \mathcal{G}_{F/K}$$

infatti,  $H < \text{Gal}\left(L/L^H\right)$  in quanto tutti gli elementi di  $L^H$  sono fissati dagli elementi di  $H$  per definizione e quindi  $H \subseteq \text{Gal}\left(L/L^H\right)$ ; d'altra parte  $\text{Gal}\left(L/L^H\right) \subseteq H$ , perché, detto  $L^H = M$ , abbiamo  $H \subseteq \text{Gal}\left(L/M\right)$  e  $L^H = M$ , dunque per il Lemma 3.67 segue che  $H = \text{Gal}\left(L/L^H\right)$ .

riscrittura e aggiunte varie

Si osserva che essendo  $L^H$  un campo e  $K \subsetneq L^H \subsetneq L$  per definizione, allora  $\beta$  è ben definita.

Osserviamo anche che si ha:

$$\begin{aligned} & [\operatorname{Gal}\left(\operatorname{faktor}\{L\}{F}\right) \subset \operatorname{Gal}\left(\operatorname{faktor}\{L\}{K}\right) \\ & ] \end{aligned}$$

perché un automorfismo di  $L$  che fissa puntualmente  $F$ , ovviamente fissa puntualmente anche il suo sottoinsieme  $K$ , pertanto anche  $\alpha$  è ben definita.  
 $\backslash\backslash$

Verifichiamo ora che  $\alpha$  e  $\beta$  descrivono una biiezione tra  $\mathcal{E}_{L/K}$  e  $\mathcal{G}_{L/K}$ , mostrando che sono una l'inversa dell'altra:

$$\begin{aligned} & [\beta \circ \alpha(F) = \beta\left(\operatorname{Gal}\left(\operatorname{faktor}\{L\}{F}\right)\right) = \\ & L^{\operatorname{Gal}\left(\operatorname{faktor}\{L\}{F}\right)} = F \quad \text{quindi } \forall F \in \mathcal{E}_{F/K} \\ & ] \end{aligned}$$

dove l'ultima uguaglianza è garantita dal \hyperref[3.67]{Lemma 3.67}. Viceversa:

$$\begin{aligned} & [\alpha \circ \beta(H) = \alpha(L^H) = \operatorname{Gal}\left(\operatorname{faktor}\{L\}{L^H}\right) = \\ & H \quad \text{quindi } \forall H \in \mathcal{G}_{F/K} \\ & ] \end{aligned}$$

sempre per il \hyperref[3.67]{Lemma 3.67}.  $\backslash\backslash$   
 $\backslash\newpage$

rr. 5257-5278, 5282-5284, 5286, 5291-5292, 5294-5296; p. 132

Verifichiamo ora la seconda parte del teorema; sappiamo che  $H \triangleleft \operatorname{Gal}\left(\frac{L}{K}\right) \iff gHg^{-1} = H, \forall \sigma \in \operatorname{Gal}\left(\frac{L}{K}\right)$  e per il Lemma 3.68 abbiamo che:

$$\sigma(L^H) = L^{\sigma H \sigma^{-1}} = L^H \quad \forall \sigma \in \operatorname{Gal}\left(\frac{L}{K}\right)$$

e ciò è equivalente al dire che  $\frac{L^H}{K}$  è normale, perché,  $\forall \psi : L^H \hookrightarrow \overline{K}$ , con  $\psi|_K = id_K$ , si ha che  $\psi(L^H) = L^H$ , poiché ogni  $\psi$  si estende a  $L$  e quindi:

$$\forall \varphi \in \operatorname{Gal}\left(\frac{L}{K}\right), \exists \sigma \in \operatorname{Gal}\left(\frac{L}{K}\right) : \sigma|_{L^H} = \psi$$

Infine, resta da verificare che  $\operatorname{Gal}\left(\frac{L^H}{K}\right) \cong \frac{G}{H}$ , consideriamo l'omomorfismo di restrizione:

$$\Gamma : \operatorname{Gal}\left(\frac{L}{K}\right) \longrightarrow \operatorname{Gal}\left(\frac{L^H}{K}\right) : \varphi \mapsto \varphi|_{L^H}$$

esso è ovviamente surgettivo perché ogni  $\psi \in \operatorname{Gal}\left(\frac{L^H}{K}\right)$  si estende ad  $L$ , ed inoltre:

$$\begin{aligned} \ker \Gamma &= \left\{ \varphi \in \operatorname{Gal}\left(\frac{L}{K}\right) \mid \varphi|_{L^H} = id \right\} = \left\{ \varphi \in \operatorname{Gal}\left(\frac{L}{K}\right) \mid \varphi(\alpha) = \alpha, \forall \alpha \in L^H \right\} = \\ &= \operatorname{Gal}\left(\frac{L}{L^H}\right) \cong H \end{aligned}$$

## riscrittura e aggiunte varie

```
Verifichiamo ora la seconda parte del teorema. \\

Sappiamo che  $H \triangleleft \text{Gal}(\text{faktor}(L\{K\})) \iff \sigma H \sigma^{-1} = H$ ,  $\forall \sigma \in \text{Gal}(\text{faktor}(L\{K\}))$  e per il \hyperref\[3.68\]{Lemma 3.68} abbiamo che:

$$\begin{aligned} & [\ \sigma(L^H) = L^{\{\sigma H \sigma^{-1}\}} = L^H \quad \forall \sigma \in \text{Gal}(\text{faktor}(L\{K\})) \\ & ] \end{aligned}$$

Ciò è equivalente a dire che  $\text{faktor}(L^H\{K\})$  è normale, perché  $\forall \psi : L^H \varlonghookrightarrow \text{Gal}(K)$  con  $\psi|_K = \text{id}_K$ , si ha che  $\psi(L^H) = L^H$ , in quanto ogni  $\psi$  si estende a  $L$  e quindi:

$$\begin{aligned} & [\ \forall \psi \in \text{Gal}(\text{faktor}(L^H\{K\})) \quad \exists \sigma \in \text{Gal}(\text{faktor}(L\{K\})) : \sigma|_{L^H} = \psi \\ & ] \end{aligned}$$

Infine, resta da verificare che  $\text{Gal}(\text{faktor}(L^H\{K\})) \cong \text{faktor}(G\{H\})$ . Consideriamo l'omomorfismo di restrizione:

$$\begin{aligned} & [\ \Gamma : \text{Gal}(\text{faktor}(L\{K\})) \twoheadrightarrow \text{Gal}(\text{faktor}(L^H\{K\})) : \varphi \mapsto \varphi|_{L^H} \\ & ] \end{aligned}$$

esso è ovviamente surgettivo perché ogni  $\psi \in \text{Gal}(\text{faktor}(L^H\{K\}))$  si estende ad  $L$ , ed inoltre:

$$\begin{aligned} & \begin{aligned} & \ker \Gamma = \left\{ \varphi \in \text{Gal}(\text{faktor}(L\{K\})) \mid \varphi|_{L^H} = \text{id} \right\} = \\ & = \left\{ \varphi \in \text{Gal}(\text{faktor}(L\{K\})) \mid \varphi(\alpha) = \alpha, \forall \alpha \in L^H \right\} = \text{Gal}(\text{faktor}(L\{L^H\})) \end{aligned} \\ & \end{aligned}$$


$$\begin{aligned} & \text{Ma per il } \text{\hyperref[3.67]{Lemma 3.67}}, \text{ Gal}(\text{faktor}(L\{L^H\})) = H, \\ & \text{quindi applicando il primo teorema di omomorfismo} \\ & \begin{aligned} & [\ \text{Gal}(\text{faktor}(L^H\{K\})) \cong \\ & \frac{\text{Gal}(\text{faktor}(L\{K\}))}{\text{Gal}(\text{faktor}(L\{L^H\}))} = \\ & \text{faktor}(G\{H\}) \\ & ] \\ & \end{aligned} \\ & \end{aligned}$$


```

**Osservazione 3.71 —** Il teorema ci dice che, data ad esempio la torre:

$$\begin{array}{c} L \\ | \\ H \\ | \\ L^H \\ | \\ G/H \\ | \\ K \end{array}$$

dove  $G$  è il gruppo di Galois di  $L/K$ . Essendo anche  $L/L^H$  di Galois per ipotesi, e detto  $H$  il suo gruppo di Galois, allora, per il teorema precedente, se  $H \triangleleft G$ , si ha che anche  $L^H/K$  è di Galois ed il suo gruppo di Galois è  $G/H$ .

**Proposizione 3.72** (Proprietà della corrispondenza di Galois)

Dati  $H, S < \text{Gal}(L/K)$ , allora valgono le seguenti:

- (1)  $H \leq S \iff L^H \supset L^S$ .
- (2)  $L^{H \cap S} = L^H L^S$ .<sup>a</sup>
- (3)  $L^{\langle S, H \rangle} = L^H \cap L^S$ .

<sup>a</sup>Intendiamo il composto dei due campi.

## riscrittura, correzioni minori

Data la torre:

dove  $G$  è il gruppo di Galois di  $\text{faktor}\{L\}\{K\}$  e  $H$  è il gruppo di Galois di  $\text{faktor}\{L\}\{L^H\}$ ,

\footnote{\$\text{faktor}\{L\}\{K\}\$ è di Galois per ipotesi e \$\text{faktor}\{L\}\{L^H\}\$ è di Galois per la \hyperref[3.50]{Proposizione 3.50}.}

allora per il teorema precedente, se  $H \triangleleft G$ , si ha che anche  $\text{faktor}\{L^H\}\{K\}$  è di Galois ed il suo gruppo di Galois è  $\text{faktor}\{G\}\{H\}$ .

```
\item $H < S \iff L^H \supset L^S$  

\item $L^{\{H \cap S\}} = L^H L^S$ \footnote{Intendiamo il composto dei due campi.}  

\item $L^{\{\left\langle H, S \right\rangle\}} = L^H \cap L^S$
```

*Dimostrazione.* Dimostriamo le affermazioni:

(1) "Ovvio".

(2) Osserviamo che  $H \cap S \subset H, S$ , dunque  $L^{H \cap S} \supset L^H, L^S$ , per il punto (1); pertanto un campo che contiene entrambi i sottocampi conterrà anche il composto,  $L^{H \cap S} \supset L^H L^S$ . D'altra parte  $L^H L^S \subset L \implies \exists N \leqslant \text{Gal}(L/K)$  tale che  $L^H L^S = L^N$ , per il Teorema di corrispondenza di Galois, inoltre:

$$\text{Gal}(L/L^N) = N \subset \left( \underbrace{\text{Gal}(L/L^H) \cap \text{Gal}(L/L^S)}_{=H \cap S} \right)$$

da cui  $N \subset H \cap S \iff L^N \supset L^{H \cap S}$ .

(3) Abbiamo che  $H \subseteq \langle H, S \rangle$  e  $S \subseteq \langle H, S \rangle$ , da cui  $L^S, L^H \supseteq L^{\langle H, S \rangle}$ , da cui  $L^{\langle H, S \rangle} \subseteq L^H \cap L^S$ .

