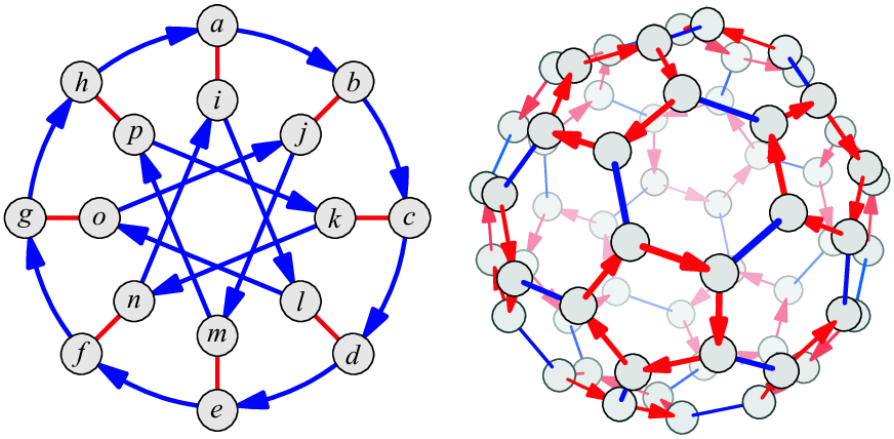
APPUNTI DI ALGEBRA

Manuel Deodato



Indice

1 Gli interi

1.1 Proprietà di base

Una proprietà dei numeri interi, che si prenderà come assiomatica, è quella del *buon ordinamento*:

Ogni insieme non-vuoto di interi maggiori o uguali a 0, *ha un elemento minimo.*

Da questa deriva la seguente.

Teorema 1.1 (Principio di induzione (prima forma))
Sia $A(n)$ un'affermazione valida per ogni intero $n \geq 1$. Se

(1). $A(1)$ è vera,

(2). $\forall n \geq 1$, se $A(n)$ è vera $\implies A(n+1)$ è vera,

allora, $\forall n \geq 1$, $A(n)$ è vera.

Dimostrazione. Sia S l'insieme di interi per cui $A(n)$ è falsa. Si mostra che S è l'insieme vuoto. Si assume per assurdo che $S \neq \varnothing \Rightarrow \exists n_0 \in S$, con n_0 minimo (esistente per il buon ordinamento), e, per assunzione, deve essere $n_0 \neq 1 \Rightarrow n_0 > 1$. Questo vuol dire che $n_0 - 1$ non è in S e, quindi, $A(n_0 - 1)$ è vera.

Per la proprietà (2), però, deve essere vera anche $A(n_0)$ perché $n_0 = (n_0 - 1) + 1$, il che è assurdo e, pertanto, $S = \varnothing$. □

Osservazione 1.1. Nella dimostrazione sopra, si sarebbe potuto sostituire 1 con 0 e far partire il principio di induzione da $n = 0$ piuttosto che da $n = 1$ e non sarebbe cambiato nulla.

Il principio di induzione può essere espresso in una forma alternativa, come segue.

Teorema 1.2 (Principio di induzione (seconda forma))
Sia $A(n)$ affermazione vera $\forall n \geq 0$ e sia possibile mostrare che:

(1'). $A(0)$ è vera;

(2'). $\forall n > 0$, se $A(k)$ è vera $\forall 0 \leq k < n$, allora $A(n)$ è vera.

Allora $A(n)$ è vera $\forall n \geq 0$.

Dimostrazione. Sia ancora S l'insieme degli interi che non soddisfano $A(n)$. Ancora per assurdo, si prende $S \neq \varnothing$, quindi deve esistere, per il buon ordinamento, un $n_0 \in S$ minimo.

Per punto (1'), deve valere $n_0 \neq 0$ e, visto che n_0 è minimo, $\forall k$ intero tale che $0 \leq k < n_0$, $A(k)$ deve essere vera. Per il punto (2'), però, deve essere vera anche $A(n_0)$, arrivando nuovamente all'assurdo. □

Un altro importante risultato del buon ordinamento è l'*algoritmo di Euclide*.

Teorema 1.3 (Algoritmo di Euclide)

Siano m, n interi, con $m > 0$; allora esistono interi q, r, con $0 \leq r < m$, tali che

$$n = qm + r \tag{1.1.1}$$

Inoltre, gli interi q, r sono univocamente determinati da tali condizioni.

Dimostrazione. Visto che l'insieme degli interi q tali per cui $qm \leq n$ è limitato superiormente per definizione, si può usare il buon ordinamento per affermare che esiste un elemento più grande[a] tale che

$$qm \leq n < (q+1)m = qm + m$$

ossia $0 \leq n - qm < m$. Sia $r = n - qm$, per cui vale $0 \leq r < m$. Questo dimostra l'esistenza di r, q come descritti.

Per l'unicità, si assume che valga contemporaneamente

$$\begin{cases} n = q_1 m + r_1 & , \ 0 \leq r_1 < m \\ n = q_2 m + r_2 & , \ 0 \leq r_2 < m \end{cases}$$

con $r_1 \neq r_2$. Sia, per esempio, $r_2 > r_1$; allora, sottraendo le due, si ha $(q_1 - q_2)m = r_2 - r_1$. Però, si ha $r_2 - r_1 > 0$ e $r_2 - r_1 < m$, il che non è possibile perché $q_1 - q_2$ è un intero per cui $(q_1 - q_2)m > 0$, quindi si avrebbe $r_2 - r_1 = (q_1 - q_2)m \geq m$ e, quindi $r_2 - r_1 \geq m$. Pertanto, deve essere $r_1 = r_2$, che fra l'altro implica $q_1 m = q_2 m$, per cui $q_1 = q_2$. □

[a] Basta applicare il buon ordinamento all'elemento più piccolo dell'insieme $n - qm$.

Da questo teorema, si definisce r come il *resto della divisione di n per m*.

1.2 Massimo comune divisore

Siano n, d due interi diversi da 0. Si dice che d *divide* n se esiste q intero tale che $n = dq$; in questo caso, si scrive $d|n$. Se m, n sono interi non-nulli, per *divisore comune* di m e n si intende un intero $d \neq 0$ tale che $d|m$ e $d|n$. Allora si ha la seguente definizione.

Definizione 1.1 (Massimo comune divisore)

Per massimo comune divisore di m, n interi non nulli, si intende un intero $d > 0$, divisore comune di m e n, e tale che $\forall e$ intero positivo che divide m e n, si ha anche $e|d$.

Chiaramente, il massimo comune divisore è univocamente determinato e si mostrerà che esiste sempre. Per farlo, si dà prima la seguente definizione.

Definizione 1.2 (Ideale)

Sia $J \subseteq \mathbb{Z}$ un sottoinsieme degli interi. Si dice che J è un *ideale* se:

- $0 \in J$;
- $m, n \in J \implies m + n \in J$
- se $m \in J$ e n è un intero qualsiasi, allora $mn \in J$.

Osservazione 1.2. Di seguito, per ideale si intenderà sempre un sottoinsieme degli interi.

Siano $m_1, \ldots, m_r$ interi. Sia J l'insieme di tutti gli interi che si scrivono come

$$x_1 m_1 + \ldots + x_r m_r$$

con $x_1, \ldots, x_r$ interi. Allora è automaticamente verificato che J è un ideale. Infatti

- se $y_1, \ldots, y_r$ sono interi, allora

  $$\sum_{i=1}^{r} x_i m_i + \sum_{j=1}^{r} y_j m_j = (x_1 + y_1)m_1 + \ldots + (x_r + y_r)m_r$$

  che, quindi, appartiene a J;

- se n è un intero, si ha

  $$n \sum_{i=1}^{r} x_i m_i = n x_1 m_1 + \ldots + n x_r m_r$$

  che, quindi, appartiene a J;

- si può scrivere 0 come $0m_1 + \ldots + 0m_r$, quindi anche $0 \in J$.

In questo caso, si dice che J è **generato** dagli interi $m_1, \ldots, m_r$ e che questi sono i suoi **generatori**. L'insieme $\{0\}$ è esso stesso un ideale, chiamato **ideale nullo**. Inoltre, $\mathbb{Z}$ è detto **ideale unità**. Ora si può dimostrare il seguente.

Teorema 1.4

Sia J un ideale di $\mathbb{Z}$. Allora esiste un intero d che è un generatore di J. Inoltre, se $J \neq \{0\}$, allora d è il più piccolo intero positivo in J.

Dimostrazione. Sia J l'ideale nullo; allora 0 è un suo generatore. Sia, ora, $J \neq \{0\}$; se $n \in J$, allora $-n = (-1)n$ è anche in J, quindi J contiene degli interi positivi. Si vuole dimostrare che d, definito come il più piccolo intero positivo, è un generatore. Per farlo, sia $n \in J$, con $n = dq + r,\ 0 \leq r < d$; allora $r = n - dq \in J$ e, visto che vale $r < d$, segue che $r = 0$[a], quindi $n = dq$ e, allora, d è un generatore. □

[a] Altrimenti d non sarebbe il più piccolo intero positivo.

Teorema 1.5

Siano m_1, m_2 due interi positivi e sia d un generatore positivo per l'ideale generato da m_1, m_2. Allora d è il massimo comune divisore di m_1, m_2.

Dimostrazione. Per definizione, $m_1, m_2 \in J$[a], quindi esiste un intero q_1 tale che $m_1 = q_1 d$, per cui $d|m_1$. Analogamente $d|m_2$. Sia, poi, e un intero non-nullo che divide sia m_1 che m_2 come $m_1 = h_1 e$ e $mm_2 = h_2 e$, con interi h_1, h_2. Visto che d è nell'ideale generato da m_1, m_2, esistono degli interi s_1, s_2 tali che $d = s_1 m_1 + s_2 m_2$, quindi

$$d = s_1 h_1 e + s_2 h_2 e = (s_1 h_1 + s_2 h_2) e$$

Quindi e divide d e il teorema è dimostrato. □

[a] Questo è ovvio perché $m_1 = 1m_1 + 0m_2$ e $m_2 = 0m_1 + 1m_2$.

Osservazione 1.3. La stessa esatta dimostrazione funziona per più di due interi, quindi se si considerassero $m_1, \ldots, m_r$ degli interi, con d generatore positivo dell'ideale da loro generato, d sarebbe anche il massimo comune divisore.

Questi due teoremi permettono di concludere i seguenti fatti.

- Ogni ideale J contiene un numero intero che lo genera interamente e questo coincide col più piccolo intero positivo in esso contenuto, quindi è l'unico generatore *singolo* dell'ideale.
- Ogni insieme di numeri interi ha un massimo comune divisore perché tale insieme genera un ideale, il quale, però, contiene un generatore (più piccolo numero intero in esso contenuto) che è un massimo comune divisore per l'insieme di interi iniziale.

Definizione 1.3 (Interi coprimi)

Siano $m_1, \ldots, m_r$ degli interi il cui massimo comune divisore è 1. Allora $m_1, \ldots, m_r$ si dicono *coprimi* e, per questi, esistono interi $x_1, \ldots, x_r$ tali che

$$x_1 m_1 + \ldots + x_r m_r = 1$$

perché 1 appartiene all'ideale generato dagli m_i.

È immediato verificare per definizione di ideale che $1 \in J \iff J \equiv \mathbb{Z}$. Dalla definizione 1.3 segue direttamente che ogni insieme di interi coprimi genera $\mathbb{Z}$.

Osservazione 1.4. Si potrebbe pensare che se p è un numero primo, allora l'insieme $\{p\}$ generi $\mathbb{Z}$, cioè p generi $\mathbb{Z}$. Questo è ovviamente falso sia perché, evidentemente, J_p non contiene 1, sia perché p non è coprimo con se stesso, avendo come altro divisore proprio p oltre che 1.

1.3 Fattorizzazione unica

Definizione 1.4 (Numero primo)
Si dice che p è un numero primo se è un intero e $p \geq 2$ tale che, data una fattorizzazione $p = mn$, con interi positivi m, n, allora $m = 1$ o $n = 1$.

Osservazione 1.5. Il fatto che $p = mn$ con $m = 1$, o $n = 1$ implica p numero primo significa che p è diviso unicamente o da 1 o, da se stesso.

Ora si mostra che ogni numero intero ammette un'unica scomposizione in numeri primi. Per dimostrare l'unicità di tale scomposizione, si introduce il seguente lemma.

Lemma 1.1
Sia p un numero primo e siano m, n interi non-nulli e tali che p divide mn. Allora o $p|m$ o $p|n$.

Dimostrazione. Senza perdita di generalità, si assume che p *non* divida m. Allora, il massimo comune divisore di p e m deve essere 1, pertanto esistono interi a, b tali per cui $1 = ap + bm$.