Viceversa sia  $\alpha \in L^H \cap L^S$ , allora  $\varphi(\alpha) = \alpha, \forall \varphi \in H, S$ , quindi  $\alpha$  è fissato dai generatori del gruppo  $\langle H, S \rangle$ , pertanto  $\alpha$  è fissato da tutti gli elementi di  $\langle H, S \rangle$ , da cui la tesi:

$$L^H \cap L^S \subseteq L^{\langle H, S \rangle}$$

typo, riscritture e aggiunte varie

[continua ...]

```

\begin{proof}
Dimostriamo le affermazioni:
\begin{enumerate}[(1)]
\item Se  $H < S$ , in particolare  $H \subset S$ , quindi  $L^S \subset L^H$  dato che un automorfismo che fissa puntualmente  $S$  a maggior ragione fissa puntualmente  $H$ , che è un suo sottoinsieme. \\
Viceversa se  $L^H \supset L^S$ , allora  $H = \text{Gal}(\text{faktor}(L\{L^H\})) < \text{Gal}(\text{faktor}(L\{L^S\})) = S$  perché un automorfismo che fissa puntualmente  $L^H$  a maggior ragione fissa puntualmente  $L^S$ , che è un suo sottoinsieme.
\item Osserviamo che  $H \cap S \subset H, S$  dunque  $L^{\{H \cap S\}} \supset L^H, L^S$  per il punto (1); pertanto un campo che contiene entrambi i sottocampi conterrà anche il composto,  $L^{\{H \cap S\}} \supset L^H L^S$ . \\
D'altra parte  $L^H L^S \subset L \implies \exists N < \text{Gal}(\text{faktor}(L\{K\}))$  tale che  $L^H L^S = L^N$ , per il \hyperref[corrG]{Teorema di corrispondenza di Galois}. Inoltre  $L^N \supset L^H, L^S \implies N < H, S$  per il punto (1), in particolare  $N \subset H, S \implies N \subset H \cap S$  da cui, sempre per il punto (1),  $L^H L^S = L^N \supset L^{\{H \cap S\}}$ .
\item Abbiamo che  $H, S \subset \langle H, S \rangle$ , quindi per il punto (1)

$$\langle L^{\{\langle H, S \rangle\}} \subset L^H, L^S \implies L^{\{\langle H, S \rangle\}} \subset L^H \cap L^S$$

\]
Viceversa sia  $\alpha \in L^H \cap L^S$ , allora:

$$\forall \varphi(\alpha) = \alpha \quad \forall \varphi \in H \cup S$$

quindi  $\alpha$  è fissato dai generatori del gruppo  $\langle H, S \rangle$ , pertanto  $\alpha$  è fissato da tutti gli elementi di  $\langle H, S \rangle$ , da cui:

$$\langle L^H \cap L^S \subset \langle L^{\{\langle H, S \rangle\}}$$

\]
\end{enumerate}
\end{proof}

```

---

*Nelle versioni più recenti:*

p. 16

**Osservazione 1.35** (Sulla definizione di sottogruppo normale) — I sottogruppi normali possono essere ridefiniti nella maniera seguente,  $H \trianglelefteq G$  se e solo se:

$$H = \bigcup_{h \in H} \mathcal{C}\ell_h$$

cioè un sottogruppo è normale se e solo se è l'unione delle classi di coniugio dei suoi elementi. Infatti:

$$H \trianglelefteq G \iff g h g^{-1} \in H \quad \forall h \in H, \forall g \in G$$

che equivale a:

$$\mathcal{C}\ell_h = \{ghg^{-1} | h \in H\} \subseteq H \quad \forall h \in H \implies \bigcup_{h \in H} \mathcal{C}\ell_h \subseteq H$$

d'altra parte se  $H$  è normale è chiuso per coniugio, ovvero il coniugio di ogni suo elemento è ancora in  $H$  ( $ghg^{-1} = h', \forall h \in H$ ) e in particolare ciò significa che:

$$H \subseteq \bigcup_{h \in H} \mathcal{C}\ell_h$$

hai fatto solo una freccia (l'ultima cosa dice che i coniugati sono in  $H$ , non il viceversa)

**Osservazione 1.86** (Schema della dimostrazione) — Sia:

$$G(p) = \{g \in G \mid \text{ord}(g) = p^k, k \in \mathbb{N}\}$$

$G(p)$  prende il nome di  **$p$ -componente** o componente di  **$p$ -torsione**. Si osserva che:

- $G(p)$  è un sottogruppo di  $G$  perché  $G$  è abeliano, dunque:

$$\text{ord}(xy) \mid [\text{ord}(x), \text{ord}(y)] \quad \forall x, y \in G$$

quindi se  $x$  ed  $y$  hanno per ordine una potenza di  $p$ , anche il prodotto ha per ordine una potenza di  $p$ , quindi  $xy \in G(p)$ , ed essendo  $G$  finito allora  $G(p)$  è un sottogruppo. <sup>a</sup>

- $G(p)$  è un sottogruppo caratteristico di  $G$  (ciò segue dal fatto che gli automorfismi conservano l'ordine degli elementi, e quindi  $G(p)$  viene mandato in  $G(p)$ ).

---

<sup>a</sup>Si osserva che le  $p$ -componenti sono  $p$ -gruppi.

magari sarebbe meglio dimostrarlo

---

**Lemma 1.96**

Sia  $G$  un  $p$ -gruppo e  $H \leq G$ , allora  $H \leq N_G(H)$ .

*Dimostrazione.* Essendo  $G$  un  $p$ -gruppo abbiamo che  $|G| = p^n$ . Procediamo per induzione su  $n$ . Se  $n = 0$  non c'è niente da dimostrare. Se  $n > 0$  consideriamo due casi:

- Se  $Z(G) \not\subseteq H$ , dato che  $H \cup Z(G) \subseteq N_G(H)$ , abbiamo che  $\emptyset \neq Z(G) \setminus H \subseteq N_G(H) \setminus H$  da cui la tesi.
- Se  $Z(G) \subseteq H$  osserviamo che  $Z(G)$  è normale in  $G$  e che  $Z(G)$  non è banale perché  $G$  è un  $p$ -gruppo, dunque possiamo considerare  $G/Z(G)$  di ordine strettamente minore all'ordine di  $G$ . Sia  $\pi : G \rightarrow G/Z(G)$  la mappa di proiezione al quoziente. Per ipotesi induttiva  $N_{G/Z(G)}(H/Z(G))$  contiene strettamente  $H/Z(G)$ , quindi per il teorema di corrispondenza si ha che anche le loro controimmagini tramite  $\pi$  rispettano un contenimento stretto (perché si preservano gli indici). Sempre per corrispondenza  $\pi^{-1}(N_{G/Z(G)}(H/Z(G))) = H$ , quindi basta mostrare che  $\pi^{-1}(N_{G/Z(G)}(H/Z(G))) \subseteq N_G(H)$ , e questo deriva dal fatto che se  $g \in \pi^{-1}(N_{G/Z(G)}(H/Z(G)))$  allora  $gHg^{-1} \subseteq HZ(G) = H$ .<sup>18</sup>

credo che sia sbagliato (anche perché non stai usando l'ipotesi induttiva), dovrebbe essere

$$\begin{aligned} N_{G/Z}(H/Z) &= \left\{ gZ \mid gZ \cdot H/Z \cdot (gZ)^{-1} \in H/Z \right\} \\ &\quad \text{se } gZ \cdot hZ \cdot g^{-1}Z \in H/Z \quad \forall hZ \in H/Z \\ N_G(H) &\not\subseteq Z \quad \text{se } ghg^{-1}Z \in H/Z \quad \forall h \in H \\ &\quad \text{se } ghg^{-1} \in H \\ N_G(H) & \end{aligned}$$

quindi  $\pi_{G/Z(G)}^{-1}(N_{G/Z(G)}(H/Z(G))) = N_G(H)$  e  
 $\pi_{G/Z(G)}^{-1}(H/Z(G)) = H$  e applicando l'ip. ind. si conclude

---

## Esercitazioni

---

r. 128; p. 5

*Dimostrazione.* Osserviamo che un elemento di  $\text{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$  deve necessariamente mandare una base di  $(\mathbb{Z}/p\mathbb{Z})^n$  in un'altra base, e si determina univocamente in questo modo. Sia  $\{v_1, \dots, v_n\}$  una base di  $(\mathbb{Z}/p\mathbb{Z})^n$  e  $\varphi \in \text{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ , consideriamo  $\varphi(v_1)$ :  $\varphi(1)$  può assumere qualsiasi valore non nullo, pertanto abbiamo  $(p^n - 1)$  possibilità per l'immagine del primo vettore. Per quanto riguarda  $v_2$ ,  $\varphi(v_2)$  può assumere qualsiasi valore non nullo che non sia multiplo di  $\varphi(v_1)$ , che sono  $p^n - p$ , analogamente  $\varphi(v_3)$  può assumere qualsiasi valore non nullo che non sia combinazione lineare di  $v_1$  e  $v_2$ , che sono  $p^n - p^2$ , e così via. Reiteriamo questo ragionamento fino a  $\varphi(v_n)$ , che può essere scelto in  $p^n - p^{n-1}$  modi, da cui

typo

$$1 \rightarrow v_1$$

`\text{Aut}((\mathbb{Z}/p\mathbb{Z})^n)`, consideriamo  $\varphi(v_1)$ :  $\varphi(v_1)$  può assumere

### §1.3 Gruppo diedrale

#### §1.3.1 Elementi del gruppo

**Definizione 1.6.** Dato  $n \geq 2$  un numero naturale consideriamo un poligono regolare di  $n$  vertici centrato nell'origine del piano  $\mathbb{R}^2$ , chiamiamo **gruppo diedrale** su  $n$  vertici l'insieme  $D_n$  delle isometrie di  $\mathbb{R}^2$  che fissano il poligono, cioè che mandano i vertici in se stessi (per  $n = 2$  consideriamo le isometrie che mandano un segmento in se stesso).

**Osservazione 1.7 —**  $D_n$  è un gruppo, in quanto l'applicazione identità che fissa tutti i vertici è un'isometria dal poligono in se stesso, la composizione di isometrie è un'isometria e un'isometria ammette sempre un'inversa, che è anch'essa un'isometria.

typo

$$se \rightarrow sé$$

vertici in sé stessi (per  $n = 2$  consideriamo le isometrie che mandano un segmento in sé stesso).

fissa tutti i vertici è un'isometria dal poligono in sé stesso, la

---

**Osservazione 1.17 —** Per  $k \mid n$  e  $0 \leq h < k$ , i sottogruppi  $H_{k,h} = \langle r^k, sr^h \rangle$  e  $H = \langle r^k \rangle \cdot \langle sr^h \rangle$  coincidono. Infatti  $H_{k,h} \subseteq H$  in quanto  $r^k, sr^h$  sono elementi di  $H$ , d'altra parte  $H \subseteq H_{k,h}$  in quanto  $H_{h,k}$  contiene tutti i prodotti finiti delle potenze di  $r^k$  e  $sr^h$ , in particolare gli elementi di  $H$ .

<sup>1</sup>Dati  $H, K$  sottogruppi di un gruppo  $G$ , se vale almeno una delle inclusioni  $H \subseteq N_G(K)$ ,  $K \subseteq N_G(H)$  allora  $HK = KH$ , quindi  $HK$  è un sottogruppo di  $G$ .

<sup>2</sup>Se  $H, K$  sono sottogruppi finiti di un gruppo  $G$  e  $HK \leq G$  allora vale  $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$ .

typo

```
{Dati $H, K$ sottogruppi  
di un gruppo $G$, se vale almeno una delle inclusioni $H \subseteq N_G(K)$,  
$K \subseteq N_G(H)$ allora $HK = KH$, quindi $HK$ è un sottogruppo di $G$}.
```

d'altra parte  $H \subseteq N_G(H_{\{k, h\}})$  in quanto  $H_{\{k, h\}}$  contiene tutti i

**Osservazione 1.22 —**  $\mathcal{R} = \langle r \rangle$  è caratteristico in  $D_n$  per  $n \geq 3$ . Infatti per ogni  $\varphi \in \text{Aut}(D_n)$  allora  $\text{ord}(\varphi) = \text{ord}(\varphi(r))$ , da cui  $|\langle \varphi(r) \rangle| = n$ . Se fosse  $\varphi(r) \notin \mathcal{R}$  avremmo  $\text{ord}(\varphi(r)) = 2$ , quindi  $|\langle \varphi(r) \rangle| = n = 2$ , che è assurdo in quanto  $|D_n| \geq 6$ . Questo non è vero per  $D_2$ , che contiene una rotazione e due simmetrie: poiché  $\text{Aut}(D_2) \cong S_3$  esiste un  $\psi \in \text{Aut}(D_2)$  che manda la rotazione in una riflessione.

riscrittura per chiarezza

```
quindi $|\langle \varphi(r) \rangle| = n = 2$, che è assurdo in quanto $n \geq 3$.
```

r. 495; p. 10

Vediamo quali sono i sottogruppi normali della forma  $\langle r^k, sr^h \rangle$ , consideriamo i coniugi

$$\varphi_s : D_n \longrightarrow D_n : x \longmapsto sx s^{-1} \quad \varphi_r : D_n \longrightarrow D_n : x \longmapsto rxr^{-1}$$

e sia  $x_1^{\pm 1} \dots x_m^{\pm 1} \in H_{k,h} = \langle r^k, sr^h \rangle$ , allora

$$\varphi_s(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_s(x_1)^{\pm 1} \dots \varphi_s(x_m)^{\pm 1} \in \langle srs, r^h s^{-1} \rangle = \langle sr^k s, r^h s^{-1} \rangle = \langle r^k, sr^{-h} \rangle$$

$$\varphi_r(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_r(x_1)^{\pm 1} \dots \varphi_r(x_m)^{\pm 1} \in \langle r^k, rsr^{h-1} \rangle = \langle r^k, sr^{h-2} \rangle$$

riscrittura per chiarezza

```
\[
\varphi_s(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_s(x_1)^{\pm 1} \dots
\varphi_s(x_m)^{\pm 1}
\in \langle \langle sr^k s, r^h s^{-1} \rangle \rangle = \langle sr^k s, r^h s^{-1} \rangle = \langle r^k, sr^{-h} \rangle
\]
```

rr. 789, 792; p. 15

- $\iota$  è iniettiva, infatti

$$\begin{aligned} \ker \iota &= \{(\varphi_1, \varphi_2) \in \text{Aut}(H) \times \text{Aut}(K) \mid \iota(\varphi_1, \varphi_2) = id_{\text{Aut}(H \times K)}\} = \\ &= \{(\varphi_1, \varphi_2) \in \text{Aut}(H) \times \text{Aut}(K) \mid (\varphi_1(g_1), \varphi_2(g_2)) = (e_H, e_K) \forall (g_1, g_2) \in H \times K\} \end{aligned}$$

Poiché gli unici elementi  $\varphi_1 \in \text{Aut}(H)$ ,  $\varphi_2 \in \text{Aut}(K)$  tali che  $\varphi_1(H) = \{e_H\}$  e  $\varphi_2(K) = \{e_K\}$  sono rispettivamente  $id_{\text{Aut}(H)}$ ,  $id_{\text{Aut}(K)}$  abbiamo

$$\ker \iota = \{(id_{\text{Aut}(H)}, id_{\text{Aut}(K)})\} = \{id_{\text{Aut}(H \times K)}\}$$

correzione

```
\item $\iota$ è iniettiva, infatti \begin{multiline*}
\ker \iota = \{(\varphi_1, \varphi_2) \in \text{Aut}(H) \times \text{Aut}(K) \mid
\iota(\varphi_1, \varphi_2) = id_{\text{Aut}(H \times K)}\} = \\
= \{(\varphi_1, \varphi_2) \in \text{Aut}(H) \times \text{Aut}(K) \mid
(\varphi_1 \times \varphi_2)(g_1, g_2) = (\varphi_1(g_1), \varphi_2(g_2)) = \\
(g_1, g_2) \forall (g_1, g_2) \in H \times K\}
\end{multiline*} Poiché gli unici elementi $\varphi_1 \in \text{Aut}(H)$,
$\varphi_2 \in \text{Aut}(K)$ tali che $\varphi_1(g_1) = g_1 \forall g_1 \in H$ e
$\varphi_2(g_2) = g_2 \forall g_2 \in K$
```

rr. 875, 877; p. 16-17

*Dimostrazione.* Posti  $n = |H|$ ,  $m = |K|$ , consideriamo l'insieme

$$S = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^n = (e_H, e_K)\}$$

Osserviamo che  $H \times \{e_K\} = S$ , infatti  $H \times \{e_K\} \subseteq S$  in quanto tutti gli elementi di  $H \times e_K$  hanno ordine che divide  $n$ . D'altra parte dato  $(g_1, g_2) \in S$ , se  $\text{ord}(g_1, g_2) \mid n$  allora  $\text{ord}(g_1) \mid n$  e  $\text{ord}(g_2) \mid n$ , ma  $\text{ord}(g_2) \mid m$  per il Teorema di Lagrange, quindi

$\text{ord}(g_2) = 1$  e  $S \subseteq H \times \{e_K\}$ , da cui l'uguaglianza. Con un ragionamento analogo possiamo caratterizzare  $\{e_H\} \times K$  come

correzione, aggiunta

hanno ordine che divide  $n$ . D'altra parte dato  $(g_1, g_2) \in S$ , si ha

$\text{ord}(g_2) \mid m$  per il Teorema di Lagrange, quindi  $\text{ord}(g_2) = 1$  (cioè  $g_2 = e_K$ ) e

---

**Proposizione 1.35**

Dato un gruppo  $G$ , valgono i seguenti fatti:

- (1)  $G'$  è un sottogruppo caratteristico di  $G$ ;
- (2)  $G/G'$  è un gruppo abeliano;
- (3) dato  $A$  un gruppo abeliano e  $\varphi \in \text{Hom}(G, A)$ , allora  $G' \subseteq \ker \varphi$ .

*Dimostrazione.* Mostriamo le affermazioni singolarmente:

- (1) consideriamo  $\varphi \in \text{Aut}(G)$ , poiché  $\varphi$  preserva la struttura di gruppo è sufficiente descrivere come  $\varphi$  agisce sui generatori di  $G'$  per determinare  $\varphi(G')$ . Fissati  $x, y \in G$  abbiamo

$$\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} \in G'$$

pertanto  $\varphi(G') \subseteq G'$ , da cui l'uguaglianza in quanto  $\varphi$  è bigettiva;

- (2) dati  $x, y \in G$ ,  $xG' \cdot yG' = yG' \cdot xG'$  se e solo se  $xyG' = yxG'$ , che è equivalente a richiedere  $xyx^{-1}y^{-1} \in G'$ . Dato che effettivamente  $xyx^{-1}y^{-1} = [x, y]$  è un elemento di  $G'$  abbiamo che  $G/G'$  è abeliano;

aggiunte, riscrittura (forse sono equivalenti)

\item \$G'\$ è un sottogruppo caratteristico di \$G\$ (in particolare \$G' \trianglelefteq G\$);

```
\[
\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}
\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)] \in G'
]pertanto $\varphi(G') \subseteq G'$, da cui l'uguaglianza in quanto
```

```
\item dati $x, y \in G$, $xG' \cdot yG' = yG' \cdot xG'$ se e solo se
$xyG' = yxG'$, che è equivalente a richiedere $x^{-1}y^{-1}xy \in G'$.
Dato che effettivamente $x^{-1}y^{-1}xy = [x^{-1}, y^{-1}]$ è un elemento
di $G'$
abbiamo che $\faktor{G}{G'}$ è abeliano;
```

- (2) un elemento  $g \in G$  con tali proprietà non può essere contenuto nello stabilizzatore di nessun elemento di  $X$ , cioè cerchiamo  $g \in G$  tale che

$$g \in \bigcap_{x \in X} (\text{St}(x))^c$$

che è equivalente a

$$g \notin \bigcup_{x \in X} \text{St}(x) = \bigcup_{h \in G} h \text{St}(x_0) h^{-1}$$

per il fatto precedente, fissato  $x_0 \in G$ . Osserviamo che  $\text{St}(x_0) \neq G$ , infatti se fosse  $\text{St}(x_0) = G$  avremmo

### rimozione, riscrittura

```
\item un elemento $g$ \in $G$ con tali proprietà non può essere contenuto  
nello stabilizzatore di nessun elemento di $X$, cioè cerchiamo $g$ \in $G$  
tale che  
\[  
g \notin \bigcup_{x \in X} \text{St}(x) = \bigcup_{h \in G} h \text{St}(x_0) h^{-1}  
\] per il fatto precedente, dove $x_0$ è un elemento fissato di $G$.  
Osserviamo che
```

osserviamo che  $|X| = |G|^{p-1}$ , possiamo infatti scegliere liberamente i primi  $p-1$  elementi di ogni  $p$ -upla, che ne determinano l'ultimo in modo univoco (per unicità dell'inverso). Definiamo un'azione di  $\mathbb{Z}/p\mathbb{Z}$  su  $X$  nel seguente modo:

$$\psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow S(X) : a \longmapsto \psi_a$$

con

$$\psi_a : X \longrightarrow X : (g_1, \dots, g_p) \longmapsto (g_{1+a}, \dots, g_p, g_1, \dots, g_a)$$

### typo

$$g \rightarrow a$$

```
\[  
 \psi_a : X \longmapsto (g_1, \dots, g_p) \mapsto (g_{1+a}, \dots, g_p, g_1, \dots, g_a)  
\]
```

rr. 1190, 1200; p. 23

Poiché  $H \cong \mathbb{Z}/5\mathbb{Z}$ , abbiamo  $\text{Aut}(H) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$ , d'altra parte  $|\text{Im}\varphi|$  divide  $(|G|, |H|) = 1$ , pertanto  $|\text{Im}\varphi| = 1$  e l'omomorfismo è banale, cioè  $H \subseteq Z(G)$ . Diamo adesso due modi per concludere l'esercizio:

- (1) osserviamo che se  $G$  è un gruppo abeliano, cioè se  $Z(G) = G$ , allora abbiamo che  $G$  è ciclico. Infatti posto  $k \in G$  un elemento di ordine 3 (che esiste in virtù del [Teorema di Cauchy](#)), abbiamo che  $\text{ord}(hk) = \text{ord}(h)\text{ord}(k) = 15$  in quanto i due elementi hanno ordine coprimo. D'altra parte, se  $G$  non fosse abeliano allora avremmo necessariamente  $Z(G) = H$ , quindi  $G/Z(G)$  sarebbe ciclico in quanto di ordine 3, pertanto  $G$  sarebbe un gruppo abeliano, da cui la tesi per quanto appena detto;

typo

$$H \rightarrow \text{Aut}(H)$$

(nel secondo siamo nel caso non abeliano)

Poiché  $H \cong \mathbb{Z}/5\mathbb{Z}$ , abbiamo  $|\text{Aut}(H)| \cong (\mathbb{Z}/5)^* \cong \mathbb{Z}/4\mathbb{Z}$ , d'altra parte  $|\text{Im}\varphi|$  divide  $(|G|, |\text{Aut}(H)|) = 1$ , pertanto

necessariamente  $Z(G) = H$ , quindi  $\text{faktor}\{G\}{Z(G)}$  sarebbe ciclico in quanto di ordine 3, pertanto  $G$  sarebbe un gruppo abeliano, che è assurdo;

$$\pi_{\mathcal{A}_{2d}} : G \longrightarrow S_{2d}/\mathcal{A}_{2d} \cong \mathbb{Z}/2\mathbb{Z}$$

possiamo caratterizzare  $\varphi^{-1}(\mathcal{A}_{2d})$  come

$$\varphi^{-1}(\mathcal{A}_{2d}) = \{g \in G \mid \varphi(g) \in \mathcal{A}_{2d}\} = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$$

pertanto  $\varphi^{-1}(\mathcal{A}_{2d}) \trianglelefteq G$ . Per il Primo Teorema di Omomorfismo abbiamo che esiste un omomorfismo iniettivo da  $G/\ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$  in  $\mathbb{Z}/2\mathbb{Z}$ , da cui  $[G : \ker(\pi_{\mathcal{A}_{2d}})] \leq 2$ . Tale sottogruppo ha indice 1 se e solo se  $G = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$ , cioè  $\varphi(G) \subseteq \mathcal{A}_{2d}$ , mostriamo che in effetti esiste un elemento di  $G$  la cui immagine tramite  $\varphi$  è una permutazione dispari. Consideriamo  $g \in G$  un elemento di ordine 2, poiché  $\varphi$  è un omomorfismo iniettivo abbiamo che  $\text{ord}(\varphi(g)) = \text{ord}(g) = 2$ , pertanto la permutazione  $\varphi(g)$  ha una decomposizione in  $d$  2-cicli, cioè è dispari. Pertanto  $G \neq \varphi^{-1}(\mathcal{A}_{2d})$ , da cui  $[G : \varphi^{-1}(\mathcal{A}_{2d})] = 2$ ,  $\square$

typo, aggiunte

```
\[
\pi_{\mathcal{A}_{2d}} \circ \varphi : G \longrightarrow
\mathbb{Z}/2\mathbb{Z}
\]
```