Ora, moltiplicando ambo i membri per n, si ha $n = nap + bmn$, ma $mn = pc$ per qualche intero c (essendo in assunzione mn divisibile per p), quindi

$$n = nap + bpc = (na + bc)p$$

il che implica che p divide n. □

Per evidenziare l'utilità del lemma nel seguente teorema, si nota che se p divide un prodotto di numeri primi $q_1 \dots q_s$, si hanno due possibilità: o p divide q_1, o divide $q_2 \dots q_s$; se divide q_1, allora $p \equiv q_1$, altrimenti si trova $p \equiv q_i$ procedendo induttivamente. Il caso interessante è quando si ha un uguaglianza tra prodotti di numeri primi

$$p_1 \dots p_r = q_1 \dots q_s$$

dove ogni p_i divide il prodotto[1]. Rinumerandoli, si può assumere senza perdita di generalità che $p_1 = q_1$ e, induttivamente, che $p_i = q_i$ e $r = s$, essendo due scomposizioni in un numeri primi.

Teorema 1.6
Ogni intero positivo $n \geq 2$ ammette una fattorizzazione come prodotto di numeri primi (non necessariamente distinti) $n = p_1 \dots p_r$ e tale fattorizzazione è unica.

Dimostrazione. Si assume per assurdo che esista almeno un intero ≥ 2 che non possa essere espresso come prodotto di numeri primi. Sia m il più piccolo di

[1] Per vederlo, è sufficiente prendere $c = p_1 \dots p_{i-1} p_{i+1} \dots p_r$, quindi si ha $cp_i = q_1 \dots q_s$, che è la definizione di $p_i | q_1 \dots q_s$.

questi.

Per costruzione, m non può essere primo, quindi $m = de$, con $d, e > 1$. Visto che d ed e sono minori di m e visto che m è scelto per essere il più piccolo fra gli interi non fattorizzabili come numeri primi, allora sia d che e ammettono scomposizione in prodotto di numeri primi:

$$\begin{aligned} d &= p_1 \dots p_r \\ e &= p'_1 \dots p'_s \end{aligned} \implies m = p_1 \dots p_r p'_1 \dots p'_s$$

da cui l'assurdo.

Per mostrare l'unicità, si usa il lemma 1.1. Come conseguenza, diretta del lemma, se esistessero due scomposizioni in primi $p_1 \dots p_r$ e $p'_1 \dots p'_s$, varrebbe $p_1 \dots p_r = p'_1 \dots p'_s \Rightarrow p_i = p'_i$ e $r = s$, da cui l'unicità □

1.4 Identità di Bézout e equazioni diofantee

1.4.1 Identità di Bézout

L'identità di Bézout non è altro che quanto espresso in teorema 1.5. Di seguito lo si enuncia senza ricorrere a tale trattazione.

Teorema 1.7 (Identità di Bézout)
Dati $a, b \in \mathbb{Z}$ non entrambi nulli, esistono altri due interi m, n tali che:

$$\gcd(a, b) = am + bn$$

Dimostrazione. Si considera l'insieme di tutte le possibili combinazioni lineari positive di a, b, dato da $\mathrm{CL}^+(a, b) := \{ar + bs : r, s \in \mathbb{Z},\ ar + bs > 0\}$. Questo è non-vuoto perché, assumendo senza perdita di generalità $a \neq 0$, esistono, per $s = 0$, degli $r \in \mathbb{Z}$ tali che $ra > 0$.

Visto che $\mathrm{CL}^+(a, b) \subseteq \mathbb{N}$, per il principio del buon ordinamento, questo ammette un minimo d; in quanto tale $\exists m, n \in \mathbb{Z} : d = am + bn$. Infine, si motra che $d = \gcd(a, b)$, cioè si mostrano i seguenti punti.

- Si ha $d|a$ e $d|b$.

  Dividendo a per d, si ha $a = qd + r$, con $0 \leq r < d$, quindi

  $$a = q(am + bn) + r$$

  da cui

  $$r = (-qm + 1)a + (-qn)b$$

  In questo modo, r è combinazione lineare di a, b ed è minore di d, ma questo

è assurdo perché d era minimo per assunzione, quindi deve essere $r = 0$. Allo stesso modo si mostra $d|b$.

- Se $c|a$ e $c|b \implies c \leq d$.

  Questo è vero perché se $c|a,\ c|b$, allora (in particolare) $c|(am+bn)$, cioè $c|d \Rightarrow c \leq d$.

□

Osservazione 1.6. Il teorema afferma l'esistenza di una possibile coppia $(m,n) \in \mathbb{Z}\times\mathbb{Z}$ che soddisfa $\gcd(a,b) = am+bn$, ma non ne specifica l'unicità; di fatto, si vedrà che di coppie simili ce ne sono infinite.

Corollario 1.1

Dati $a,b \in \mathbb{Z}$ non entrambi nulli e sia $c \in \mathbb{Z} : c|a$ e $c|b$; allora $c|\gcd(a,b)$.

Complessivamente, esattamente come riportato nel teorema 1.5, si è dimostrato che il massimo comune divisore di due interi a,b è la più piccola combinazione lineare positiva ottenibile dai due.

Corollario 1.2

Dati a,b non entrambi nulli e $\gcd(a,b)$ il loro massimo comune divsore, allora gli interi

$$a' = \frac{a}{\gcd(a,b)} \qquad\qquad b' = \frac{b}{\gcd(a,b)}$$

sono coprimi.

Dimostrazione. Si può dimostrare in due modi diversi. Nel primo, si assume per assurdo che esista un divisore comune $d > 1$ di a', b'; se così fosse, però, $d \cdot \gcd(a,b)$ dividerebbe sia a che b e sarebbe più grande di $\gcd(a,b)$ stesso, il che è assurdo.

Il secondo fa uso dell'identità di Bézout per cui $\gcd(a,b) = am+bn$; dividendo per $\gcd(a,b)$, si ha:

$$1 = a'm + b'n$$

per cui 1 è il più piccolo intero positivo ottenibile come combinazione lineare positiva di a', b', quindi i due sono coprimi. □

Teorema 1.8

Siano $a,b,c \in \mathbb{Z}$; se $a|bc$ e $\gcd(a,b) = 1$, allora $a|c$.

Dimostrazione. Per Bézout, visto che $\gcd(a,b) = 1$, si ha $1 = an+bm$ per una coppia di numeri $m,n \in \mathbb{Z}$. Moltiplicando ambo i membri per c, ne segue che $c = acn + bcm$, quindi $a|c$ perché, ovviamente, $a|acn$, mentre $a|bcm$ perché, per ipotesi, $a|bc$, quindi $a|(acn+bcm)$, cioè $a|c$. □

Il teorema appena dimostrato è alla base del fatto che la fattorizzazione di interi in

numeri primi è unica.

1.4.2 Equazioni diofantee

Dati $a, b, c \in \mathbb{Z}$, si dice **equazione diofantea** un'equazione del tipo

$$ax + by = c \tag{1.4.1}$$

La sua soluzione è una coppia di interi $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ che la soddisfa.

> **Osservazione 1.7.** L'equazione diofantea con $a = b = 0$ ha soluzione $\iff c = 0$ e ne ammette infinite, consistenti in tutte le possibili coppie $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$, perché ogni coppia soddisfa $0x + 0y = c$.

Per il caso generale di a, b non entrambi nulli, si ha il seguente.

Teorema 1.9

L'equazione $ax + by = c$, con a, b non entrambi nulli, ha soluzione $\iff \gcd(a, b) | c$.

Dimostrazione. Per l'identità di Bézout, si sa che vi è soluzione all'equazione

$$ax + by = \gcd(a, b)$$

L'equazione da risolvere è diversa: al posto di $\gcd(a, b)$ c'è c; allora la dimostrazione si basa sul capire se $\gcd(a, b)$ divide o meno c.

Nel caso in cui $\gcd(a, b) | c$ (per cui si ha $c = k \cdot \gcd(a, b)$ per qualche intero k), allora l'equazione diofantea ammette soluzione. Infatti, dopo aver trovato $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ che risolve $am + bn = \gcd(a, b)$, si ha che $(mk, nk) \in \mathbb{Z} \times \mathbb{Z}$ risolve l'equazione diofantea perché

$$k \cdot (am + bn) = akm + bkn = k \cdot \gcd(a, b) = c$$

Viceversa, se $\gcd(a, b)$ non divide c, allora non vi è soluzione. Se, per assurdo, vi fosse soluzione, sia questa $(\overline{x}, \overline{y})$, allora $a\overline{x} + b\overline{y} = c$ implica che $\gcd(a, b) | c$ perché $\gcd(a, b)$ divide il membro di sinistra (essendo un divisore sia di a che di b). Questo, però, è assurdo perché si era nell'ipotesi in cui $\gcd(a, b) \nmid c$. □

Si considera il caso in cui l'equazione $ax + by = c$ ha soluzione; si vuole capire se la soluzione è unica, o se ve ne sono di più. Si considera, a tal proposito, l'**omogenea associata** $ax + by = 0$.

> **Osservazione 1.8.** La comodità nel lavorare con l'omogenea associata sta nel fatto che se $(\overline{x}, \overline{y})$ risolve $ax + by = c$ e (γ, δ) risolve l'omogenea, allora $(\overline{x} + \gamma, \overline{y} + \delta)$ è ancora soluzione di $ax + by = c$.

L'obiettivo, ora, è di trovare il numero delle soluzioni per l'omogenea associata. Si nota che $ax + by = 0 \Rightarrow ax = -by$; si risolve

$$\frac{a}{\gcd(a,b)}x = -\frac{b}{\gcd(a,b)}y$$

Sia (γ, δ) una soluzione di questa; visto che $a/\gcd(a,b)$ e $b/\gcd(a,b)$ sono coprimi[1], il teorema 1.8 afferma che $a/\gcd(a,b)$ divide δ, quindi δ è della forma $\frac{a}{\gcd(a,b)}t$ e γ, analogamente, è della forma $-\frac{b}{\gcd(a,b)}t$.

Al contrario, si nota facilmente che una qualunque coppia della forma

$$\left(-\frac{b}{\gcd(a,b)}t, \frac{a}{\gcd(a,b)}t\right)$$

con $t \in \mathbb{Z}$ è una soluzione dell'omogenea associata. Questo significa che le soluzioni dell'omogenea associata sono tutte di questa forma, pertanto sono infinite.

Da questo discorso, si può concludere che anche le soluzioni dell'equazione diofantea iniziale $ax + by = c$ sono infinite. Il teorema di seguito permette di concludere, ulteriormente, che *tutte* le soluzioni di $ax + by = c$ sono esprimibili tramite quelle dell'omogenea, quindi equazione originale e omogenea hanno lo stesso numero di soluzioni.

Teorema 1.10

Se l'equazione $ax + by = c$ ammette soluzione, allora ne ammette infinite. Data $(\overline{x}, \overline{y})$ una sua soluzione, l'insieme $\mathcal{S}$ di tutte le soluzioni di $ax + by = c$ è ottenibile come

$$\mathcal{S} = \{(\overline{x} + \gamma, \overline{y} + \delta) : (\gamma, \delta) \text{ soluzione dell'omogenea associata}\}$$

Dimostrazione. Per quanto detto sopra, si conclude che

$$\{(\overline{x} + \gamma, \overline{y} + \delta) : (\gamma, \delta) \text{ soluzione dell'omogenea associata}\} \subseteq \mathcal{S}$$

Si deve mostrare l'inclusione inversa. Questo segue direttamente dal fatto che, se (α, β) è soluzione di $ax + by = c$, allora $(\alpha - \overline{x}, \beta - \overline{y})$ è soluzione dell'omogenea associata. □

1.5 Relazioni di equivalenza e congruenza

Definizione 1.5 (Relazione di equivalenza)

Sia S un insieme. Una relazione di equivalenza su S è una relazione indicata con $x \sim y$, $x, y \in S$, tale che:

ER 1. $\forall x \in S,\ x \sim x$;

[1] Vedi corollario 1.2.

ER 2. se $x \sim y$ e $y \sim z$, allora $x \sim z$;

ER 3. se $x \sim y$, allora $y \sim x$.

Se su S è definita una relazione di equivalenza $\sim$, le classi di equivalenza sono insiemi $C_x := \{y \in S : y \sim x\}$ partizionano S in insiemi disgiunti. Inoltre, dati due elementi $r, s \in S$, si ha $C_r \equiv C_s$, oppure C_r, C_s non hanno elementi in comune. Si sceglie un elemento che identifica la classe di equivalenza, ad esempio x per C_x, e tale elemento si chiama rappresentante della classe di equivalenza. Un esempio di relazione di equivalenza è la congruenza.

Definizione 1.6 (Congruenza)

Sia $m \in \mathbb{Z}^+$ e $a, b \in \mathbb{Z}$; si dice che a è *congruente b modulo m* se $\exists k \in \mathbb{Z} : a - b = km$. In tal caso, si scriverà $a \equiv b \pmod{m}$.

Osservazione 1.9. La definizione più esplicativa di congruenza è che due numeri $a, b \in \mathbb{Z}$ di dicono congruenti modulo $m \in \mathbb{Z}^+$ se, divisi per m, restituiscono lo stesso resto. Di fatto, da questa discende la definizione data sopra: se $a = qm + r$, $b = pm + r \Rightarrow a - b = (q - p)m$.

Definizione 1.7 (Interi pari e dispari)

Si definiscono gli interi **pari** come quelli che sono congruenti a $0 \pmod{2}$ (quindi $n = 2m$) e quelli **dispari** come gli interi che non sono pari, quindi della forma $2m + 1$, per qualche intero m.

Dalla definizione di congruenza, si ha che $a \equiv b \pmod{m} \Rightarrow a - b = qm$, quindi $a - b$ appartiene all'ideale generato da m.

Inoltre, la stessa relazione implica che $m|(a - b)$; viceversa, se $a \not\equiv b \pmod{m}$, allora i due numeri divisi per m avrebbero resti diversi: $a = k_1 m + r_a$, $b = k_2 m + r_b$, il che implica che $a - b = (k_1 - k_2)m + (r_a - r_b)$, che non è divisibile per m; allora si ha il seguente.

Proposizione 1.1

Siano $m \in \mathbb{Z}^+$ e $a, b \in \mathbb{Z}$; a e b sono congruenti se e soltanto se $m|(a - b)$.

Proposizione 1.2 (Addizione e moltiplicazione in congruenza)

Dati $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, si ha:

$$a + b \equiv a' + b' \pmod{m}$$
$$ab \equiv a'b' \pmod{m}$$

Dimostrazione. Per definizione, si ha $a' = a + km$ e $b' = b + k'm$; quindi:

$$a' + b' = a + b + (k + k')m \implies a' + b' \equiv a + b \pmod{m}$$

Per la moltiplicazione, si nota che

$$a'b' = ab + m(kb + k'a) + kk'm^2$$

da cui si vede che $a'b' - ab$ è divisibile per m, quindi $a'b' \equiv ab \pmod{m}$. □

La divisione in congruenza funziona diversamente; infatti $2 \cdot 7 \equiv 2 \cdot 4 \pmod{6}$, ma $7 \not\equiv 4 \pmod{6}$. Si ha il seguente.

Teorema 1.11 (Divisione in congruenza)

Sia $m \in \mathbb{Z}^+$; $\forall a \in \mathbb{Z} \setminus \{0\}$ e dati $b_1, b_2 \in \mathbb{Z}$, vale

$$ab_1 \equiv ab_2 \pmod{m} \iff b_1 \equiv b_2 \mod \frac{m}{\gcd(a,m)}$$

Questo vuol dire che la divisione è ammessa a patto di dividere il modulo per $\gcd(a,m)$.

Dimostrazione. Si mostra l'implicazione verso destra. Per definizione, $m \mid (ab_1 - ab_2)$, quindi $\exists q \in \mathbb{Z} : mq = ab_1 - ab_2$. Dividendo per $\gcd(a,m)$:

$$\frac{a}{\gcd(a,m)}(b_1 - b_2) = \frac{m}{\gcd(a,m)}q$$

Ma $a/\gcd(a,m)$ e $m/\gcd(a,m)$ sono coprimi, quindi $\left(m/\gcd(a,m)\right) \mid (b_1 - b_2)$, il che implica che

$$b_1 \equiv b_2 \mod \frac{m}{\gcd(a,m)}$$

Per l'implicazione inversa, si assume che

$$b_1 \equiv b_2 \mod \frac{m}{\gcd(a,m)}$$

per cui $\exists t \in \mathbb{Z}$ tale che

$$t\frac{m}{\gcd(a,m)} = b_1 - b_2 \implies tm = (b_1 - b_2)\gcd(a,m)$$

quindi $m \mid (b_1 - b_2)\gcd(a,m)$. Usando che $\gcd(a,m) \mid a$, si ottiene che

$$m \mid (b_1 - b_2)a \implies ab_1 \equiv ab_2 \pmod{m}$$

□

1.5.1 Inversi in congruenze

Gli unici inversi moltiplicativi in $\mathbb{Z}$ sono $+1, -1$; operando con le congruenze, si riescono a trovare altri inversi moltiplicativi a patto di definire correttamente cosa vuol

dire.

Definizione 1.8 (Inverso in congruenza)

Sia $m \in \mathbb{Z}^+$; l'inverso di $a \in \mathbb{Z}$ è un certo $e \in \mathbb{Z}$ tale che

$$e \cdot a \equiv 1 \pmod{m}$$

Esempio 1.1. Per esempio, 2 è l'inverso di $3 \bmod 5$ perché $2 \cdot 3 = 6 \equiv 1 \pmod{5}$.

Osservazione 1.10. Quando un numero ammette inverso in congruenza, ne ammette infiniti; infatti, se a è l'inverso di $n \bmod m$, allora

$$n \cdot (a + km) \equiv n \cdot a + knm \equiv 1 + knm \equiv 1 \pmod{m}$$

Non sempre un numero ammette un inverso moltiplicativo per qualche modulo; di seguito, è riportata una condizione necessaria e sufficiente per l'esistenza dell'inverso.

Teorema 1.12

Un numero $a \in \mathbb{Z}$ ha inverso $\bmod m$ se e solo se $\gcd(a, m) = 1$.

Dimostrazione. Si assume che $\gcd(a, m) = 1$; per Bézout, si ha:

$$au + mv = 1$$

per qualche coppia $u, v \in \mathbb{Z}$. Questa uguaglianza, letta modulo m, diventa:

$$au \equiv 1 \pmod{m}$$

cioè u è inverso di $a \bmod m$.

Per l'implicazione inversa, si assume che a abbia inverso moltiplicativo u. Questo implica che $au \equiv 1 \pmod{m}$, che, a sua volta, diventa:

$$au - mk = 1$$

per qualche $k \in \mathbb{Z}$. Questo è sufficiente per affermare che $\gcd(a, m) = 1$. □

1.5.2 Congruenze lineari in una incognita

Si cercano le soluzioni x alla congruenza $ax \equiv b \pmod{m}$. Si inizia col notare che se $\exists d \in \mathbb{Z}$ tale che $d|a$ e $d|m$, ma $d \nmid b$ allora l'equazione non ha soluzioni.

Dimostrazione. Se per assurdo ne avesse almeno una $\overline{x}$, allora sarebbe soddisfatta $a\overline{x} - b = qm$, per qualche $q \in \mathbb{Z}$. Ma, nonostante m sia divisibile per d, l'altro membro non risulta tale per via di b, il che è assurdo. □

Da quanto appena notato, si conclude la condizione necessaria perché esista almeno una soluzione, ossia $\gcd(a, m)|b$.

Osservazione 1.11. Se $k|a, b$, allora l'equazionoe

$$\frac{a}{k}x \equiv \frac{b}{k} \pmod{\frac{m}{\gcd(k,m)}}$$

è equivalente a $ax \equiv b \pmod{m}$, cioè hanno le stesse soluzioni. Si nota in particolare che, se s è un numero primo, allora l'equazione $sax \equiv sb \pmod{m}$ ha stesse soluzioni di quella di partenza.

Teorema 1.13

La congruenza $ax \equiv b \pmod{m}$ ha soluzione se e soltanto se $\gcd(a,m)|b$. Inoltre, il numero totale di soluzioni è $\gcd(a,m)$: le altre si ottengono sommandogli un multiplo di m.

Dimostrazione. La prima parte si è già dimostrata, quindi si dimostra solo quella relativa al numero di soluzioni. Assumendo che effettivamente $\gcd(a,m)|b$, allora $\gcd(a,m)$ è il massimo divisore comune di a, b, m; allora, dividendo la congruenza per questo, si ha:

$$a'x \equiv b' \pmod{m'}$$

dove

$$a' = \frac{a}{\gcd(a,m)} \qquad b' = \frac{b}{\gcd(a,m)} \qquad m' = \frac{m}{\gcd(a,m)}$$

dove a' e m' sono coprimi per costruzione. Essendo coprimi, significa che a' ha inverso moltiplicativo mod m'; sia questo e', il quale soddisfa $a'e' \equiv 1 \pmod{m'}$. Si può guardare la relazione dal punto di vista per cui l'inverso moltiplicativo di e' è a' e e' è coprimo con m'; in questo modo, si può moltiplicare per e' senza modificare il modulo:

$$e'a'x \equiv x \equiv e'b' \pmod{m'}$$

quindi le soluzioni dell'equazione sono tutte e sole quelle della forma

$$x = e'b' + qm' = e'b' + \frac{q}{\gcd(a,m)}m$$

per qualche $q \in \mathbb{Z}$. Questa forma permette di notare che esistono esattamente $\gcd(a,m)$ interi che risolvono questa equazione che non sono multipli di m. □

1.5.3 Il piccolo teorema di Fermat

Teorema 1.14 (Il piccolo teorema di Fermat)

Sia $p \in \mathbb{Z}$ un numero primo e $a \in \mathbb{Z}$ tale che $a \not\equiv 0 \pmod{p}$, cioè a non è multiplo di p[a]; allora

$$a^{p-1} \equiv 1 \pmod{p}$$

Dimostrazione. Per assunzione, $a \not\equiv 0 \pmod{p}$, quindi i numeri

$$a,\ 2a, \ldots, (p-1)a$$

sono, a due a due, non congrui mod p fra di loro; infatti, se così non fosse ed esistessero due numeri $i, j : 1 \leq i < j \leq p-1$ tali per cui $ia \equiv ja \pmod{p}$, allora $(i-j)a = qp$ per $q \in \mathbb{Z}$. Questo significa che, essendo a e p coprimi, per cui a ha inverso moltiplicativo b: $iab \equiv jab \pmod{m} \Rightarrow i \equiv j \pmod{m}$; questo non è possibile perché i e j erano stati assunti diversi e compresi tra 1 e $p-1$, quindi non possono avere stesso resto se divisi per p.

Allora, i resti dalla divisione per p di questi numeri sono nell'insieme $\{1, 2, \ldots, p-1\}$ perché il resto deve essere strettamente compreso da 1 e $p-1$ e deve essere diverso per ciascuno di quei numeri, per quanto appena mostrato. Questo permette di scrivere la seguente congruenza:

$$a \cdot (2a) \cdot \ldots \cdot \Big((p-1)a\Big) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$$

Raccogliendo a sinistra tutti i fattori a:

$$a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$$

Visto che ciascuno dei numeri è coprimo con p perché sono strettamente minori di p, si può moltiplicare questa congruenza per il loro inverso e arrivare a

$$a^{p-1} \equiv 1 \pmod{p}$$

□

[a] Questo basta per affermare che i due sono coprimi.

Corollario 1.3

Se $p \in \mathbb{Z}$ è primo, allora $\forall a \in \mathbb{Z}$ vale

$$a^p \equiv a \pmod{p}$$

Dimostrazione. Nel caso $a \not\equiv 0 \pmod{p}$, allora vale $a^{p-1} \equiv 1 \pmod{p}$ per il teorema di Fermat; usando ancora che a e p sono coprimi, si ottiene direttamente per moltiplicazione $a^p \equiv a \pmod{p}$.

Nel caso in cui $a \equiv 0 \pmod{p}$, invece, anche $a^p \equiv 0 \pmod{p}$; quindi, per transitività, si ha $a^p \equiv a \pmod{p}$. □

Corollario 1.4

Se $n \in \mathbb{Z}^{>1}$ è un intero tale che, per qualche $a \in \mathbb{Z}$, si ha $a^n \not\equiv a \pmod{n}$, allora n non è primo.

Osservazione 1.12. I numeri $n \in \mathbb{Z}^{>1}$ che soddisfano $a^n \equiv a \pmod{n}$ non sono necessariamente primi; questi sono noti come *falsi primi* e sono detti *numeri di Carmichael*.

Teorema 1.15 (Teorema di Wilson)

Sia $p > 1$ un intero; allora p è primo se e solo se $(p-1)! \equiv -1 \pmod{p}$.

Dimostrazione. Si divide la dimostrazione nelle due implicazioni.

- ($\Rightarrow$) Sia $p > 1$ un intero primo. Allora ogni elemento del gruppo $(Z_p, \cdot)$ ha inverso modulo p. In questo gruppo, ogni elemento ha un inverso distinto, eccetto quegli elementi che sono inversi di loro stessi, ossia quegli $a : a^2 \equiv 1 \pmod{p}$. Questa congruenza implica che

$$a^2 - 1 \equiv 0 \pmod{p} \implies (a-1)(a+1) \equiv 0 \pmod{p}$$

  ossia $a \equiv \pm 1 \pmod{p}$. Da questo, si ricava che gli unici elementi che sono inversi di loro stessi sono 1 e $p-1$. Ora, visto che

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$$

  si ha che

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (a_1 a_1^{-1}) \cdot \ldots \cdot (a_k a_k^{-1}) \equiv (p-1) \equiv -1 \pmod{p}$$

  dove si sono riorganizzati gli elementi di Z_p a coppie di inversi.