$\mathbb{Z}/2\mathbb{Z}$ , da cui  $[G : \ker(\pi_{\mathcal{A}_{2d}})] \leq 2$ . Tale sottogruppo ha indice 1 se e solo se  $G = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi) = \varphi^{-1}(\mathcal{A}_{2d})$ , cioè  $\varphi(G) \subseteq \mathcal{A}_{2d}$  ( $\varphi$ , e quindi  $\pi_{\mathcal{A}_{2d}}$ ) in generale non sono surgettive). Mostriamo che in effetti esiste un elemento di  $G$  la cui immagine tramite  $\varphi$  è una permutazione

r. 1594; p. 29

### §1.7.3 Classi di coniugio in $\mathcal{A}_n$

Studiamo le classi di coniugio in  $\mathcal{A}_n$ . In particolare, fissato  $\sigma \in \mathcal{A}_n$ , vogliamo determinare una relazione tra  $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$  e  $\mathcal{C}\ell_{S_n}(\sigma)$ . Poiché valgono  $|\mathcal{A}_n| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| \cdot |Z_{\mathcal{A}_n(\sigma)}|$  e  $Z_{\mathcal{A}_n}(\sigma) = Z_{S_n}(\sigma) \cap \mathcal{A}_n$ , abbiamo

typo

Poiché valgono  $|\mathcal{A}_n| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| \cdot |Z_{\mathcal{A}_n(\sigma)}|$

Più precisamente, abbiamo  $\mathcal{C}\ell_{S_n}(\sigma) = \mathcal{C}\ell_{A_n}(\sigma) \cup \mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})$  per ogni  $\tau$  permutazione dispari. Infatti  $\mathcal{C}\ell_{A_n}(\sigma) \cup \mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1}) \subseteq \mathcal{C}\ell_{S_n}(\sigma)$  (i coniugati di  $\tau\sigma\tau^{-1}$  sono anche coniugati di  $\sigma$ ), d'altra parte per ogni  $\rho \in S_n$  abbiamo  $\rho\sigma\rho^{-1} \in \mathcal{C}\ell_{A_n}(\sigma)$  se  $\rho$  è pari,  $\rho\sigma\rho^{-1} = (\rho\tau^{-1})(\tau\sigma\tau^{-1})(\rho\tau^{-1})^{-1} \in \mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})$  se  $\rho$  è dispari, da cui l'uguaglianza. Abbiamo altri due casi:

- $|\mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{S_n}(\tau\sigma\tau^{-1})|$ ;
- $|\mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})| = \frac{1}{2}|\mathcal{C}\ell_{S_n}(\tau\sigma\tau^{-1})|$ .

Tuttavia se fosse  $|\mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{S_n}(\tau\sigma\tau^{-1})|$  avremmo  $\mathcal{C}\ell_{A_n}(\sigma) = \mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})$ , che è assurdo in quanto  $\tau\sigma\tau^{-1} \notin \mathcal{C}\ell_{A_n}(\sigma)$ , pertanto

typo, aggiunta

$$\tau \rightarrow \tau^{-1}$$

`\in \mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})$ se $\rho$ è dispari, da cui  
l'uguaglianza.`

Tuttavia se fosse  $|\mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{S_n}(\tau\sigma\tau^{-1})|$ ,  
dato che  $\mathcal{C}\ell_{S_n}(\tau\sigma\tau^{-1}) = \mathcal{C}\ell_{S_n}(\sigma) = \mathcal{C}\ell_{A_n}(\sigma) \cup \mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})$ ,  
avremmo  $\mathcal{C}\ell_{A_n}(\sigma) = \mathcal{C}\ell_{A_n}(\tau\sigma\tau^{-1})$ ,

r. 1794; p. 32

In generale, un sottogruppo è normale se e solo se è unione disgiunta delle classi di coniugio dei suoi elementi, quindi la cardinalità di  $N \trianglelefteq A_5$  deve essere somma di alcuni termini nella seconda colonna, compreso 1. D'altra parte  $|N| \mid A_5 = 60$ , da cui  $|N| = 1$  oppure  $|N| = 60$ . Pertanto  $A_5$  è semplice.  $\square$

typo

termini nella seconda colonna, compreso 1. D'altra parte  $|N| \mid |A_5| = 60$ ,

- se  $k = 1$  abbiamo  $l = n + 1$ , cioè  $\sigma$  è un  $n+1$ -ciclo. Scriviamo  $\sigma = (a_1 \dots a_l)$  e consideriamo la permutazione pari  $\tau = (a_1 a_2)(a_3 a_4)$ , poiché  $N$  è normale in  $A_{n+1}$  contiene

$$\tau\sigma\tau^{-1} = (a_2 a_1 a_4 a_3 a_5 a_6 \dots a_l)$$

Consideriamo  $\rho = (\tau\sigma\tau^{-1})\sigma \in N$ , notiamo che  $\rho \neq id$  in quanto

$$\rho(a_4) = (\tau\sigma\tau^{-1})(\sigma(a_4)) = (\tau\sigma\tau^{-1})(a_5) = a_6 \neq a_4$$

d'altra parte  $a_1$  è un punto fisso per  $\rho$ , che è assurdo;

- se  $k > 1$  e  $l > 2$ , poiché  $\sigma_1^{-1}$  è un  $l$ -ciclo disgiunto da  $\sigma_2, \dots, \sigma_k$  la permutazione  $\rho = \sigma_1^{-1}\sigma_2 \dots \sigma_k$  è un elemento di  $N$ . Consideriamo  $\alpha = \rho\sigma \in N$ , osserviamo che

typo

(aggiunte delle parentesi per chiarezza)

$$\sigma^{-1} \rightarrow \sigma_1^{-1}$$

\item se  $k = 1$ abbiamo $l = n + 1$, cioè $\sigma$ è un $(n + 1)$-ciclo.$

$\rho = \sigma_1^{-1}\sigma_2 \dots \sigma_k$  è un elemento di  $N$ .

r. 1972; p. 35

*Dimostrazione.* Sia  $\sigma \in Z(S_n) \setminus \{id\}$ , allora esistono distinti  $x, y \in \{1, \dots, n\}$  tali che  $\sigma(x) = y$ . Fissiamo  $z \in \{1, \dots, n\} \setminus \{x, y\}$  e consideriamo la permutazione  $\tau = (y z)$ , abbiamo

$$(\tau\sigma)(x) = z \quad (\sigma\tau)(x) = y$$

che è assurdo in quanto  $y \neq z$ . Pertanto  $Z(S_n) = \{id\}$ .  $\square$

riscrittura

$$\begin{aligned} & \text{\textbackslash [} \\ & \quad z = (\tau\sigma)(x) = (\sigma\tau)(x) = y \\ & \text{\textbackslash ]} \end{aligned}$$

*Dimostrazione.* Sia  $N$  un sottogruppo normale di  $S_n$ , consideriamo  $K = N \cap \mathcal{A}_n$ .  $K$  è normale in  $\mathcal{A}_n$ , pertanto  $K = \{id\}$  oppure  $K = \mathcal{A}_n$ , distinguiamo 2 casi:

- se  $K = \mathcal{A}_n$  allora  $\mathcal{A}_n \leq N$ : per il Teorema di Corrispondenza i sottogruppi di  $S_n$  contenenti  $\mathcal{A}_n$  sono in biiezione con i sottogruppi di  $S_n/\mathcal{A}_n \cong \mathbb{Z}/2\mathbb{Z}$ , pertanto  $N = \mathcal{A}_n$  oppure  $N = S_n$ ;
- se  $K = \{id\}$ , poiché  $[S_n : \mathcal{A}_n] = 2$  per la [Proposizione 1.49](#) vale  $[N : K] \in \{1, 2\}$ , da cui  $|N| \leq 2$ . Se  $|N| = 1$  allora  $N = \{id\}$ , se  $|N| = 2$  consideriamo l'azione di coniugio di  $S_n$  su  $N$

$$\varphi : N_{S_n}(N) \longrightarrow \text{Aut}(N) : g \longmapsto \varphi_g$$

dove  $\varphi_g$  è la mappa

$$\varphi_g : H \longrightarrow H : h \longmapsto ghg^{-1}$$

il nucleo di  $\varphi$  coincide con  $Z_{S_n}(N)$ . Per il Primo Teorema di Omomorfismo allora abbiamo un omomorfismo iniettivo

$$\psi : \frac{N_{S_n}(N)}{Z_{S_n}(N)} \hookrightarrow \text{Aut}(N)$$

Poiché  $|N| = 2$  abbiamo  $N \cong \mathbb{Z}/2\mathbb{Z}$ , pertanto  $\text{Aut}(N) = \{id\}$ . Dato che  $N_{S_n}(N) = S_n$  per la normalità di  $N$  questo implica che sia  $Z_{S_n}(N) = S_n$ , cioè che  $N \subseteq Z(S_n)$ , ma questo è assurdo in quanto  $Z(S_n) = \{id\}$  per il [Lemma 1.65](#).

## typo, aggiunte varie

$$H \rightarrow N$$

Dato che  $K$  è normale in  $\mathcal{A}_n$ , per semplicità  $K = \{id\}$  oppure  $K = \mathcal{A}_n$ ,

consideriamo l'azione di coniugio di  $S_n$  su  $N$ , ristretta a  $\varphi$ :  
 $N_{S_n}(N)$

$$\varphi_g : N \longrightarrow N : h \longmapsto ghg^{-1}$$

Dato che  $N_{S_n}(N) = S_n$  per la normalità di  $N$ , questo implica che  $Z_{S_n}(N) = S_n$ , cioè che  $N \subseteq Z(S_n)$ , ma questo è assurdo

**Osservazione 1.67 —** L'enunciato è vero anche per  $n = 3$  con la stessa dimostrazione, infatti  $A_3 \cong \mathbb{Z}/3\mathbb{Z}$  è un gruppo semplice, ed è vero anche per  $n = 4$  anche se con una dimostrazione diversa. Infatti un sottogruppo  $H$  di indice 2 di  $S_n$  contiene necessariamente il commutatore, in quanto  $S_n/H \cong \mathbb{Z}/2\mathbb{Z}$ , d'altra parte il commutatore di  $S_n$  è  $A_n$ , pertanto  $H = A_4$ .

correzione (per  $n=4$  è falso, c'è il Klein; qui hai solo dimostrato che  $A_4$  è l'unico sottogruppo di indice 2, non l'unico normale)

```
\begin{remark}
L'enunciato è vero anche per $n = 3$ con la stessa dimostrazione, infatti
$\mathcal{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ è un gruppo semplice.
Per $n = 4$, $\mathcal{A}_4$ non è semplice: contiene il gruppo di Klein
\[
V = \{ \text{id}, \text{cycle}\{1,2\}\text{cycle}\{3,4\}, \text{cycle}\{1,3\}\text{cycle}\{2,4\},
\text{cycle}\{1,4\}\text{cycle}\{2,3\} \}
\]
che è normale in $\mathcal{A}_4$ e anche in $S_4$.
I sottogruppi normali di $S_4$ sono quindi $\{\text{id}\}$, $V$, $\mathcal{A}_4$ e
$S_4$.
\end{remark}
```

r. 2061; p. 36

in particolare  $\ker \varphi \neq S_n$ . Poiché  $\ker \varphi \trianglelefteq S_n$  allora il nucleo di  $\varphi$  è banale oppure è  $A_n$ . D'altra parte se fosse  $\ker \varphi = A_n$  avremmo  $|\text{Im } \varphi| = 2$ , pertanto l'orbita di ogni elemento di  $S_n/H$  contiene al più due elementi, ma questo è assurdo in quanto per la transitività di  $\varphi$  si ha  $\text{Orb}(\rho H) = S_n/H$  per ogni  $\rho \in S_n$ , che contiene almeno 5 elementi. Pertanto  $\ker \varphi = \{\text{id}\}$ , cioè  $\varphi$  è un omomorfismo iniettivo e in particolare un isomorfismo. Notiamo che  $H$  è lo stabilizzatore della classe  $H$ , infatti

$$\text{St}(H) = \{\sigma \in S_n \mid \sigma H = H\} = \{\sigma \in H\} = H$$

aggiunta

per questa dimostrazione mi ero segnato [Va spiegato meglio]

```
\[
\text{St}(H) = \{\sigma \in S_n \mid \sigma H = H\} = \{\sigma \in S_n \mid
\sigma \in H\} = H
\]
```