- ($\Leftarrow$) Si procede per controposizione, cioè dimostrando che p non primo $\Rightarrow$ $(p-1)! \not\equiv -1 \pmod{p}$.

  Se p non è primo, allora $\exists a, b \in \{2, \ldots, p-1\} : p = ab$. Essendo $a, b < p$, significa che questi compaiono in $(p-1)!$ e, quindi, $ab \mid (p-1)!$, cioè $p \mid (p-1)!$, quindi

$$(p-1)! \equiv 0 \pmod{p}$$

□

1.6 Il teorema cinese del resto e classi di resto

1.6.1 Il teorema cinese del resto

Stabilisce una condizione per risolvere sistemi di congruenze. Si vuole risolvere un sistema del tipo

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases} \tag{1.6.1}$$

La soluzione della prima è data $x = a + km_1,\ k \in \mathbb{Z}$; inserendolo nella seconda (considerando k come variabile), si ottiene $a + km_1 \equiv b \pmod{m_2}$, da cui

$$m_1 k \equiv b - a \pmod{m_2} \implies km_1 - k'm_2 = b - a$$

che si sa avere soluzione (per th. 1.9) se e soltanto se $\gcd(m_1, m_2) \mid b - a$.

Si cerca di capire come trovare tutte le soluzioni una volta concluso che tale sistema ne ammette. A tale proposito, si considera una soluzione particolare k_0 di $km_1 \equiv b - a \pmod{m_2}$; quindi $x_0 = a + k_0 m_1$ risolve il sistema di partenza in eq. 1.6.1:

$$\begin{cases} x_0 \equiv a \pmod{m_1} \\ x_0 \equiv b \pmod{m_2} \end{cases}$$

Sia x_1 un'altra soluzione di tale sistema; prendendo la differenza, si ottiene:

$$\begin{cases} x_0 - x_1 \equiv 0 \pmod{m_1} \\ x_0 - x_1 \equiv 0 \pmod{m_2} \end{cases}$$

Quindi la differenza tra le soluzioni è sia multiplo di m_1 che di m_2. Il più piccolo intero che soddisfa questa condizione è chiamato *minimo comune multiplo* di m_1 e m_2 e si indica con $\operatorname{lcm}(m_1, m_2)$. Tutto questo si riassume nel seguente teorema.

Teorema 1.16 (Teorema cinese del resto)

Sia dato il sistema

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

Questo sistema ammette soluzione $\iff \gcd(m_1, m_2) \mid b - a$; in questo caso, data x_0 una soluzione, tutte le altre soluzioni del sistema sono della forma

$$x_0 + s \cdot \operatorname{lcm}(m_1, m_2),\ s \in \mathbb{Z}$$

Osservazione 1.13. Equivalentemente, si può scrivere che tutte le soluzioni del sistema sono le x tali che

$$x \equiv x_0 \pmod{\operatorname{lcm}(m_1, m_2)} \tag{1.6.2}$$

Si nota, infine, che esiste un'unica soluzione x tale che $0 \leq x < \operatorname{lcm}(m_1, m_2)$.

Quando i moduli delle equazioni sono primi fra loro, cioè dato il sistema

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

con $\gcd(m_1, m_2) = 1$, il sistema ammette sempre soluzione e ne esiste un'unica x_0 tale che $0 \leq x_0 \leq m_1 \cdot m_2$; tutte le altre sono i numeri della forma

$$x_0 + 1 \cdot m_1 \cdot m_2,\ q \in \mathbb{Z} \tag{1.6.3}$$

Il teorema cinese del resto è generalizzabile ed enunciabile nella sua forma più classica, che è la seguente.

Teorema 1.17 (Teorema cinese del resto classico)

Dato il sistema di congruenze

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

dove i moduli sono, a due a due, coprimi, cioè $\gcd(m_i, m_j) = 1,\ \forall i \neq j$. Il sistema ammette sempre soluzione ed esiste un'unica soluzione x_0 tale che $0 \leq x_0 < m_1 \cdot \ldots \cdot m_n$. Tutte le altre soluzioni sono numeri della forma

$$x_0 + q \cdot m_1 \cdot \ldots \cdot m_n,\ q \in \mathbb{Z}$$

Dimostrazione. Si mostra a partire dal caso di un sistema di due congruenze, procedendo per induzione. □

1.6.2 Classi di resto

I possibili resti della divisione euclidea per 10 sono $0, 1, 2, \ldots, 9$; ad esempio, i numeri che danno resto 1 sono $1, 11, 21, 31, \ldots, -9, -19, 29, \ldots$ e si indica con $[1]_{10}$ l'insieme di tutti questi numeri, cioè:

$$[1]_{10} = \{x \in \mathbb{Z} \mid x \equiv 1 \mod 10\} \tag{1.6.4}$$

In generale, si indica con $[i]_{10}$ l'insieme degli interi che danno i come resto da divisione euclidea per 10. Gli insiemi per $i = 0, \ldots, 9$ si chiamano *classi di resto modulo 10* e la loro unione coincide con $\mathbb{Z}$. L'insieme i cui elementi sono le classi di resto modulo 10 si indica con

$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, \ldots, [9]_{10}\} \tag{1.6.5}$$

Su questo insieme, si possono definire una somma e una moltiplicazione, ma prima è necessario estendere la notazione sviluppata finora perché al momento $[11]_{10}$ non è ben definito. Si sceglie di prendere $[11]_{10} = [1]_{10}$, o anche $[127]_{10} = [7]_{10}$ e, più in

generale, $[s]_{10} = [i]_{10}$ qualora $s \equiv i \pmod{10}$.

In questo modo, la somma e il prodotto di elementi di $\mathbb{Z}_{10}$ sono definiti come:

$$\begin{aligned} [a]_{10} \cdot [b]_{10} &= [ab]_{10} \\ [a]_{10} + [b]_{10} &= [a+b]_{10} \end{aligned} \tag{1.6.6}$$

Esempio 1.2. Si ha:

$$\begin{aligned} [7]_{10} \cdot [5]_{10} &= [35]_{10} = [5]_{10} \\ [6]_{10} + [8]_{10} &= [14]_{10} = [4]_{10} \end{aligned}$$

In realtà, la verifica di avere definiti una buona somma e una buona moltiplicazione richiede la verifica che se $[a]_{10} = [a']_{10}$, $[b]_{10} = [b']_{10}$, allora

$$\begin{aligned} [a]_{10} \cdot [b]_{10} &= [a']_{10} \cdot [b']_{10} \\ [a]_{10} + [b]_{10} &= [a']_{10} + [b']_{10} \end{aligned}$$

Dimostrazione. DA DIMOSTRARE! *Suggerimento:* da $[a']_{10} = [a]_{10} \Rightarrow a' = a + 10k$ per qualche k e l'analogo vale per b'. Per la moltiplicazione, per esempio:

$$[a']_{10} \cdot [b']_{10} = [(a+10k)(b+10t)]_{10} = [ab + 10bk + 10at + 100kt]_{10} = [ab]_{10} = [a]_{10} \cdot [b]_{10}$$

□

Con queste operazioni, $\mathbb{Z}_{10}$ è un anello commutativo con unità; si nota che tali operazioni soddisfano la proprietà commutativa, associativa, distributiva, esistenza dell'elemento neutro e dell'opposto rispetto alla somma, eccetera. Una novità, invece, è che $[2]_{10} \cdot [5]_{10} = [10]_{10} = [0]_{10}$, cioè il prodotto di due numeri non-nulli può fare zero: in questo caso, ad esempio, si dirà che $[2]_{10}, [5]_{10}$ sono divisori dello zero in $\mathbb{Z}_{10}$.

Questo discorso si può generalizzare per $m \in \mathbb{Z}^+$, cioè per $i = 0, 1, \ldots, m-1$, si definisce la classe di resto $[i]_m = \{x \in \mathbb{Z} \mid x \equiv i \pmod{m}\}$. Come nel caso $m = 10$, le classi di resto forniscono una partizione di $\mathbb{Z}$, cioè sono a due a due disgiunte e la loro unione restituisce proprio $\mathbb{Z}$. Si indica con $\mathbb{Z}_m$ o $\mathbb{Z}/m\mathbb{Z}$ l'insieme di queste classi:

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\} \tag{1.6.7}$$

che ha, dunque, cardinalità m. In modo del tutto analogo, si prende $[i]_m = [s]_m$ qualora $s \equiv i \pmod{m}$ e si definiscono le operazioni

$$\begin{aligned} [a]_m \cdot [b]_m &= [a']_m \cdot [b']_m \\ [a]_m + [b]_m &= [a']_m + [b']_m \end{aligned}$$

Verificando come nel caso precedente che sono ben definite, si ottiene che $\mathbb{Z}_m$ è un anello commutativo con unità.

Osservazione 1.14. Il piccolo teorema di Fermat si può esprimere in modo equivalente tramite le classi di resto: dato p primo e la classe $[a]_p$ in $\mathbb{Z}_p$, con $[a]_p \neq [0]_p$, vale:

$$\left([a]_p\right)^{p-1} = [1]_p \tag{1.6.8}$$

Tramite questa osservazione, si vede che esiste un intero minimo $b \in \mathbb{Z}^+$ tale che $[a]_p^b = [1]_p$, con $b \leq p-1$; in questo caso, b sarà l'ordine moltiplicativo di $[a]_p$ in $\mathbb{Z}_p$. Questo b ha la proprietà per cui se $m \in \mathbb{Z}^+$ tale che $[a]_p^m = [1]_p$, allora $b|m$; in particolare, $b|p-1$.

Dimostrazione. Per vederlo, si usa la divisione euclidea per scrivere $m = qb + r$ e si ricava che $[a]_p^r = [1]_p$; a questo punto, si vede che deve essere $r = 0$ altrimenti verrebbe contraddetta la minimalità di b. □

1.7 La funzione di Eulero

Definizione 1.9 (Funzione di Eulero)

La funzione ϕ di Eulero è definita come

$$\phi : \mathbb{N}^{>0} \to \mathbb{N}^{>0} \qquad \phi(n) = \#\{a \leq n \mid \gcd(a,n) = 1\}$$

ossia rappresenta il numero degli interi positivi minori o uguali ad n che sono anche coprimi con n stesso.

Tramite questa, si enuncia un teorema che è la generalizzazione del piccolo teorema di Fermat.

Teorema 1.18

Sia $m \in \mathbb{Z}^{>0}$ e $a \in \mathbb{Z}$ tale che $\gcd(a,m) = 1$; allora

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Dimostrazione. Se $m = 1$, è ovvio perché tutti i numeri sono congrui fra loro modulo 1. Si può assumere, allora, $m \geq 2$ e si considerano le classi di resto $[a^0], [a^1], \ldots$; visto che queste sono le classi di resto modulo m, devono essere tutte diverse fino a un certo k, che è il più piccolo numero per cui una classe di resto si ripete: $[a^j] = [a^k] \Rightarrow j = 0$, altrimenti $[a^{j-1}] = [a^{k-1}]$ che è assurdo perché k era il più piccolo. Quindi $[a^k] = [a^0]$, cioè $a^k \equiv 1 \pmod{m}$. Si nota che se a è coprimo con m, allora anche tutte le sue potenze lo sono, il che vuol dire che le classi di resto distinte sono, al massimo, tante quante $\phi(m)$, cioè $k \leq \phi(m)$.

Se $k = \phi(m)$, il teorema è dimostrato. Si assume, altrimenti, che sia $k < \phi(m)$ e che sia $b < m$ un intero coprimo con m tale che $[b] \notin \left\{[a^0], [a^1], \ldots, [a^{k-1}]\right\}$; allora gli elementi $[ba^0], \ldots, [ba^{k-1}]$ sono tutti distinti fra loro e dai precedenti perché,

essendo b corpimo con m per assunzione, se fosse $[ba^s] = [ba^t]$ per qualche $0 \leq s, t < k$, si avrebbe $[a^s] = [a^t]$ per le regole di divisione delle congruenze, da cui $s = t$. Invece, se fosse $[ba^s] = [a^t]$ per s, t come prima, moltiplicando per a^{k-s} (che è sempre coprimo con m), si ottiene $[b] = [a^{k-s+t}]$, il che è assurdo per costruzione di b.

In questo modo, si hanno $2k$ elementi distinti fra le $\phi(m)$ classi di resto coprime con m; se $\phi(m) = 2k$, il teorema è dimostrato, altrimenti si ripete il procedimento finché non si esauriscono le classi di resto, ottenendo $kd = \phi(m)$ per qualche intero $d > 0$. A questo punto:

$$a^{\phi(m)} \equiv a^{kd} \equiv (a^k)^d \equiv 1^d \equiv 1 \pmod{m}$$

che dimostra il teorema. □

Osservazione 1.15. Si nota che per $m = p$ primo, si ritrova l'enunciato del piccolo teorema di Fermat, visto che $\phi(p) = p - 1$.

Vista l'importanza della funzione ϕ, si cerca un modo per poterla calcolare efficacemente.

Definizione 1.10 (Funzione aritmetica moltiplicativa)

Una funzione $f : \mathbb{N}^{>0} \to \mathbb{N}^{>0}$ si dice *aritmetica moltiplicativa* se $\forall a, b \in \mathbb{Z} : \gcd(a, b) = 1 \Rightarrow f(ab) = f(a)f(b)$.

Proposizione 1.3

La funzione di Eulero ϕ è aritmetica moltiplicativa.

Dimostrazione. Si nota, preliminarmente, che dati s, t, m interi, con $m > 0$, tali che $s \equiv t \pmod{m}$, si ha che s è coprimo con m se e solo se lo è t, visto che la congruenza è una relazione di equivalenza.

Sia, ora, $u \in \mathbb{Z}^{>0}$ coprimo con ab e $u < ab$; allora u è, in particolare, coprimo sia con a che con b, quindi risolve un sistema del tipo

$$\begin{cases} x \equiv v \pmod{a} \\ x \equiv w \pmod{b} \end{cases}$$

con $v \in \mathbb{Z}^{>0}$ coprimo con a e $v < a$ e $w \in \mathbb{Z}^{>0}$ coprimo con b e $w < b$. Viceversa, per il teorema cinese del resto, ogni sistema del genere ha una sola soluzione intera positiva minore di ab e, essendo coprima con a e con b, lo è anche con ab. Quindi i numeri interi positivi coprimi con ab e minori di ab sono tanti quanti i sistemi della forma di quello sopra, che sono $\phi(a)\phi(b)$, cioè il prodotto delle possibili scelte di v e w. □

Teorema 1.19

Sia $m \in \mathbb{Z}^{>0}$; se $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ è la sua decomposizione in fattori primi, allora:

$$\phi(m) = \left(p_1^{a_1} - p_1^{a_1-1}\right) \cdots \left(p_k^{a_k} - p_k^{a_k-1}\right)$$

Dimostrazione. Dalla proposizione precedente, si sa che $\phi(m)$ è il prodotto dei $\phi(p_i^{a_i})$; si deve, dunque, capire quanto vale $\phi(p^n)$, con p numero primo. Si nota che gli interi positivi minori di p^n sono tutti primi con p^n, tranne quelli che sono multipli di p; tuttavia, i multipli di p minori di p^n sono proprio p^{n-1}, quindi $\phi(p^n) = p^n - p^{n-1}$. □

Esempio 1.3. Con la teoria finora sviluppata, si può calcolare subito la classe di resto di 2^{365} modulo 225; visto che $\phi(225) = (25-5)(9-3) = 120$, per il teorema 1.18, si ha:

$$2^{120} \equiv 1 \pmod{225}$$

quindi

$$2^{365} \equiv (2^{120})^3 \cdot 2^5 \equiv 2^5 \equiv 32 \pmod{225}$$

Si nota che $\phi(m)$ non è il minimo intero che soddisfa il teorema 1.18; infatti, per questo teorema, si ha $2^8 \equiv 1 \pmod{15}$, ma, d'altra parte, vale anche $2^4 \equiv 1 \pmod{15}$. Questo si ha perché 1^n è congruo a 1 modulo m per qualunque n; inoltre, se $m > 2$, si ha $\phi(m) \neq 1$.

2 Teoria dei gruppi

2.1 Introduzione

Definizione 2.1 (Gruppo)

Un *gruppo* G è un insieme su cui è definita una *legge di composizione* $* : G \to G$ che soddisfa le seguenti condizioni per gli elementi di G:

GR 1. $(x * y) * z = z * (y * z)$ (*associatività*);

GR 2. $\exists e \in G : x * e = e * x = x$ (elemento neutro);

GR 3. $\forall x \in G$, $\exists y \in G$ tale che $x * y = y * x = e$ (elemento inverso).

Quando $*$ è la moltiplicazione, G si dice **gruppo moltiplicativo**; quando $*$ è l'addizione, G si dice **gruppo additivo**.

Definizione 2.2 (Gruppo commutativo)

Un insieme G è detto *gruppo commutativo* se è un gruppo e se soddisfa ulteriormente

$$x * y = y * x,\ \forall x, y \in G$$

L'elemento neutro di ciascun gruppo è unico.

Dimostrazione. Sia e' un altro elemento neutro; si nota che: $e = ee' = e'$. □

L'elemento inverso di ciascun elemento di un gruppo G è unico.

Dimostrazione. Siano y, y' gli elementi inversi di x; allora: $e = xy \implies y'e = y'xy \Rightarrow y' = y$. □

Questo elemento inverso si indica con x^{-1}; per gruppo additivo, si indicherà con $-x$.

Esempio 2.1. I numeri reali $\mathbb{R}$ e i numeri complessi $\mathbb{C}$ sono entrambi gruppi additivi. I numeri reali diversi da 0, $\mathbb{R}^*$, e i numeri complessi diversi da 0, $\mathbb{C}^*$, sono gruppi moltiplicativi.

Esempio 2.2. L'insieme dei numeri complessi di modulo 1, $\mathcal{S} := \{z \in \mathbb{C} : |z| = 1\}$, è un gruppo moltiplicativo.

Definizione 2.3 (Prodotto diretto)

Siano $G_1, \ldots, G_n$ dei gruppi; si definisce *prodotto diretto* l'insieme

$$G_P = \prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$$

e contiene tutte le n-uple $(x_1, \ldots, x_n)$, $x_i \in G_i$.

Prendendo un prodotto diretto di gruppi ed equipaggiandolo con il prodotto componente per componente, dove l'elemento unità è $(e_1, \dots, e_n)$, con e_i unità di G_i, si ottiene un gruppo moltiplicativo.

Definizione 2.4 (Gruppo finito)

Un gruppo G si dice *finito* se ha un numero limitato di elementi; si chiama **ordine** il numero di elementi di tale gruppo e si indica con $|G|$.

Definizione 2.5 (Sottogruppo)

Sia G un gruppo e $H \subset G$ un sottoinsieme di G. Si dice che H è un sottogruppo di G se:

- $e \in H$;
- $\forall x, y \in H,\ x * y \in H$;
- $\forall x \in H,\ x^{-1} \in H$.

Definizione 2.6 (Generazione di un sottogruppo)

Sia $S = \{x_1, \dots, x_n\} \subset G$ un sottoinsieme di un gruppo G; l'insieme $H := \{x \in G : x = x_1 * \dots * x_n\} \cup \left\{x^{-1} \in G : x \in S\right\} \cup \{e \in G\}$ è un sottogruppo di G ed è detto *generato* da S, dove gli elementi di S sono detti i *generatori di* H.

In questo caso, si scriverà che $H = \langle S \rangle \equiv \langle x_1, \dots, x_n \rangle$.

Esempio 2.3. Si nota che $\{1\}$ è un generatore per il gruppo additivo degli interi, visto che ogni $z \in \mathbb{Z} \setminus \{0\}$ si può scrivere come $1 + 1 + \dots + 1$, o $-1 - 1 - \dots - 1$, mentre l'elemento neutro ne fa parte per definizione.

Definizione 2.7 (Centro di un gruppo)

Sia G un gruppo; si definisce il *centro di* G come l'insieme

$$Z(G) := \{g \in G \mid gh = hg,\ \forall h \in G\}$$

cioè è composto da tutti gli elementi di G che commutano con tutti gli altri elementi di G.

Proposizione 2.1

$Z(G)$ è un sottogruppo di G.

Dimostrazione. Intanto $e \in Z(G)$ perché l'unità rispetto all'operazione di G commuta con tutti gli altri elementi del gruppo; poi si nota che $Z(G)$ è chiuso sotto tale operazione perché se $h, k \in Z(G)$ e $g \in G$:

$$(hk)g = hgk = g(hk)$$

Infine, per $h \in Z(G)$, anche $h^{-1} \in Z(G)$ perché, dato $g \in G$:

$$g = h^{-1}hg = h^{-1}gh \iff [h^{-1}, g] = 0$$

□

Ora si definisce una notazione per indicare una ripetizione dell'operazione di composizione con lo stesso elemento. In generale, si scriverà:

$$x^n \equiv \underbrace{x * x * \ldots * x}_{n \text{ volte}} \tag{2.1.1}$$

Se $n = 0$, si definisce $x^n = e$; invece, se $n = -m$, si ha la seguente definizione:

$$x^{-m} = (x^{-1})^m$$

Allora si possono verificare le seguenti:

- $x^{n+m} = x^n x^m$;
- $x^{-m}x^n = x^{n-m}$;
- $(x^n)^m = x^{nm}$.

Queste sono direttamente valide per la moltiplicazione, mentre per l'addizione si ha un qualcosa di analogo. Per cominciare $x^n \equiv nx$ nel caso dell'addizione, per definizione. Conseguentemente, le regole soddisfatte sono le seguenti:

$$(m+n)x = mx + nx \; ; \;\; (mn)x = m(nx)$$

Sia, G un gruppo e sia $a \in G$. Si definisce il sottogruppo H di G come quell'insieme avente tutti elementi del tipo a^n, $\forall n \in \mathbb{Z}$. In questo senso, H è generato da a. Per mostrare che è un gruppo, si nota che $e \in H$ perché $e = a^0$; dati, poi, $a^n, a^m \in H$, anche $a^{n+m} \equiv a^n a^m \in H$ perché $n + m \in \mathbb{Z}$. Infine, l'inverso di ciascun elemento a^n appartiene ad H perché $(a^n)^{-1} \equiv a^{-n}$, che appartiene ad H perché $-n \in \mathbb{Z}$.

Definizione 2.8 (Gruppo ciclico)

Sia G un gruppo; si dice che G è *ciclico* se esiste $a \in G : \forall g \in G,\ g = a^n$, per qualche intero n.

Riprendendo l'esempio 2.3, $\mathbb{Z}$ è un gruppo additivo ciclico, con generatore 1. Visto che un sottogruppo di Z è quello che si è chiamato *ideale*, si ha la seguente.

Proposizione 2.2

Sia H un sottogruppo di $\mathbb{Z}$. Se H non è il sottogruppo banale, sia d il più piccolo intero in esso contenuto; allora H contiene tutti elementi della forma nd, con $n \in \mathbb{Z}$, pertanto H è ciclico.

Sia G un gruppo ciclico e sia $a \in G$ il suo generatore; si hanno due casi possibili.

- *Caso 1*: non esiste $n \in \mathbb{Z}^{>0} : a^n = e$.

  Allora per ogni intero $n \neq 0$, $a^n \neq e$ e, allora, G si dice **infinitamente ciclico**, o che a ha **ordine infinito** perché ogni elemento $a^n \in G$ è distinto dall'altro.

  Dimostrazione. Si assume $a^r = a^s$ per qualche coppia di interi r, s; allora $a^{s-r} = e \Rightarrow s - r = 0 \Rightarrow r = s$. □

- *Caso 2*: $\exists m \in \mathbb{Z}^{>0} : a^m = e$.

  In questo caso, a ha **ordine finito**. Evidentemente, il gruppo è finito perché i suoi elementi si ripetono periodicamente.

  Sia J l'insieme degli $n \in \mathbb{Z}$ tali che $a^n = e$; allora J è un sottogruppo di $\mathbb{Z}$.

  Dimostrazione. Si ha $0 \in J$ perché $a^0 = e$ per definizione. Se $m, n \in J$, allora $a^{m+n} = a^m a^n = e \Rightarrow m + n \in J$. Infine, visto che $a^{-m} = (a^m)^{-1} = e$, anche $-m \in J$. □

Per il teorema 1.4, il più piccolo intero positivo contenuto in J genera J stesso; allora, per definizione, d è il più piccolo intero tale che $a^d = e$.

Definizione 2.9 (Periodo di un elemento)

Il più piccolo intero d tale che $a^d = e$ viene chiamato **periodo** di a. In quanto tale, se $a^n = e$ per qualche intero n, allora $n = ds$, per qualche intero s.

Osservazione 2.1. Alcune volte, il periodo di un elemento di dice anche ordine e si indica con $o(g)$, $g \in G$.

Teorema 2.1

Sia G un gruppo e sia $a \in G$ un elemento di periodo d; allora a genera il sottogruppo ciclico di ordine d, i cui elementi sono $e, a, \ldots, a^{d-1}$.

Dimostrazione. Per mostrare l'esistenza di tale sottogruppo, si nota che per $a \in G$, di periodo d, e per generico $n \in \mathbb{Z}$, l'algoritmo euclideo afferma che $n = qd + r$, con $q, r \in \mathbb{Z}$ e $0 \leq r < d$, per cui vale $a^n = a^r$.

Ora si mostra che gli elementi sono distinti. Se fosse $a^r = a^s$, con $0 \leq r, s \leq d - 1$ e, per assunzione, $r \leq s$, allora $a^{s-r} = e$; però $0 \leq s - r < d$, quindi bisogna avere $s - r = 0$, da cui $r = s$. □

2.2 Mappe tra gruppi

Dati S, S' due insiemi, una mappa fra questi è indicata con $f : S \to S'$; per $x \in S$, si indica con $f(x) \in S'$ l'immagine di x attraverso la mappa f. Per definire l'immagine di x attraverso f, si usa anche la notazione $x \mapsto f(x)$.