---

r. 2221; p. 38

$$(1 \ 2 \ 3)((1 \ 2)(3 \ 4))(1 \ 3 \ 2) = (1 \ 4)(2 \ 3)$$

$$(1 \ 2 \ 3)((1 \ 3)(2 \ 4))(1 \ 3 \ 2) = (1 \ 2)(3 \ 4)$$

$$(1 \ 2)((1 \ 2)(3 \ 4))(1 \ 2) = (1 \ 2)(3 \ 4)$$

$$(1 \ 2)((1 \ 3)(2 \ 4))(1 \ 2) = (1 \ 4)(1 \ 3)$$

Pertanto  $\varphi((1 \ 2 \ 3)) = f$  e  $\varphi((1 \ 2)) = g$ , dove  $f$  e  $g$  sono gli automorfismi di  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  tali che

$$f : (1, 0) \mapsto (1, 1), (0, 1) \mapsto (1, 0)$$

$$g : (1, 0) \mapsto (1, 0), (0, 1) \mapsto (1, 1)$$

---

typo

$$1 \rightarrow 2$$

```
\[
\text{cycle}\{1, 2\}(\text{cycle}\{1, 3\}\text{cycle}\{2, 4\})\text{cycle}\{1, 2\} = \text{cycle}\{1, 4\}\text{cycle}\{2, 3\}
\]
```

---

### §1.8.2 Automorfismi di $D_n$

Consideriamo il gruppo

$$G = \{f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \mid \exists a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z} \text{ per cui } f(x) = ax + b \ \forall x \in \mathbb{Z}/n\mathbb{Z}\}$$

delle sostituzioni lineari in  $\mathbb{Z}/n\mathbb{Z}$ , effettivamente  $G$  è un gruppo con l'operazione di composizione. Infatti fissati  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ ,  $b \in \mathbb{Z}/n\mathbb{Z}$  e  $f \in G$  tali che  $f(x) = ax + b$ , abbiamo che  $f^{-1}$  è tale che  $f^{-1}(x) = a^{-1}(x - b)$  (chiaramente  $G$  contiene l'applicazione nulla ed è chiuso per composizione). Notiamo che un elemento di  $G$  è univocamente determinato dalla coppia  $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$ <sup>10</sup>, pertanto  $G$  contiene  $n\phi(n)$  elementi. In realtà possiamo essere più precisi:

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|} = |N| \cdot |H| = n\phi(n) = |G|$$

Mostriamo quindi che  $N$  è un sottogruppo normale di  $G$ : fissati  $f \in N$  e  $g \in H$  tali che  $f(x) = x + t$  e  $g(x) = ax + b$ , con  $b, t \in \mathbb{Z}/n\mathbb{Z}$  e  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ , abbiamo

$$(g^{-1} \circ f \circ g)(x) = (g^{-1} \circ f)(ax + b) = g^{-1}(ax + b + t) = x + a^{-1}t$$

#### Proposizione 1.72

Il gruppo  $G$  delle sostituzioni lineari in  $\mathbb{Z}/n\mathbb{Z}$  è isomorfo a  $\text{Aut}(D_n)$  per  $n \geq 3$ .

typo

sostituzioni lineari → trasformazioni affini

$$H \rightarrow G$$

delle trasformazioni affini di  $\mathbb{Z}_n$ , effettivamente  $G$  è un gruppo con

e  $g \in G$  tali che  $f(x) = x + t$  e  $g(x) = ax + b$ , con  $b, t \in \mathbb{Z}_n$  e

Il gruppo  $G$  delle trasformazioni affini di  $\mathbb{Z}_n$  è isomorfo a  $\text{Aut}(D_n)$

r. 2357; p. 40

- $N \cap H = \{Id\}$  in quanto  $M = \lambda Id \in N \cap H$  è tale che  $\det M = \lambda^3 = 1$ , cioè  $\lambda = 1$  e quindi  $M = Id$ ;
- $H$  è un sottogruppo normale di  $GL_3(\mathbb{R})$ , in quanto tutti i suoi elementi sono multipli scalari della matrice identità e quindi commutano con gli elementi di  $GL_3(\mathbb{R})$ ;
- $GL_3(\mathbb{R}) = NH$ , infatti per ogni  $M \in GL_3(\mathbb{R})$  possiamo scrivere  $M = S(\lambda Id)$ , dove  $\lambda = (\det M)^{\frac{1}{3}}$  e  $S = (\det M)^{-\frac{1}{3}}M \in N$ .

typo

*mutlipli* → *multipli*

\item \$H\$ è un sottogruppo normale di \$GL\_3(\mathbb{R})\$, in quanto tutti i suoi elementi sono multipli scalari della matrice identità e quindi commutano con gli elementi di \$GL\_3(\mathbb{R})\$;

---

rr. 2442, 2450; p. 41

con  $(g_1 g_2^{-1}, e) \in N$  e  $(g_2, g_2) \in H$ , pertanto possiamo scrivere  $G = N \rtimes_{\varphi} H$ , dove  $\varphi$  è un omomorfismo

$$\varphi : H \longrightarrow \text{Aut}(N)$$

Tale  $\varphi$  è banale se e solo se  $\varphi(h) = id$  per ogni  $h \in H$ , se e solo se  $hn h^{-1} = n$  per ogni  $h \in H$ , per ogni  $n \in N$ . Questo è equivalente a richiedere

$$(g, g)(n, e)(g^{-1}, g^{-1}) = (gng^{-1}, e) = (n, e) \quad \forall g \in G, \forall n \in N$$

typo, correzione

con \$(g\_1 g\_2^{-1}, e) \in N\$ e \$(g\_2, g\_2) \in H\$, pertanto possiamo scrivere \$G \times\_{\varphi} H\$, dove \$\varphi\$ è un omomorfismo

$$\begin{aligned} & \forall [ \\ & \quad (g, g)(g', e)(g'^{-1}, g'^{-1}) = (gg'g'^{-1}, e) = (g', e) \sim \forall g, g' \in G \\ & \forall ] \end{aligned}$$

---

*Dimostrazione.* Dimostriamo la contronominale, cioè che se  $X_1$  e  $X_2$  sono isomorfi allora  $\ker \varphi_1 \cong \ker \varphi_2$ .

Sia  $f : X_1 \longrightarrow X_2$  un isomorfismo, poniamo  $\mathcal{G}_1 = G \rtimes_{\varphi_1} \{e_H\}$ ,  $\mathcal{G}_2 = G \rtimes_{\varphi_2} \{e_H\}$ ,  $\mathcal{H}_1 = \{e_G\} \rtimes_{\varphi_1} H$ ,  $\mathcal{H}_2 = \{e_G\} \rtimes_{\varphi_2} H$ . Osserviamo che  $f(\mathcal{G}_1) = \mathcal{G}_2$  in quanto  $\mathcal{G}_1$  è l'unico  $p$ -Sylow di  $X_1$  e  $\mathcal{G}_2$  è l'unico  $p$ -Sylow di  $X_2$  (infatti  $\mathcal{G}_1 \trianglelefteq X_1$  e  $\mathcal{G}_2 \trianglelefteq X_2$ ), mentre  $f(\mathcal{H}_1)$  è un  $q$ -Sylow di  $X_2$  coniugato a  $\mathcal{H}_2$ . In particolare esiste  $\psi \in \text{Inn}(X_2)$  tale che

typo

Sia  $f: X_1 \longrightarrow X_2$  un isomorfismo, poniamo  $\mathcal{G}_1 = G \rtimes_{\varphi_1} \{e_H\}$ ,  $\mathcal{G}_2 = G \rtimes_{\varphi_2} \{e_H\}$ ,  $\mathcal{H}_1 = \{e_G\} \rtimes_{\varphi_1} H$ ,  $\mathcal{H}_2 = \{e_G\} \rtimes_{\varphi_2} H$ .

---

rr. 2615-2627; p. 44

aggiunta (ho scritto un programma per testare gli altri casi e ho verificato quali metodi funzionano, se vuoi aggiungere per curiosità)

- $A_5$  è un gruppo semplice di ordine 60.

Ci riduciamo quindi a studiare i gruppi di ordine 56, 60, 72, 80, 96.

```
\item $\mathcal{A}_5$ è un gruppo semplice di ordine $60$.  
\end{itemize}
```

Dopo queste osservazioni rimangono i gruppi di cardinalità 12, 20, 24, 28, 36, 40, 44, 45, 48, 52, 56, 60, 63, 68, 72, 75, 76, 80, 84, 88, 92, 96, 99, 100.

Sia  $|G|=n$ , si può verificare che:

```
\begin{itemize}
```

• per  $n \in \{20, 28, \mathbf{40}, 44, 45, 52, \mathbf{63}, 68, 75, 76, \mathbf{84}, \mathbf{88}, 92, 99, 100\}$   $G$  ha un Sylow normale, applicando direttamente il quarto teorema di Sylow;

• per  $n \in \{12, 24, 36, 48, \mathbf{56}, 80, 96\}$   $G$  ha almeno uno dei due Sylow normale, infatti se entrambi i Sylow fossero non normali si avrebbe che il numero di elementi in essi contenuti supererebbe la cardinalità del gruppo;

• per  $n \in \{12, 24, 28, 36, 44, 48, 52, 68, 75, 76, 92, 96, 100\}$   $G$  contiene un sottogruppo normale proprio, per applicazione del teorema di Poincaré (osservazione 1.51) usando come sottogruppo un Sylow;

• per  $n \in \{12, 24, 36, 48, \mathbf{72}, 80, 96\}$   $G$  contiene un sottogruppo normale proprio, il nucleo dell'azione sull'insieme  $X$  dei  $p$ -Sylow ( $p$  dipende da  $n$ ), infatti questo non può essere tutto  $G$  (perché l'azione è transitiva) e non è banale (si dimostra caso per caso ragionando sulle cardinalità di  $G$  e  $S(X)$ );

• per  $n \in \{12, 20, 24, 28, 36, 44, 45, 48, 52, 68, 75, 76, 80, 92, 96, 99, 100\}$   $G$  contiene un sottogruppo normale proprio, il nucleo dell'azione sull'insieme  $G/P$  delle classi laterali di  $P$  un  $p$ -Sylow ( $p$  dipende da  $n$ ), per lo stesso motivo del punto precedente.

```
\end{itemize}
```

Fun fact: in grassetto le cardinalità che si possono escludere con uno solo dei metodi illustrati.

Nota: per Poincaré e l'azione su  $G/P$  non c'è bisogno di applicare il teorema di Sylow (e quindi andare a risolvere i sistemi) ma basta guardare la fattorizzazione in fattori primi di  $n$ .

In ogni caso solo col teorema di Sylow si possono già escludere tutte le cardinalità tranne 60 e 72.

Ci riduciamo quindi a studiare i gruppi di ordine 56, 60, 72, 80, 96.

il nucleo di  $\Phi$  è

$$\begin{aligned}\ker \Phi &= \{g \in S \mid gPg^{-1} = P \ \forall P \in X\} = \\ &= \{g \in S \mid g \in N_S(P) \ \forall P \in X\} = \\ &= \bigcap_{P \in X} N_S(P) = \bigcap_{P \in X} PZ(S) = Z(S)\end{aligned}$$

dove l'ultima uguaglianza è giustificata dal fatto che i 3-Sylow di  $S$  si intersecano banalmente. Per il Primo Teorema di Omomorfismo otteniamo che  $\text{Im } \Phi \cong S/Z(S)$ , che ha cardinalità 12. D'altra parte  $A_4$  è l'unico sottogruppo di  $S_4$  con 12 elementi, pertanto  $S/Z(S) \cong A_4$ , sfruttiamo questo fatto per studiare i 2-Sylow di  $S$ . Per il Teorema di Corrispondenza i sottogruppi di  $S$  contenenti  $Z(S)$  sono in biiezione con i sottogruppi di  $A_4$ , e tale biiezione preserva l'indice e la normalità dei sottogruppi. Poiché  $V_4$  è l'unico 2-Sylow di  $A_4$  abbiamo che  $S$  contiene un unico 2-Sylow di indice 3, cioè di cardinalità 8, chiamiamo  $J$  tale sottogruppo.  $J$  contiene le matrici

formattazione, spazi, typo

$$S_4 \rightarrow A_4$$

```
begin{align*}
\ker\Phi &= \{g \in S \mid gPg^{-1} = P \quad \forall P \in X\} = \\
&= \{g \in S \mid g \in N_S(P) \quad \forall P \in X\} = \\
&= \bigcap_{P \in X} N_S(P) = \bigcap_{P \in X} PZ(S) = Z(S)
\end{align*}
```

$V_4$  è l'unico 2-Sylow di  $A_4$  abbiamo che  $S$  contiene un unico 2-Sylow

rr. 3058-3059; p. 50

*Dimostrazione.* Posto  $I_i = (x - a_i)$  per  $i \in \{1, \dots, n\}$ , osserviamo che  $I_i + I_j = \mathbb{Q}[x]$  per  $i \neq j$ , infatti  $a_i - a_j \in I_i + I_j$ , che è un elemento invertibile di  $\mathbb{Q}[x]$ . Per il Teorema Cinese del Resto abbiamo quindi

$$\frac{\mathbb{Q}[x]}{I_1 \dots I_n} \cong \mathbb{Q}[x] / I_1 \times \dots \times \mathbb{Q}[x] / I_n$$

aggiunta, riscrittura

Posto  $I_i = (x - a_i)$  per  $i \in \{1, \dots, n\}$ , osserviamo che  $I_i + I_j = (1) = \mathbb{Q}[x]$  per  $i \neq j$ , infatti  $a_i - a_j \in I_i + I_j$  ed è un elemento non nullo ( $a_i \neq a_j$ ), quindi è invertibile in  $\mathbb{Q}[x]$  ( $(\mathbb{Q}[x])^* = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ ). Per il Teorema Cinese del Resto

---

rr. 3113-3116; p. 51

Per quanto già visto, sappiamo che  $S^{-1}\mathbb{Z}$  è un anello contenente un unico ideale massimale, detto anche **anello locale**. Più precisamente, tale ideale è  $S^{-1}\mathbb{Z} \setminus (S^{-1}\mathbb{Z})^*$  e il gruppo degli elementi invertibili è

$$(S^{-1}\mathbb{Z})^* = \left\{ \frac{a}{s} \mid a, s \in S \right\}$$

ci sarebbe da spiegare perché (nel caso generale non è così)

---

r. 3136; p. 51

$$S^{-1}(m) = S^{-1}(n) \iff \exists u \in (S^{-1}\mathbb{Z})^* \text{ tale che } m = un \iff u = \frac{m}{n} \in (S^{-1}\mathbb{Z})^*$$

dove l'ultima uguaglianza è giustificata dal fatto che  $S^{-1}\mathbb{Z}$  è un sottoanello di  $\mathbb{Q}$ , pertanto esiste  $\frac{m}{n}$  come numero razionale ed è l'unico valore per cui l'equazione è verificata. D'altra parte abbiamo

correzione

dove l'ultima equivalenza è giustificata dal fatto che  $S^{-1}\mathbb{Z}$  è un

---

### §2.3 Ideali massimali e primi di $\mathbb{Z}[x]$

#### Lemma 2.3

Se  $A \subseteq R$  sono due anelli e  $P \subseteq R$  è un ideale primo di  $R$  allora  $P \cap A$  è un ideale primo di  $A$ .

*Dimostrazione.*  $P \cap A$  è un ideale di  $A$  in quanto controimmagine di  $P$  tramite l'omomorfismo di anelli

$$\varphi : A \longrightarrow R : a \longmapsto a$$

Poiché  $P$  è un ideale primo di  $R$ , per ogni  $a, b \in A$  tali che  $ab \in P \cap A$  si ha  $a \in P$  oppure  $b \in P$ , cioè  $a \in P \cap A$  oppure  $b \in P \cap A$ , quindi  $P \cap A$  è un ideale primo di  $A$ .  $\square$

Consideriamo  $P \subseteq \mathbb{Z}[x]$  un ideale primo, studiamo l'intersezione  $P \cap \mathbb{Z}$ . Questo è un ideale primo di  $\mathbb{Z}$  per il Lemma 2.3, pertanto  $P \cap \mathbb{Z} = (0)$  oppure esiste un primo  $p \in \mathbb{Z}$  tale che  $P \cap \mathbb{Z} = (p)$ . Se non è l'ideale nullo allora  $(p)\mathbb{Z}[x]$  è un ideale contenuto in  $P$ , per il Teorema di Corrispondenza gli ideali primi di  $\mathbb{Z}[x]$  contenenti  $(p)\mathbb{Z}[x]$  sono in biiezione con gli ideali primi del quoziente  $\mathbb{Z}[x]/(p)\mathbb{Z}[x] \cong \mathbb{F}_p[x]$  e vale la stessa cosa per gli ideali massimali. Poiché  $\mathbb{F}_p[x]$  è un dominio a ideali principali, i suoi ideali primi sono  $(\bar{0})$  e quelli generati da un polinomio irriducibile, in particolare tutti i suoi ideali primi non nulli sono anche massimali. Pertanto se  $\overline{f(x)} \in \mathbb{F}_p[x]$  è un polinomio irriducibile allora  $(\overline{f(x)})$  è un ideale primo di  $\mathbb{F}_p[x]$  e quindi  $(p, f(x))$  è un ideale primo e massimale di  $\mathbb{Z}[x]$ . Abbiamo quindi che l'insieme degli ideali massimali di  $\mathbb{Z}[x]$  contenenti  $p$  è

#### riscrittura e aggiunte varie

Se  $A \subseteq R$  sono due anelli e  $P \subseteq R$  è un ideale primo di  $R$  allora  $P \cap A$  è un ideale primo di  $A$  (cioè restrizioni di ideali primi a sottoanelli sono ideali primi).

$(p)\mathbb{Z}[x]$  è un ideale contenuto in  $P$ , ma per il Teorema di

Poiché  $\mathbb{F}_p[x]$  è un PID, i suoi ideali primi sono  $(\overline{0})$  e quelli massimali,

cioè generati da un polinomio irriducibile.

Pertanto se  $\overline{f(x)} \in \mathbb{F}_p[x]$  è un polinomio irriducibile, allora  $(\overline{f(x)})$  è un ideale massimale di  $\mathbb{F}_p[x]$  e, per corrispondenza,  $(p, f(x))$  è un ideale massimale (quindi primo) di  $\mathbb{Z}[x]$ .

Abbiamo quindi che l'insieme degli ideali massimali di  $\mathbb{Z}[x]$  contenenti  $p$  è

Supponiamo adesso che  $P$  sia un ideale primo di  $\mathbb{Z}[x]$  tale che  $P \cap \mathbb{Z} = \{0\}$ .  $S = \mathbb{Z} \setminus \{0\}$  è una parte moltiplicativa di  $\mathbb{Z}$  e l'ipotesi appena data su  $P$  può essere espressa come  $P \cap S = \emptyset$ . Consideriamo la bigezione

$$\{\text{Ideali primi di } S^{-1}\mathbb{Z}[x]\} \longleftrightarrow \{\text{Ideali primi } P \subseteq \mathbb{Z}[x] \mid P \cap S = \emptyset\} : \mathfrak{P} \longmapsto \mathfrak{P} \cap \mathbb{Z}[x]$$

poiché  $S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$  abbiamo che  $P$  corrisponde a un unico ideale primo di  $\mathbb{Q}[x]$ . Essendo  $\mathbb{Q}[x]$  un dominio a ideali principali, questi sono l'ideale nullo e gli ideali generati da polinomi irriducibili. Se  $f(x) \in \mathbb{Q}[x]$  è un polinomio irriducibile il cui ideale corrisponde a  $P$  allora, posto  $m$  il minimo comune denominatore dei suoi coefficienti, abbiamo che  $P = (f(x))\mathbb{Q}[x] \cap \mathbb{Z}[x] = (mf(x))\mathbb{Q}[x] \cap \mathbb{Z}[x] = (mf(x))\mathbb{Z}[x]$ . In particolare  $P$  è generato da un polinomio primitivo irriducibile. Gli ideali primi di  $\mathbb{Z}[x]$  possono quindi avere la seguente forma:

**typo, riscritture e aggiunte varie**

$$0 \rightarrow \{0\}$$

$\$P \cap \mathbb{Z} = \{0\}$ .  $\$S = \mathbb{Z} \setminus \{0\}$  è una parte moltiplicativa di

poiché  $(S^{-1}\mathbb{Z})[x] = \mathbb{Q}[x]$  abbiamo che  $P$  corrisponde a un unico ideale primo di  $\mathbb{Q}[x]$ . Essendo  $\mathbb{Q}[x]$  un PID, questi sono

Mostriamo che gli ideali primi di quest'ultimo tipo non sono massimali.  
 Siano  $f(x) \in \mathbb{Z}[x]$  un polinomio primitivo, irriducibile, non costante,  $a \in \mathbb{Z}$  tale che  $f(a) \notin \{-1, 0, 1\}$ ,  $p \in \mathbb{Z}$  un primo che divide  $f(a)$  e consideriamo le applicazioni

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]/(p)\mathbb{Z}[x] : g(x) \longmapsto \overline{g(x)}$$

$$\psi : \mathbb{Z}[x]/(p)\mathbb{Z}[x] \longrightarrow \mathbb{F}_p : \overline{g(x)} \longmapsto g(a)$$

Osserviamo che  $(\psi \circ \varphi)(f(x)) = \overline{a} \equiv 0 \pmod{p}$  e che  $(\psi \circ \varphi)(p) = p \equiv 0 \pmod{p}$ , pertanto  $p, f(x) \in \ker \psi \circ \varphi$  e quindi  $(p, f(x)) \subseteq \ker(\psi \circ \varphi) \neq \mathbb{Z}[x]$ . Abbiamo quindi  $(f(x)) \subseteq (p, f(x))$ , se  $(f(x))$  fosse massimale allora conterrebbe  $p$ , che è assurdo in quanto  $\deg f \geq 1$ .

Poiché gli ideali di questo tipo non sono massimali, gli ideali massimali di  $\mathbb{Z}[x]$  sono tutti e soli quelli della forma

$$(p, f(x)) \text{ con } \overline{f(x)} \text{ irriducibile in } \mathbb{F}_p[x]$$

typo, riscritture e aggiunte varie

$$a \rightarrow f(a)$$

Siano  $f(x) \in \mathbb{Z}[x]$  un polinomio primitivo, irriducibile (quindi non costante),

Osserviamo che  $(\psi \circ \varphi)(f(x)) = f(a) \equiv 0 \pmod{p}$  e che

conterrebbe  $p$ , cioè  $f(x) \mid p$ , che è assurdo in quanto  $\deg f \geq 1$ .

Da riguardare, questa dimostrazione non mi convince (non importa che  $A[x]$  sia UFD, io avrei bisogno di  $(A/p)[x]$  UFD)

**Corollario 2.6**

Siano  $A$  un PID e  $B$  un dominio di integrità e  $\varphi : A \rightarrow B$  un omomorfismo di anelli surgettivo, allora  $\varphi$  è un isomorfismo oppure  $B$  è un campo.

*Dimostrazione.* Notiamo che  $\ker \varphi$  è un ideale primo di  $A$  in quanto  $A/\ker \varphi \cong B$  è un dominion di integrità. Se  $\ker \varphi = (0)$ , allora  $\varphi$  è un isomorfismo di anelli. Altrimenti  $\ker \varphi$  è un ideale massimale, pertanto  $A/\ker \varphi \cong B$  è un campo.  $\square$

**Corollario 2.7**

Se  $C$  è un anello tale che  $C[x]$  è un PID, allora  $C$  è un campo.