Data $f : S \to S'$ e $T \subset S$, si può definire una mappa che è la restrizione di f a T, assegnando $x \mapsto f(x)$, $\forall x \in T \subset S$; questa si indica con $f|_T : T \to S'$.

Una mappa $f : S \to S'$ si dice **iniettiva** se $\forall x, y \in S,\ x \neq y \Rightarrow f(x) \neq f(y)$. Una mappa si dice **suriettiva** se $\forall y \in S', \exists x \in S : f(x) = y$. Infine, f è **biettiva** se è sia iniettiva che suriettiva. Il fatto che f sia biettiva permette di individuare univocamente il suo inverso, la cui esistenza è assicurata dalla suriettività, mentre l'unicità dall'iniettività.

Definizione 2.10 (Mappa inclusione)

Sia S un insieme e $T \subset S$; la mappa identità di T, id_T, vista come mappa $\mathrm{id}_T : T \to S$ è chiamata *inclusione* e si indica con il simbolo $T \hookrightarrow S$.

Definizione 2.11 (Composizione)

Date due mappe $f : S \to T$, $g : T \to U$, si definisce la *mappa composta* come:

$$g \circ f : S \to U,\ (g \circ f)(x) = g\Big(f(x)\Big)$$

Va notato che la composizione *non* è commutativa[1], invece è, per definizione, associativa[2].

Proposizione 2.3

Siano S, T, U insiemi e siano $f : S \to T$, $g : T \to U$ due mappe; allora:

- f, g iniettive $\Rightarrow g \circ f$ iniettiva;
- f, g suriettive $\Rightarrow g \circ f$ suriettiva.

Definizione 2.12 (Mappa inversa)

Data $f : S \to S'$ una mappa; la sua inversa è la mappa $f^{-1} : S' \to S$ tale che

$$(f \circ f^{-1})(x') = \mathrm{id}_{S'};\ (f^{-1} \circ f)(x) = \mathrm{id}_S$$

Indicare l'inversa di f con f^{-1} presuppone che l'inversa sia unica, e infatti è così.

Dimostrazione. Sia $f : S \to S'$ e siano g_1, g_2 due mappe inverse per f; ma allora:

$$\mathrm{id}_{S'}(x') = (f \circ g_1)(x') \implies (g_2 \circ \mathrm{id}_{S'})(x') \equiv g_2 = g_2 \circ (f \circ g_1) = (g_2 \circ f) \circ g_1 \equiv g_1$$

□

Proposizione 2.4

Sia $f : S \to S'$; allora f è biettiva se e solo se f ha un'inversa.

Dimostrazione. Si divide la dimostrazione nelle due implicazioni.

[1] se $f(x) = x^2$ e $g(x) = x + 1$, si ha $g \circ f = x^2 + 1$, mentre $f \circ g = (x+1)^2$.

[2] Infatti, se f, g, h sono tre mappe tali per cui $h(g(f(x)))$ è ben definita, allora si ha $h \circ \Big(g \circ f\Big) = h \circ (g(f(x)) = h(g(f(x)))$, ma anche $(h \circ g) \circ f = (h \circ g)\Big(f(x)\Big) = h(g(f(x)))$.

- ($\Rightarrow$) Si assume che f sia biettiva e si mostra che ha un'inversa.

  La mappa f è tale che $\forall x' \in X', \exists! x \in X : f(x) = x'$; la mappa $x' \mapsto x$ è, allora, ben definita e questa coincide con l'inversa.

- ($\Leftarrow$) Si assume che f abbia un'inversa e si mostra che è biettiva.

  Per l'iniettività, si nota che se $x_1 \neq x_2$, allora deve essere anche $x_1' = f(x_1) \neq f(x_2) = x_2'$, altrimenti, se si avesse $f(x_1) = f(x_2) = x'$, $f^{-1}(x')$ non sarebbe una mappa ben definita perché ad un singolo elemento, ne fa corrispondere due.

  Per la suriettività, il discorso è analogo: $f^{-1} : S' \to S$ non sarebbe ben definita se si avesse $x_0' \in S' : \nexists x \in X,\ f(x) = x_0'$, allora non varrebbe $(f \circ f^{-1})(x_0') = \mathrm{id}_{S'}$.

□

Nonostante la precedente proposizione, la notazione f^{-1} si usa anche quando $f : X \to Y$ non ha propriamente un'inversa. In questo caso, f^{-1} è definita come una mappa tra l'insieme dei sottoinsiemi di Y e l'insieme dei sottoinsiemi di X. Così facendo, si rende possibile avere sempre una f^{-1} perché il suo risultato può essere l'insieme vuoto (nel caso in cui f non sia suriettiva), oppure un insieme composto da più elementi nel caso in cui f non sia iniettiva.

Definizione 2.13 (Sistemi di coordinate)

Siano gli $Y_1, \ldots, Y_n$ degli insiemi; si definisce sistema di coordinate una mappa

$$f : X \to \prod_{i=1}^{n} Y_i = Y_1 \times \ldots \times Y_n,\ f(x) = \Big(f_1(x), \ldots, f_n(x)\Big)$$

dove $f_i : X \to Y_i,\ i = 1, \ldots, n$.

2.3 Omomorfismi, isomorfismi e automorfismi

Definizione 2.14 (Omomorfismo)

Dati G, G' due gruppi, un omomorfismo $f : G \to G'$ è una mappa che conserva le operazioni di gruppo, cioè

$$\forall x, y \in G,\ f(x *_G y) = f(x) *_{G'} f(y)$$

con $*_G$, $*_{G'}$ leggi di composizione, rispettivamente, di G e G'.

Si ometteranno i pedici alle leggi di composizioni, ma la distinzione è sottintesa. Per brevità, invece di specificare che in $f : G \to G'$, G e G' sono gruppi, si dirà che $f : G \to G'$ è un *omomorfismo di gruppi*.

Esempio 2.4. Sia G un gruppo commutativo; allora la mappa $x \mapsto x^{-1} : G \to G$ è un omomorfismo. Si nota che la richiesta che G sia commutativo è fondamentale perché si abbia tale omomorfismo; infatti, $(x*y)^{-1} = x^{-1}*y^{-1}$ solamente se G è commutativo, altrimenti $x*y*(x*y)^{-1} = e \neq x*y*x^{-1}*y^{-1}$.

Esempio 2.5. La mappa $x \mapsto e^x : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ è un omomorfismo, infatti:

$$x + y \mapsto e^{x+y} = e^x \cdot e^y$$

Questo è un esempio in cui le leggi di composizione di gruppo sono diverse perché i due gruppi sono fondamentalmente diversi.

Proposizione 2.5

Siano G, H due gruppi, con $H = \prod_{i=1}^{n} H_i$. La mappa $f : G \to H$ è un omomorfismo se e soltanto se $\forall i,\ f_i$ è un omomorfismo.

Proposizione 2.6

Sia $f : G \to G'$ un omomorfismo di gruppi. Allora f conserva l'unità, nel senso che $f(e) = e'$, e conserva l'inversa, nel senso $f(x^{-1}) = f(x)^{-1}$.

Dimostrazione. Per la prima, si nota che $f(e) = f(ee) = f(e) * f(e)$. Moltiplicando (nel senso della legge $*_{G'}$) ambo i membri per $f(e)^{-1}$, si ottiene $e' = f(e)$.

Per la seconda, sia $x \in G$ tale che $\exists f^{-1}(x)$; allora $e' = f(x * x^{-1}) = f(x) * f(x^{-1})$. Moltiplicando ambo i membri a sinistra per $f(x)^{-1}$, si ottiene $f(x)^{-1} = f(x^{-1})$. □

Si nota che nella proposizione di sopra, si è usata la notazione $f(x)^{-1}$ per indicare l'elemento inverso nel gruppo, ossia quell'elemento tale che $f(x) *_{G'} f(x)^{-1} = e'$, ben diverso da $f^{-1}(x)$ funzione inversa, tale che $f \circ f^{-1} = \mathrm{id}$.

Proposizione 2.7

Siano $f : G \to G'$, $g : G' \to G''$ due omomorfismi di gruppi; allora la loro composizione $g \circ f : G \to G''$ è un omomorfismo di gruppi.

Dimostrazione. Per calcolo diretto, si ha: $(g \circ f)(x*y) = g\Big(f(x*y)\Big) = g\Big(f(x)*f(y)\Big) = g\Big(f(x)\Big) * g\Big(f(y)\Big)$. □

Proposizione 2.8

Dato $f : G \to G'$ un omomorfismo di gruppi, l'immagine di f è un sottogruppo di G'.

Dimostrazione. Dati due elementi $f(x) = x',\ f(y) = y' \in \mathrm{Im}(f) \subset G'$, si ha:

$$x' * y' = f(x) * f(y) = f(x * y) \in \mathrm{Im}(f)$$

Quindi $\mathrm{Im}(f)$ è chiuso rispetto alla legge di composizione definita in G'. Anche

l'inverso appartiene a $\mathrm{Im}(f)$ perché $x^{-1} \in G \Rightarrow f(x)^{-1} = f(x^{-1}) \in \mathrm{Im}(f)$. Infine, anche l'identità vi appartiene sempre perché $e \in G \Rightarrow e' = f(e) \in \mathrm{Im}(f)$. □

Definizione 2.15 (Kernel di un omomorfismo)

Sia $f : G \to G'$ un omomorfismo di gruppi; il suo kernel (o nucleo) è l'insieme

$$\mathrm{Ker}(f) := \{x \in G : f(x) = e' \in G'\}$$

Proposizione 2.9

Il kernel di un omomorfismo di gruppi $f : G \to G'$ è un sottogruppo di G.

Dimostrazione. Se $x, y \in \mathrm{Ker}(f)$, allora $x*y \in \mathrm{Ker}(f)$ perché $f(x*y) = f(x)*f(y) = e'*e' = e'$. L'identità appartiene a $\mathrm{Ker}(f)$ perché $f(e) = e'$ e, per finire, se $x \in \mathrm{Ker}(f)$, anche x^{-1} vi appartiene perché $e' = f(e) = f(x * x^{-1}) = f(x) * f(x^{-1}) = e' * f(x^{-1}) \Rightarrow e' = f(x^{-1})$. □

Si considera, ora, un gruppo G e si prende un suo elemento $a \in G$; si nota che la mappa $n \mapsto a^n$ è un omomorfismo di $\mathbb{Z}$ in G. Questo è facile da dimostrare, ma più interessante è il fatto che il kernel di questo omomorfismo può essere composto o dal solo $0 \in \mathbb{Z}$, o è un sottogruppo generato dal periodo di a.

Proposizione 2.10

Sia $f : G \to G'$ un omomorfismo di gruppi; allora $\mathrm{Ker}(f) = \{e\}$ se e solo se f è iniettivo.

Dimostrazione. Si assume, quindi, che $\mathrm{Ker}(f) = \{e\}$ e si mostra che f è iniettiva. Dati $x, y \in G$, $x \neq y$, se per assurdo, si avesse $f(x) = f(y)$, allora $e' = f(x) * f(y)^{-1} = f(x * y^{-1}) \Rightarrow x * y^{-1} \in \mathrm{Ker}(f)$, con $x * y^{-1} \neq x * x^{-1} = e$ perché, per assunzione, $x \neq y$. Ne segue che f è iniettiva.

Il viceversa è banale perché se fosse $e \neq g \in \mathrm{Ker}(f)$, si avrebbe un assurdo dal momento che, per definizione di kernel, $f(g) = f(e) = e'$, dove e è l'unità di G ed e' è quella di G'. □

Un omomorfismo iniettivo fra due gruppi $G \to G'$ è chiamato **embedding** (o **iniezione**) e, come l'inclusione, si indica con $G \hookrightarrow G'$.

Proposizione 2.11

Sia $f : G \to G'$ un omomorfismo e sia $H' \subset G'$; prendendo $H = f^{-1}(H')$ come l'insieme delle $x \in G : f(x) \in H'$, allora H è un sottogruppo di G.

Si nota che nella proposizione sopra, per $H' = \{e'\}$, si ha $f^{-1}(H') \equiv \mathrm{Ker}(f)$.

Definizione 2.16 (Isomorfismo di gruppi)

Dato $f : G \to G'$ un omomorfismo di gruppi, si dice che è un *isomorfismo di gruppi* se esiste un altro omomorfismo di gruppi $g : G' \to G$ e tale che $f \circ g = \mathrm{id}_{G'}$ e $g \circ f = \mathrm{id}_G$. In tal caso, si dirà che $G \cong G'$.