*Dimostrazione.* Dall'inclusione  $C \subseteq C[x]$  abbiamo che  $C$  è un dominio di integrità. L'ideale  $(x)$  è quindi primo in  $C[x]$  in quanto  $C[x]/(x) \cong X$  è un dominio, quindi è massimale dato che  $C[x]$  è un PID. Pertanto  $C$  è un campo.  $\square$

typo, aggiunta

*dominion*  $\rightarrow$  *dominio*

$X \rightarrow C$

$\backslash \text{cong} B \backslash$  è un dominio di integrità. Se  $\backslash \ker \varphi = (0)$ , allora

L'ideale  $(x)$  è quindi primo non nullo in  $C[x]$  in quanto  $\backslash \text{faktor}\{C[x]\}\{(x)\}$   
 $\backslash \text{cong} C \backslash$

r. 3355; p. 56

**§2.6 Operazioni tra ideali**

Ricordiamo che in un anello commutativo con identità  $A$ , sono ben definite le seguenti operazioni su due ideali  $I, J$  e danno luogo a un terzo ideale (possibilmente uguale a uno dei due):

riscrittura

le seguenti operazioni su due ideali  $I, J$  e danno luogo a un ideale:

$$b^{m+n} = \underbrace{b^m}_{\in I} \cdot \underbrace{b^n}_{\in J} \in I \cap J$$

Pertanto  $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$ . Viceversa, Se  $c \in \sqrt{I \cap J}$  allora esiste  $n \in \mathbb{N}$  tale che  $c^n \in I \cap J$ , in particolare  $c^n \in I$  e  $c^n \in J$ , quindi  $c \in \sqrt{I} \cap \sqrt{J}$ , da cui l'uguaglianza.  $\square$

### Proposizione 2.9

Dato  $A$  un anello commutativo con identità, allora

$$\sqrt{(0)} = \bigcap_{\substack{P \subseteq A \\ P \text{ ideale primo}}} P$$

### riscrittura

```
\[
b^{m+n} = \underset{\in I}{\underbrace{b^m}} \cdot \underset{\in J}{\underbrace{b^n}} \in IJ \subsetneq I \cap J
]
```

```
\[
\sqrt{(0)} = \bigcap_{\substack{P \subseteq A \\ P \text{ ideale primo}}} P
]
```

---

$$\sqrt{I} = \pi^{-1}(\sqrt{(0)}) = \pi^{-1} \left( \bigcap_{\substack{P \subseteq A/I \\ P \text{ ideale primo}}} P \right) = \bigcap_{\substack{P \supseteq I \\ P \subseteq A \text{ ideale primo}}} P$$

□

Grazie a questo risultato, possiamo classificare gli elementi invertibili degli anelli di polinomi.

### Proposizione 2.11

Se  $A$  è un anello commutativo con identità allora

$$A[x]^* = \left\{ p(x) = \sum_{i=0}^n a_i x^i \mid n \in \mathbb{N}, a_0 \in A^*, a_i \in \sqrt{0} \forall i \in \{1, \dots, n\} \right\}$$

riscrittura

magari qui si potrebbe andare a pagina nuova

```
\[
    \sqrt{I} = \pi^{-1}(\sqrt{(0)}) = \pi^{-1} \left( \bigcap_{\substack{P \subseteq A/I \\ P \text{ ideale primo}}} P \right) = \bigcap_{\substack{P \supseteq I \\ P \subseteq A \text{ ideale primo}}} P
\]
\end{proof}

\newpage
```

Grazie a questo risultato, possiamo classificare gli elementi invertibili degli anelli di polinomi.

r. 3513; p. 58

Abbiamo  $\pi(f(x))\pi(g(x)) = \pi(1)$ , cioè  $\pi(f(x))$  è invertibile in  $A/P[x]$ , da cui otteniamo  $\pi(f(x)) \in (A/P)^*$  in quanto  $A/P$  è un dominio di integrità. Allora abbiamo  $a_i \in P$  per ogni  $i \in \{1, \dots, n\}$ , in particolare tali coefficienti sono contenuti nell'intersezione di tutti gli ideali primi di  $A$  per l'arbitrarietà di  $P$ , sono quindi nilpotenti per la [Proposizione 2.9](#). Vale quindi l'inclusione  $A[x]^* \subseteq X$ , da cui l'uguaglianza.  $\square$

riscrittura

Abbiamo  $\pi(f(x))\pi(g(x)) = \pi(1)$ , cioè  $\pi(f(x))$  è invertibile in  $\text{\faktor}{A}{P}[x]$ , da cui otteniamo  $\pi(f(x)) \in (\text{\faktor}{A}{P}[x])^*$  =  $(\text{\faktor}{A}{P})^*$  in quanto  $\text{\faktor}{A}{P}$

rr. 3536, 3540, 3542-3543; p. 58-59

(1) poiché  $I+J+K = A$  esistono  $i \in I, j \in J, k \in K$  tali che  $i+j+k = 1$ . Consideriamo la potenza

$$(i+j+k)^N = \sum_{x+y+z=N} \binom{N}{x,y,z} i^x j^y k^z$$

Se  $N \geq 3n$  osserviamo che  $\max x, y, z \geq n$  per ogni  $x, y, z \in \mathbb{N}$  tali che  $x+y+z = N$ , pertanto scegliendo  $N$  in questo modo abbiamo che  $(x+y+z)^N = 1$  è un elemento di  $I^n + J^n + K^n$ , quindi l'ideale coincide con  $A$ ;

spazi, typo, aggiunta

```
\[
(i + j + k)^N = \sum_{x + y + z = N} \binom{N}{x, y, z} i^x j^y k^z \quad
\footnote{
    Ricordiamo che \displaystyle \binom{N}{x, y, z} =
    \frac{N!}{x! y! z!}.
}
]
```

Se  $N \geq 3n$  osserviamo che  $\max\{x, y, z\} \geq n$  per ogni  $x, y, z \in \mathbb{N}$  tali che  $x+y+z = N$ , pertanto scegliendo  $N$  in questo modo abbiamo che  $(i+j+k)^N = 1$  è un elemento di  $I^n + J^n + K^n$  (perché ogni addendo dello sviluppo appartiene ad almeno uno dei tre), quindi l'ideale coincide con  $A$ ;

r. 3592; p. 60

**Lemma 2.14**

Dato  $p \in \mathbb{Z}$  un primo, se  $p \equiv 3 \pmod{4}$  allora  $p$  è irriducibile in  $\mathbb{Z}[i]$ .

*Dimostrazione.* Supponiamo per assurdo che  $p$  sia irriducibile in  $\mathbb{Z}[i]$ , scriviamo quindi la fattorizzazione

$$p = (a + ib)(c + id)$$

typo

*irriducibile*  $\rightarrow$  *riducibile*

Supponiamo per assurdo che  $p$  sia riducibile in  $\mathbb{Z}[i]$ , scriviamo quindi

---

r. 3660; p. 61

Notiamo che 2 è un elemento dell'ideale  $(x^2 + 1, 1+x)$ , in quanto possiamo scrivere

$$2 = x^2 + 1 - x(x+1) + x + 1$$

Pertanto

$$\frac{\mathbb{Z}[i]}{(i+1)} \cong \frac{\mathbb{Z}[x]}{(2, 1+x)} \cong \frac{\mathbb{Z}[x]/(2)}{(2, 1+x)/(2)} \cong \frac{\mathbb{F}_2[x]}{(1+x)} \cong \mathbb{F}_2$$

riscrittura

$$\begin{aligned} & \backslash[ \\ & 2 = (x^2 + 1) - (x-1)(x+1) \\ & \backslash] \end{aligned}$$

---

Poiché  $a + bi \mid a^2 + b^2$  in  $\mathbb{Z}[i]$ , poiché primo si ha che esiste  $j_0 \in \{1, \dots, k\}$  tale che  $a + bi \mid p_{j_0}$ , distinguiamo tre casi:

- se  $p_{j_0} \equiv 3 \pmod{4}$  allora  $p_{j_0}$  è irriducibile in  $\mathbb{Z}[i]$ , pertanto  $a + bi$  è associato a  $p_{j_0}$ ;
- se  $p_{j_0} \equiv 1 \pmod{4}$  allora si fattorizza in  $\mathbb{Z}[i]$  come

$$p_{j_0} = (c + di)(c - di)$$

con  $c + di, c - di$  primi, quindi irriducibili, di  $\mathbb{Z}[i]$  non associati, pertanto  $a + bi$  è associato a uno dei due;

- se  $p_{j_0} = 2$  allora  $a + bi \mid -i(1+i)^2$ . Poiché  $a + bi$  non è invertibile si ha  $a + bi \mid 1+i$ , cioè  $a + bi$  è associato a  $1+i$ .

aggiunte

Poiché  $a + bi \mid a^2 + b^2$  in  $\mathbb{Z}[i]$ , e dato che  $a + bi$  è primo deve dividere uno dei fattori irriducibili di  $a^2 + b^2$ , cioè esiste  $j_0 \in \{1, \dots, k\}$  tale che  $a + bi \mid p_{j_0}$ , distinguiamo tre casi:

\item se  $p_{j_0} = 2$  allora  $a + bi \mid 2 = -i(1 + i)^2$ . Poiché  $a + bi$

r. 3767; p. 63

### Proposizione 2.19

Sia  $p \in \mathbb{Z}$  un primo dispari:

- (1) se  $p \equiv 3 \pmod{4}$  allora  $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$ ;
- (2) se  $p \equiv 1 \pmod{4}$  e  $p = (a + bi)(a - bi)$  è la sua fattorizzazione in primi di  $\mathbb{Z}[i]$   
allora  $\frac{\mathbb{Z}[i]}{(a + bi)} \cong \mathbb{F}_p$ .

typo

$di \rightarrow in$

fattorizzazione in primi in  $\mathbb{Z}[i]$  allora  $\frac{\mathbb{Z}[i]}{(a + bi)}$

pertanto

$$A/I \cong \frac{A/I^2}{I/I^2}$$

da cui ricaviamo

$$\left| A/I \right| = \left| \frac{A/I^2}{I/I^2} \right| = \left| \frac{A/I^2}{A/I} \right| = \frac{\left| A/I^2 \right|}{\left| A/I \right|}$$

riscrittura

e per il Secondo Teorema di Omomorfismo

---

La cardinalità di questo quoziente è  $N(z)$ , infatti applicando il Lemma 2.21 abbiamo

$$\begin{aligned}
 \left| \frac{\mathbb{Z}[i]}{I} \right| &= \left| \frac{\mathbb{Z}[i]}{(1+i)^e} \right| \cdot \left| \prod_{j=1}^r \frac{\mathbb{Z}[i]}{(a_j + b_j i)^{e_j}} \right| \cdot \left| \prod_{h=1}^s \frac{\mathbb{Z}[i]}{(p)^{e_h}} \right| = \\
 &= \left| \frac{\mathbb{Z}[i]}{(1+i)} \right|^e \cdot \left| \prod_{j=1}^r \frac{\mathbb{Z}[i]}{(a_j + b_j i)} \right|^{e_j} \cdot \left| \prod_{h=1}^s \frac{\mathbb{Z}[i]}{(p)} \right|^{e_h} = \\
 &= N(1+i)^e \prod_{j=1}^r N(a_j + b_j i)^{e_j} \prod_{h=1}^s N(p_h)^{e_h} = \\
 &= N \left( u(1+i)^e \prod_{j=1}^r (a_j + b_j i)^{e_j} \prod_{h=1}^s p_h^{e_h} \right) = N(z)
 \end{aligned}$$

## riscrittura

```

\begin{multiline*}
\left| \frac{\mathbb{Z}[i]}{I} \right| = \left| \frac{\mathbb{Z}[i]}{(1+i)^e} \right| \cdot \left| \prod_{j=1}^r \frac{\mathbb{Z}[i]}{(a_j + b_j i)^{e_j}} \right| \cdot \left| \prod_{h=1}^s \frac{\mathbb{Z}[i]}{(p)^{e_h}} \right| =
= \left| \frac{\mathbb{Z}[i]}{(1+i)} \right|^e \cdot \left| \prod_{j=1}^r \frac{\mathbb{Z}[i]}{(a_j + b_j i)} \right|^{e_j} \cdot \left| \prod_{h=1}^s \frac{\mathbb{Z}[i]}{(p)} \right|^{e_h} =
= N(1+i)^e \prod_{j=1}^r N(a_j + b_j i)^{e_j} \prod_{h=1}^s N(p_h)^{e_h} =
= N(u(1+i)^e \prod_{j=1}^r (a_j + b_j i)^{e_j} \prod_{h=1}^s p_h^{e_h}) =
= N(z)
\end{multiline*}

```

$$\begin{aligned}
 \left| \frac{\mathbb{Z}[i]}{I} \right| &= \left| \frac{\mathbb{Z}[i]}{(1+i)^e} \right| \cdot \left| \prod_{j=1}^r \frac{\mathbb{Z}[i]}{(a_j + b_j i)^{e_j}} \right| \cdot \left| \prod_{h=1}^s \frac{\mathbb{Z}[i]}{(p)^{e_h}} \right| = \\
 &= \left| \frac{\mathbb{Z}[i]}{(1+i)} \right|^e \cdot \prod_{j=1}^r \left| \frac{\mathbb{Z}[i]}{(a_j + b_j i)} \right|^{e_j} \cdot \prod_{h=1}^s \left| \frac{\mathbb{Z}[i]}{(p)} \right|^{e_h} = \\
 &= N(1+i)^e \prod_{j=1}^r N(a_j + b_j i)^{e_j} \prod_{h=1}^s N(p_h)^{e_h} = \\
 &= N \left( u(1+i)^e \prod_{j=1}^r (a_j + b_j i)^{e_j} \prod_{h=1}^s p_h^{e_h} \right) = N(z)
 \end{aligned}$$

r. 3985; p. 67

**Osservazione 2.24 —** Il risultato appena visto non è un fatto ovvio. Consideriamo  $\beta = 1 + \frac{\sqrt{3}}{2}$ , il suo polinomio minimo su  $\mathbb{Q}$  è  $\mu(x) = x^2 - x - \frac{1}{2}$ . Ragionando in modo analogo a quanto fatto sopra, il nucleo della valutazione in  $\beta$  è

$$\mathbb{Z}[x] \cap \left( x^2 - x - \frac{1}{2} \right) \mathbb{Q}[x] = (2x^2 - 2x - 1)\mathbb{Z}[x]$$

E  $\frac{\mathbb{Z}[x]}{(2x^2 - x - 1)} \cong \mathbb{Z}[\beta]$ . D'altra parte

correzione minore

$$E \rightarrow e$$

$$e \quad \text{e } \frac{\mathbb{Z}[x]}{(2x^2 - x - 1)} \cong \mathbb{Z}[\beta].$$

---

rr. 4031-4033; p. 68

che rispetta gli assiomi di norma euclidea, ricordiamo che gli elementi invertibili di  $A^*$  sono gli elementi di norma  $\mathcal{N}$  minima. Consideriamo l'insieme  $X = \{\mathcal{N}(x) \mid x \in A \setminus A^*\}$ , poiché  $X$  è un sottoinsieme non vuoto di  $\mathbb{N}$  esiste un elemento minimo  $m \in X$ , sia  $x \in A \setminus A^*$  tale che  $\mathcal{N}(x) = m$ . Per definizione di dominio euclideo, per ogni  $a \in A$  esistono  $q, r \in A$  tali che  $a = qx + r$ , con  $r = 0$  oppure  $\mathcal{N}(r) < \mathcal{N}(x)$ . Se  $r \neq 0$  allora  $r \in A^*$  per minimalità di  $\mathcal{N}(x)$ , pertanto l'insieme dei possibili resti della divisione per  $x$  è  $\{0, 1, -1\}$ . Abbiamo quindi che l'insieme  $\{0, 1, -1\}$  è un insieme di rappresentanti, possibilmente con ripetizioni, per gli elementi del quoziente  $A/(x)$ , che è quindi isomorfo a  $\mathbb{F}_2$  oppure  $\mathbb{F}_3$ .

Il polinomio  $\mu(x) = x^2 - x + 5$  ha come soluzioni in  $A$   $\omega$  e  $\bar{\omega}$ , pertanto è riducibile in  $A[x]$ . Da questo si ricava che le classi di  $\omega$  e  $\bar{\omega}$  nel quoziente  $A/(x)$  sono le radici della classe del polinomio  $\mu(x)$ , che è assurdo in quanto  $\mu(x)$  è irriducibile in  $\mathbb{F}_2[x]$  e in  $\mathbb{F}_3[x]$ . Pertanto  $A$  non è un dominio euclideo.

riscrittura

Il polinomio  $\mu(x) = x^2 - x + 5$  ha come soluzioni in  $A$   $\omega$  e  $\bar{\omega}$ , pertanto è riducibile in  $A[x]$ . Da questo si ricava che le classi di  $\omega$  e  $\bar{\omega}$  nel quoziente  $A/(x)$  sono le radici di  $\mu(x)$ , che è assurdo in quanto  $\bar{\mu}(x)$  è irriducibile in  $\mathbb{F}_2[x]$  e in  $\mathbb{F}_3[x]$ . Pertanto  $A$  non è un dominio euclideo.

r. 4174; p. 71

$$\Phi^k = id_{\mathbb{F}_{p^n}} \iff x^{p^k} = x \quad \forall x \in \mathbb{F}_{p^n}$$

e l'equazione è verificata se e solo se il polinomio  $t^{p^k} - t$  ha almeno  $p^n$  radici, cioè se  $k \geq n$ . D'altra parte l'ordine di  $\Phi$  deve dividere  $n$ , pertanto  $\text{ord } \Phi = n$ . Quindi  $\Phi$  è un generatore di  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ , che è isomorfo a  $\mathbb{Z}/n\mathbb{Z}$ .  $\square$

aggiunta

$p^n$  radici, cioè se  $k \geq n$ . D'altra parte l'ordine di  $\Phi$  deve dividere  $|\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$ , pertanto  $\text{ord } \Phi = n$ . Quindi  $\Phi$  è un generatore

---

- mostriamo che  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$ . Un'immersione  $\psi \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  è univocamente determinata dall'immagine di  $\zeta_n$ , inoltre  $\psi(\zeta_n)$  è un elemento dell'insieme  $\{\zeta_n^k \mid k = 0, \dots, n-1\}$  in quanto è radice di  $x^n - 1$ . Supponiamo per assurdo che  $\psi(\zeta_n) = \zeta_n^k$  con  $d = (k, n) \neq 1$ , allora

$$\psi(\zeta_n^{\frac{n}{d}})\psi(\zeta_n)^{\frac{n}{d}} = \zeta_n^{k\frac{n}{d}} = \zeta_n^{\frac{k}{d}n} = 1$$

da cui  $\zeta_n^{\frac{n}{d}} = 1$ , che è assurdo in quanto  $\text{ord } \zeta_n = n$ . Pertanto  $\psi(\zeta_n) \in \{\zeta_n^k \mid k < n, (n, k) = 1\}$ , quindi  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$ ;

- siano  $p$  un primo che non divide  $n$ ,  $f(x)$  e  $g(x)$  i polinomi minimi su  $\mathbb{Q}$  rispettivamente di  $\zeta_n$  e  $\zeta_n^p$ , osserviamo che  $f(x) \mid g(x^p)$  in quanto  $g(\zeta_n^p) = 0$ ;
- supponiamo per assurdo  $f(x) \neq g(x)$ , allora  $f(x)$  e  $g(x)$  sono coprimi in  $\mathbb{Q}[x]$  ed entrambi dividono  $x^n - 1$ , pertanto  $f(x)g(x) \mid x^n - 1$ . Per il Lemma di Gauss esistono  $q(x), r(x) \in \mathbb{Z}[x]$  tali che

$$f(x)g(x)q(x) = x^n - 1 \quad f(x)r(x) = g(x^p)$$

## typo, aggiunte

```
\[
  \psi(\zeta_n^{\frac{n}{d}}) = \psi(\zeta_n)^{\frac{n}{d}} = \zeta_n^{k\frac{n}{d}}
  \zeta_n^{\frac{k}{d}n} = 1
]
da cui $\zeta_n^{\frac{n}{d}} = 1$,
\footnote{$\psi$ è un omomorfismo di anelli con identità iniettivo, quindi l'unico elemento che può andare in 1 è proprio 1.}
che è assurdo in quanto $\text{ord } \zeta_n = n$.
```

```
\item supponiamo per assurdo $f(x) \neq g(x)$, allora $f(x)$ e $g(x)$ sono coprimi in $\mathbb{Q}[x]$ (perché sono irriducibili) ed entrambi dividono $x^n - 1$, pertanto $f(x)g(x) \mid x^n - 1$.
Per il Lemma di Gauss
\footnote{Queste divisibilità valgono in $\mathbb{Q}[x]$ quindi, per un corollario del Lemma di Gauss, valgono anche in $\mathbb{Z}[x]$.}
esistono $q(x), r(x) \in \mathbb{Z}[x]$ tali che
```

r. 4330; p. 73

Poiché  $H$  contiene le restrizioni a  $K$  degli elementi di  $\text{Gal}(KL/L)$ , si ha

$$\begin{aligned} K^H &= \{x \in K \mid \psi(x) = x \ \forall \psi \in \text{Gal}(KL/L)\} = \\ &= K \cap \{x \in KL \mid \psi(x) = x \ \forall \psi \in \text{Gal}(KL/L)\} = \\ &= K \cap (KL)^{\text{Gal}(KL/L)} = K \cap L \end{aligned}$$

pertanto  $H = \text{Gal}(K/K \cap L)$  per il Teorema di Corrispondenza di Galois. Quindi  $\Phi$  è surgettivo, di conseguenza è un isomorfismo tra  $\text{Gal}(KL/L)$  e  $\text{Gal}(K/K \cap L)$ .

typo

pertanto  $H = \text{Gal}(K/K \cap L)$  per il Lemma di Artin. Quindi  $\Phi$  è surgettivo, di conseguenza è un isomorfismo

---

*Nelle versioni più recenti:*

p. 73

*Dimostrazione.* Sia  $f(x) = \prod_{d|n} \Phi_d(x)$ , notiamo che:

- sia  $\alpha$  una radice di  $x^n - 1$ , posta  $\zeta_n$  una radice primitiva  $n$ -esima si ha  $\alpha = \zeta_n^{\frac{n}{d}}$  con  $d | n$ . Allora  $\text{ord } \alpha = d$ , pertanto  $\alpha$  è una radice primitiva  $d$ -esima. In particolare ogni radice di  $x^n - 1$  è una radice di  $f(x)$ , cioè  $x^n - 1 | f(x)$ ;
- sia  $\alpha$  una radice di  $f(x)$ , allora  $\alpha$  è una radice primitiva  $d$ -esima dell'unità con  $d | n$ , in particolare  $\alpha^d = 1$  e quindi  $\alpha^n = 1$ . Allora  $\alpha$  è una radice  $n$ -esima dell'unità, cioè  $f(x) | x^n - 1$ ;
- dai due punti precedenti si deduce che esiste  $\lambda \in \mathbb{Q}^*$  tale che  $x^n - 1 = \lambda f(x)$ , d'altra parte entrambi i polinomi sono monici, quindi  $x^n - 1 = f(x)$ .

typo (da staccare)

---

p. 76

Abbiamo quindi che la sottoestensione  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  ha grado 3 su  $\mathbb{Q}$ , mostriamo quindi che è una sua estensione normale. Posto  $\alpha = \zeta_7 + \zeta_7^{-1}$ , le immersioni di  $\mathbb{Q}(\alpha) \hookrightarrow \overline{(\mathbb{Q}\mathbb{Q})}$  sono le restrizioni a  $\mathbb{Q}(\alpha)$  degli elementi di  $\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ , pertanto sono univocamente determinate dalle assegnazioni

$$\zeta_7 + \zeta_7^{-1} \mapsto \zeta_7 + \zeta_7^{-1} \quad \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2} \quad \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^3 + \zeta_7^{-3}$$

typo (`\overline` è andato sulla parentesi e non ha preso `\QQ`)

---

p. 77

Il polinomio minimo di  $\alpha$  su  $\mathbb{Q}$  è quindi

$$\mu_\alpha(x) = (x - (\zeta_7 + \zeta_7^{-1}))(x - (\zeta_7^2 + \zeta_7^{-2}))(x - (\zeta_7^3 + \zeta_7^{-3})) = x^3 + x^2 - 2x - 1$$

Notiamo che  $\zeta_7^2 + \zeta_7^{-2}$  e  $\zeta_7^3 + \zeta_7^{-3}$  sono elementi di  $\mathbb{Q}(\alpha)$ , in quanto

$$\zeta_7^2 + \zeta_7^{-2} = (\zeta_7 + \zeta_7^{-1})^2 - 1$$

$$\zeta_7^3 + \zeta_7^{-3} = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 - \zeta_7^{-1})$$

pertanto  $\mathbb{Q}(\alpha)/\mathbb{Q}$  è un'estensione normale di grado 3 in quanto campo di spezzamento di  $\mu_\alpha(x)$  su  $\mathbb{Q}$ , quindi il suo gruppo di Galois è isomorfo a  $\mathbb{Z}/3\mathbb{Z}$ .

typo

$$1 \rightarrow 2$$

$$- \rightarrow +$$