Questo significa che se uno dei due ha delle proprietà esprimibili esclusivamente in termini delle operazioni di gruppo, allora anche ogni altro gruppo isomorfo a questo conserva le stesse proprietà. Alcune di queste sono:

- la ciclicità;
- l'ordine;
- l'essere abeliano.

Proposizione 2.12

Un omomorfismo di gruppi $f : G \to G'$ che è anche biettivo è un isomorfismo.

Dimostrazione. L'esistenza di $f^{-1} : G' \to G$ è assicurata dal fatto che f è biettiva. Si deve mostrare che f^{-1} è un omomorfismo.

Siano dati $x, y \in G' : f(x) = x',\ f(y) = y' \Rightarrow f(x * y) = x' * y'$, visto che f è un omomorfismo; allora si nota che:

$$f^{-1}(x' * y') = x * y = f^{-1}(x) * f^{-1}(y)$$

□

Dalla precedente proposizione, si ottiene il seguente teorema che permette di capire se un omomorfismo è un isomorfismo.

Teorema 2.2

Sia $f : G \to G'$ un omomorfismo di gruppi. Allora:

(a). se $\mathrm{Ker}(f) = \{e\} \implies f$ è un isomorfismo da $G \to f(G) \equiv \mathrm{Im}(f)$;

(b). $f : G \to G'$ è suriettiva e $\mathrm{Ker}(f) = \{e\}$, allora f è un isomorfismo da $G \to G'$.

Dimostrazione. Si è già dimostrato che se il nucleo di f è banale, allora f è iniettiva; chiaramente f è sempre suriettiva dall'insieme di partenza nella sua immagine, quindi la tesi è verificata dalla proposizione 2.12.

Sempre per la stessa, segue direttamente il punto (b). □

Definizione 2.17 (Automorfismo)

Un *automorfismo di gruppi* è un isomorfismo $f : G \to G'$ con $G' \equiv G$.

Si indica con $\mathrm{Aut}(G)$ l'insieme di tutti gli automorfismi definiti su G.

Definizione 2.18 (Traslazione)

Dato un gruppo G, la mappa che, per qualche $a \in G$, associa $x \mapsto a * x$, definita da $T_a : G \to G$, è chiamata *traslazione*. Questa, in particolare, è chiamata traslazione sinistra. La mappa inversa di una traslazione è $T_{a^{-1}}$, in quanto $x = a^{-1}ax$.

Si consideri la mappa che, per $a \in G$, associa $a \mapsto T_a : G \to \mathrm{Perm}(G)$; questa è un omomorfismo perché dati $a, b \in G$, si ha $T_{ab}(x) = abx = (T_a \circ T_b)(x)$, cioè $T_{ab} = T_a \circ T_b$. Evidentemente, questo isomorfismo è anche iniettivo perché per $a \neq b$, si ha $T_a \neq T_b$, pertanto $a \mapsto T_a$ risulta un isomorfismo su G, la cui immagine non è necessariamente coincidente con $\mathrm{Perm}(G)$.

Definizione 2.19 (Somma diretta)

Siano $B_1, \ldots, B_r$ dei sottogruppi di un gruppo abeliano additivo A; si dice che A è *somma diretta* di questi se

$$A = \bigoplus_{i=1}^{r} B_i = B_1 \oplus B_2 \oplus \ldots \oplus B_r$$

cioè se $\forall x \in A$, $x = \sum_{i=1}^{r} b_i$, $b_i \in B_i$ è scritto *univocamente* come somma di elementi dei B_i.

In generale, se A è un gruppo additivo abeliano, con B, C suoi sottogruppi, allora $B + C$ forma un sottogruppo di A, i cui elementi sono tutti della forma $b + c$, $b \in B$, $c \in C$.

Teorema 2.3

Sia A un gruppo abeliano; questo è somma diretta di suoi sottogruppi B, C se e soltanto se $A = B + C$ e $B \cap C = \{0\}$. Questo è vero se e soltanto se la mappa $(b, c) \mapsto b + c : B \times C \to A$ è un isomorfismo.

Per finire, si considera l'insieme degli omomorfismi tra due gruppi abeliani additivi A, B, indicato con $\mathrm{Hom}(A, B)$. È possibile rendere questo un gruppo, definendo $f + g : A \to B$, per $f, g \in \mathrm{Hom}(A, B)$, come

$$(f + g)(x) = f(x) + g(x), \ \forall x \in A$$

Dimostrazione. Si mostra che questo, così definito, è un gruppo. Intanto si osserva l'*associatività*:

$$\Big((f + g) + h\Big)(x) = (f + g)(x) + h(x) = f(x) + g(x) + h(x)$$
$$\Big(f + (g + h)\Big)(x) = f(x) + (g + h)(x) = f(x) + g(x) + h(x)$$

da cui $f + (g + h) = (f + g) + h$. Si ha anche l'elemento unità rispetto a $+$, indicato con 0, che ad ogni elemento di A, assegna l'elemento nullo di B, che risulta un omomorfismo.

Per finire, si definisce l'elemento $-f$ con la proprietà che $f+(-f)=0$ e si mostra che $f+g$ e $-f$ sono omomorfismi:

$$(f+g)(x+y)=f(x+y)+g(x+y)=f(x)+f(y)+g(x)+g(y)=(f+g)(x)+(f+g)(y)$$

e

$$(-f)(x+y)=-\Big(f(x+y)\Big)=-\Big(f(x)+f(y)\Big)=-f(x)-f(y)$$

Quindi $\mathrm{Hom}(A,B)$ è un gruppo. □

2.4 Permutazioni e gruppi simmetrici

Definizione 2.20 (Permutazione)

Sia S un generico insieme; è chiamata *permutazione* di S una mappa biettiva $f: S\to S$ e si indica con $\mathrm{Perm}(S)$ l'insieme delle permutazioni di S.

Le permutazioni dei numeri $1,2,\dots,n$ sono gli elementi di un gruppo, indicato con S_n, dove l'operazione è la legge di composizione di funzioni, come riportato di seguito.

Proposizione 2.13

L'insieme $\mathrm{Perm}(S)$ è un gruppo, la cui legge di composizione è data dalla composizione di mappe.

Dimostrazione. Si è già mostrato che la composizione di mappe è associativa e, chiaramente, esiste la permutazione identità che è id_S.

Inoltre, se f,g sono permutazioni, allora $g\circ f$, $f\circ g: S\to S$ e sono biettive, quindi sono permutazioni. Questo mostra che $\mathrm{Perm}(S)$ è chiuso sotto la composizione di mappe.

Infine, ogni permutazione f ha un'inversa f^{-1} perché f è biettiva per definizione. □

Questo risultato, più generale, afferma che l'insieme formato da qualunque permutazione su un insieme S è un gruppo, mentre i gruppi simmetrici S_n contengono solamente permutazioni dei primi n interi, cioè è il caso specifico di $S=\{1,\dots,n\}$. Generalmente, per la composizione di permutazioni, si scrive direttamente $\sigma\tau$, invece di $\sigma\circ\tau$.

Proposizione 2.14

Sia G un gruppo; l'insieme $\mathrm{Aut}(G)$, equipaggiato con la legge di composizione delle funzioni, è un sottogruppo di $\mathrm{Perm}(G)$.

Ora si caratterizzano le permutazioni nel caso del gruppo simmetrico S_n; una nota-

zione possibile è la seguente nel caso di $\tau \in S_9$:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 1 & 7 & 2 & 8 & 5 & 9 \end{pmatrix}$$

Tuttavia risulta ridondante perché basterebbe guardare la seconda riga, cioè invece di scrivere, per $\sigma \in S_n$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

si può semplicemente scrivere $\sigma = \sigma(1)\sigma(2)\dots\sigma(n)$. Nel caso della permutazione τ scritta sopra, si avrebbe $\tau = 346172859$.

Un altro modo di rappresentare una permutazione è la *decomposizione in cicli disgiunti*:

$$\sigma = (1,3,6,2,4)(5,7,8)(9)$$

manda 1 in 3, 3 in 6, 6 in 2 e 4 in 1 e così via per i cicli successivi. In pratica, ogni elemento viene mandato in quello che lo segue, tranne l'ultimo che viene mandato nel primo (da qui "cicli"). L'ultimo ciclo afferma che il 9 viene mandato in se stesso, cioè viene lasciato fisso; in questi casi, è consuetudine non indicare elementi del genere, quindi la permutazione sopra si scriverebbe come $\sigma = (1,3,6,2,4)(5,7,8)$.

Si può dimostrare che ciascuna permutazione si può sempre scrivere come decomposizione di cicli disgiunti; il termine *disgiunti*, infatti, si riferisce proprio al fatto che all'interno di ciascun ciclo, un numero compare una sola volta. Inoltre, questa decomposizione non è unica; riprendendo l'esempio di $\sigma = (1,3,6,2,4)(5,7,8)$, questa è scrivibile anche come $\sigma = (5,7,8)(1,3,6,2,4) = (7,8,5)(6,2,4,1,3)$.

Definizione 2.21 (Trasposizione)

Si dice che τ è una trasposizione se è una permutazione che scambia due interi e lascia gli altri fissati. Questo significa che dati $i, j \in S_n : i \neq j \Rightarrow \tau(i) = j,\ \tau(j) = i$ e $\forall k \in S_n, k \neq i, j,\ \tau(k) = k$.

Si vede che se τ è una trasposizione, allora $\tau^2 = \mathrm{Id}$; inoltre, vale il seguente. Le trasposizioni sono permutazioni relative decomponibili in 2-cicli.

Teorema 2.4

Ogni permutazione di S_n si scrive come prodotto di trasposizioni.

Dimostrazione. Si procede per induzione su n. Per $n = 1$, non c'è nulla da provare. Si assume che questo sia vero in generale per $n > 1$ e, in particolare, per $n-1$, quindi si dimostra che vale per n. Sia σ una permutazione di S_n tale che $\sigma(n) = k$ e sia τ una trasposizione tale che $\tau(k) = n$ e $\tau(n) = k$; allora $\tau\sigma$ è una permutazione tale che $\tau\sigma(n) = \tau(k) = n$, cioè lascia n fissato. Questo vuol dire che può essere vista come permutazione di S_{n-1} che, per induzione, si può scrivere come

prodotto di trasposizioni $\tau_1, \dots, \tau_s \in S_{n-1}$: $\tau\sigma = \tau_1\tau_2\cdots\tau_s$. Conseguentemente, si ha $\sigma = \tau^{-1}\tau_1\cdots\tau_s$, che è un prodotto di trasposizioni in S_n. □

Esempio 2.6. Si considera S_{10}; date $\sigma = (1,3,6,2,4,7)(5,8,10)$ e $\tau = (1,3)(2,9)$, calcolare la decomposizione in cicli di $\tau\sigma$.

Svolgimento. La composizione delle due può essere calcolata notando preliminarmente che τ non modifica il ciclo $(5,8,10)$ di σ; in pratica, τ agisce unicamente su $(1,3,6,2,4,7)$[a]:

$$\begin{aligned}(1,3)(2,9)\circ(5,8,10)(1,3,6,2,4,7) &= (5,8,10)(2,4,7,3,6,9)(1)\\ &= (5,8,10)(2,4,7,3,6,9)\end{aligned}$$

■

[a] Si ricorda che i cicli vanno applicati da sinistra verso destra.

2.5 Classi di coniugio

Definizione 2.22 (Coniugazioni)

Sia G un gruppo e sia $a \in G$; si definisce *coniugazione* la mappa $\mathfrak{c}_a : G \to G$ tale che $x \mapsto axa^{-1}$.

Proposizione 2.15

$\mathfrak{c}_a$ è un automorfismo di G, in particolare, si definisce **automorfismo interno**. La mappa $a \mapsto \mathfrak{c}_a$ è un omomorfismo di $G \to \mathrm{Aut}(G)$, la cui legge di composizione è la composizione di funzioni.

Dimostrazione. Dato $g \in G$, si nota che $\mathfrak{c}_g$ è bigettiva perché ha un inverso dato da $\mathfrak{c}_{g^{-1}}$. Per mostrare che è un omomorfismo, quindi un automorfismo, si prendono $h,k \in G$ e si vede che:

$$\mathfrak{c}_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = (ghg^{-1})(gkg^{-1}) = \mathfrak{c}_g(h)\mathfrak{c}_g(k)$$

□

Definizione 2.23 (Orbita rispetto al coniugio)

Dato G un gruppo e $\gamma \in G$, si definisce la *classe di coniugio* (o *orbita*) di γ l'insieme

$$\mathrm{Orb}(\gamma) = \left\{ g\gamma g^{-1} \mid g \in G \right\}$$

Le classi di coniugio formano una partizione di G, cioè ogni elemento di G appartiene ad una ed una sola classe di coniugio.

Dimostrazione. Si assume che esista un elemento comune ad entrambe le orbite $\mathrm{Orb}(\gamma_1)$

e $\mathrm{Orb}(\gamma_2)$, per esempio $g_1\gamma_1 g_1^{-1} = g_2\gamma_2 g_2^{-1}$. Da questo si ottiene che

$$\gamma_1 = (g_1^{-1}g_2)\gamma_2(g_2^{-1}g_1) = (g_1^{-1}g_2)\gamma_2(g_1^{-1}g_2)^{-1} = g'\gamma_2 g'^{-1} \iff \gamma_1 \in \mathrm{Orb}(\gamma_2)$$

Ma il fatto che $\gamma_1 \in \mathrm{Orb}(\gamma_2) \Rightarrow \mathrm{Orb}(\gamma_1) = \mathrm{Orb}(\gamma_2)$. Questo dimostra che ogni elemento di G può appartenere ad un'unica classe di coniugio, altrimenti due classi distinte coinciderebbero e sarebbero comunque una sola. □

Infatti, si può definire la relazione di equivalenza per cui $x \sim y \iff x = gyg^{-1}$ per $g \in G$, quindi il gruppo si partiziona sotto questa relazione di equivalenza.

Ora si studiano le classi di coniugio di S_n; per farlo, date le permutazioni σ e τ si usa la decomposizione in cicli:

$$\sigma = (a_1, a_2, \dots, a_{k_1})(b_1, b_2, \dots, b_{k_2})\cdots$$

Allora vale la seguente formula, utile per i calcoli:

$$\tau\sigma\tau^{-1} = \Big(\tau(a_1), \tau(a_2), \dots, \tau(a_{k_1})\Big)\Big(\tau(b_1), \dots, \tau(b_{k_2})\Big)\cdots \tag{2.5.1}$$

Esempio 2.7. Se $\sigma, \tau \in S_5$, con $\sigma = (1,3,5)(2,4)$ e $\tau = (1,2,4,5)$, allora

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

2.6 Classi laterali

Siano S, S' due sottoinsiemi di un gruppo $(G, *)$; il loro **prodotto** è:

$$S * S' = \{x \in G : x = s * s',\ s \in S,\ s' \in S'\}$$

Allora, se $S_1, S_2, S_3 \subset G$, vale $(S_1 * S_2) * S_3 = S_1 * (S_2 * S_3)$. Di seguito, alcune altre proprietà.

- Sia H sottogruppo di G; allora $H * H = H$.

  Dimostrazione. È sufficiente prendere l'elemento neutro di uno dei due e far variare tutti gli elementi dell'altro per ottenere tutto H. Non si può uscire da H perché H stesso è un gruppo, quindi è chiuso rispetto a $*$. □

- Sia $S \subset H$ un generico sottoinsieme e H come sopra; allora $S * H = H$.

  Dimostrazione. Corrisponde a traslare ciascun elemento di H, ma si riottiene comunque H. Per vederlo, sia $s \in S$ fissato; dato un generico $h_0 \in H$, si vuole mostrare che $\exists h \in H : s * h = h_0$.

Visto che H è un sottogruppo di G, H contiene l'inverso di qualunque suo elemento e di ogni elemento di S, pertanto è ben definito $h = s^{-1} * h_0$, che soddisfa la richiesta. □

- Dati $S_1, S_2, S_3 \subset G$, allora $S_1 * (S_2 \cup S_3) = S_1 * S_2 \cup S_1 * S_3$.

  Dimostrazione. Si indica con $S := S_1 * (S_2 \cup S_3)$ e con $\overline{S} := S_1 * S_2 \cup S_1 * S_3$.

  Un generico elemento di S è il prodotto tra $s_1 \in S_1$ e un altro elemento che sta in S_2 o in S_3. Un generico elemento di $\overline{S}$ è o il prodotto tra $s_1 \in S_1$ e $s_2 \in S_2$, o $s_1 \in S_1$ e $s_3 \in S_3$. Allora $S = \overline{S}$. □

Definizione 2.24 (Classe laterale)

Sia G un gruppo e sia H un suo sottogruppo. Dato $a \in G$, l'insieme di tutti gli elementi della forma ax, $x \in H$ è chiamato *classe laterale* di H in G.

Si indicherà con aH.

Si nota che, essendo in generale G non-commutativo, la scrittura $aH \neq Ha$; la prima si chiama *classe laterale sinistra*, mentre la seconda sarà la *classe laterale destra*.

Osservazione 2.2. Più precisamente dovrebbe essere $a * H$, ma si elimina $*$ per alleggerire la notazione. Nel caso della somma, diventerebbe $a + H$.

Teorema 2.5

Siano aH e bH due classi laterali di H in G: o le due classi laterali sono uguali, o non hanno alcun elemento in comune.

Dimostrazione. Si assume che $\exists x, y \in H : ax = by$. Allora si osserva che, essendo $xH = H = yH$:

$$aH = axH = byH = bH$$

□

È possibile decomporre un gruppo in classi laterali. Si considera il caso specifico di G gruppo finito; ogni elemento $x \in G$ appartiene ad una classe laterale, per esempio xH, con H sottogruppo di G. Allora, G si può scrivere come unione finita di classi laterali di H[1]:

$$G = \bigsqcup_{i=1}^{r} a_i H \tag{2.6.1}$$

dove ogni classe laterale è distinta dall'altra, altrimenti sarebbero uguali e non si sarebbe aggiunto nessun nuovo elemento di G. Ogni elemento ah, $h \in H$ è chiamato **rappresentante** della classe laterale aH.

[1] Il simbolo $\bigsqcup$ indica unione di insiemi disgiunti.

Lo stesso si può dire per gruppi infiniti, ma sono ammesse unioni di infinite classi laterali; indicando con I un certo insieme di indicizzazione potenzialmente infinito:

$$G = \bigsqcup_{i \in I} a_i H \tag{2.6.2}$$

con G finito o infinito.

Teorema 2.6

Sia G un gruppo e H un sottogruppo finito. Allora il numero di elementi di una certa classe laterale aH è il numero di elementi di H.

Dimostrazione. Siano $x, x' \in H : x \neq x'$; allora, $ax \neq ax'$ perché se fosse $ax = ax'$, si potrebbe moltiplicare ambo i membri per a^{-1} e ottenere $x = x'$, il che è falso per assunzione di partenza.

Ne segue che, prendendo $x_1, \ldots, x_n \in H$ tutti diversi, anche $ax_1, \ldots, ax_n$ sono diversi, quindi il numero di elementi di una classe coincide col numero di elementi di H. □

Dati G, H come al solito, si indica con G/H l'insieme di tutte le classi laterali sinistre di H in G. Si chiama **indice** il numero di tutte le distinte classi laterali di H in G e si indica con $(G : H)$. Se $|S|$ è il numero di elementi in S, allora $|(G/H)| = (G : H)$ e $|G| = (G : 1)$.

Teorema 2.7 (Teorema di Lagrange)

Sia G un gruppo finito e H un suo sottogruppo; allora

$$|G| = (G : H)|H|$$

Dimostrazione. Per il teorema 2.6, ciascuna classe ha lo stesso numero di elementi e ogni elemento di G deve essere contenuto in una classe laterale (ciò non toglie che più elementi di G siano nella stessa), visto che $e \in H$ e ogni elemento $g \in G$ si ottiene come $g * e$.

La relazione, allora, segue direttamente dal fatto che il numero complessivo di elementi contenuti nelle classi laterali è proprio il numero di elmenti per ciascuna classe, $|H|$, per il numero di classi, cioè $(G : H)$. □

Corollario 2.1

Sia G un gruppo finito e H un suo sottogruppo; allora $|H|$ divide $|G|$.

Corollario 2.2

Sia G un gruppo e $a \in G$ un suo elemento; il periodo di a, divide $|G|$.

Dimostrazione. Il periodo di a è il numero di elementi del sottogruppo generato da a stesso. □

Corollario 2.3

Sia G un gruppo finito e siano $K \subset H \subset G$ due sottogruppi; allora $(G : K) = (G : H)(H : K)$.

Dimostrazione. Applicando due volte Lagrange:

$$|G| = (G : H)|H| = (G : H)(H : K)|K|$$

Allo stesso tempo, sempre per Lagrange, $|G| = (G : K)|K|$, quindi:

$$(G : K)|K| = (G : H)(H : K)|K| \implies (G : K) = (G : H)(H : K)$$

□

Si considera d'esempio il gruppo S_n delle permutazioni di $\{1, \dots, n\}$. Sia H il sottogruppo di S_n che contiene tutte le permutazioni σ della forma $\sigma(n) = n$; questo, come sottogruppo, coincide con $S_{n-1}, n > 1$. Si studiano le classi laterali di H; più in dettaglio, vale il seguente.

Proposizione 2.16

Le sole classi laterali distinte di $H \equiv S_{n-1},\ n > 1$ come sottogruppo di S_n sono

$$\tau_1 H, \dots, \tau_n H \tag{2.6.3}$$

con $\tau_i(n) = i,\ \tau_i(i) = n$ e tutti gli altri interi sono lasciati invariati.

Dimostrazione. Per prima cosa, si mostra che ogni elemento $\sigma \in S_n$ è contenuto in una classe laterale. Intanto si nota che H coincide con $\tau_n H$ perché τ_n è l'identità per definizione; allora, si prende un elemento che non sta in H e si mostra che appartiene ad una classe laterale. Senza perdita di generalità, quindi, sia $\sigma \in S_n$: $\sigma(n) = i$; allora

$$\tau_i^{-1} \circ \sigma(n) = \tau_i^{-1}(i) = n$$

Questo significa che $\tau_i^{-1}\sigma \in H \implies \sigma \in \tau_i H$. Questo dimostra che $S_n/H \equiv \{\tau_i H\}_{i=1}^n$; manca da mostrare che queste sono tutte distinte.

Per vederlo, si assume $i \neq j$ e si nota che, $\forall \sigma \in H$, $\tau_i \circ \sigma(n) = \tau_i(n) = i$ e $\tau_j \circ \sigma(n) = j$, quindi $\tau_i H$ e $\tau_j H$ non possono avere elementi in comune, □

Vista la proposizione 2.16, il teorema di Lagrange permette anche di concludere che $|S_n| = n|S_{n-1}|$; per induzione, si mostra che, in generale:

$$|S_n| = n! \tag{2.6.4}$$

Teorema 2.8

Sia $f : G \to G'$ un omomorfismo di gruppi. Dato $a' \in \mathrm{Im}(f) \subset G'$, con $a' = f(a)$ per qualche $a \in G$, allora l'insieme degli elementi $x \in G : f(x) = a'$ coincide con la classe laterale $a\mathrm{Ker}(f)$.

Dimostrazione. L'idea è di mostrare che i due insiemi sono contenuti uno nell'altro.

Sia $x \in a\mathrm{Ker}(f)$, cioè per qualche $h \in \mathrm{Ker}(f)$, $x = ah$; allora:

$$f(x) = f(a) * f(h) = f(a)$$

cioè $x \in a\mathrm{Ker}(f) \implies x \in \{y \in G : f(y) = a'\}$.

Sia ora $x \in \{y \in G : f(y) = a'\}$; allora:

$$f(a^{-1}x) = f(a)^{-1} * f(x) = a'^{-1} * a' = e'$$

cioè $a^{-1}x \in \mathrm{Ker}(f)$, per esempio $h = a^{-1}x$, quindi $x = ah \implies x \in a\mathrm{Ker}(f)$. □

2.7 Gruppi ciclici finiti

Sia $o(x)$ l'ordine di un certo elemento $x \in G$, con G gruppo; per definizione, $x^{o(x)} = e$ ed è il più piccolo $n \in \mathbb{N}^{>0} : x^n = e$. Tutti gli elementi dell'insieme

$$\langle x \rangle = \left\{e, x, x^2, \dots, x^{o(x)-1}\right\}$$

sono diversi fra loro perché, altrimenti, esisterebbe $x^k = e$ con $k < o(x)$ che è assurdo. Questo insieme è quello generato da x ed è un sottogruppo ciclico di G, la cui cardinalità coincide proprio con $o(x)$; per il teorema di Lagrange: $o(x)$ divide $|G|$. Come altro corollario del teorema di Lagrange, quindi, si ha il seguente.

Corollario 2.4

Se $x \in G$, con $|G| < \infty$, si ha $x^{|G|} = e$.

Dimostrazione. Visto che $o(x)$ deve dividere $|G|$, si può scrivere che $|G| = ko(x)$, per qualche$k \in \mathbb{Z}$; da questo segue che: $x^{|G|} = x^{ko(x)} = \left(x^{o(x)}\right)^k = e^k = e$. □

Osservazione 2.3. Tramite questo, si può dare un'ulteriore dimostrazione del teorema 1.18; infatti, preso $a, m \in \mathbb{Z}^{>0}$: $\gcd(a, m) = 1$, l'elemento $[a]_m \in \mathbb{Z}_m^*$, per il corollario appena mostrato, è tale per cui

$$[a]_m^{\phi(m)} = [1]_m$$

visto che $\mathbb{Z}_m^*$ ha esattamente $\phi(m)$ elementi.

Dato, ora, un gruppo ciclico G, ci si chiede quanti elementi complessivamente esistano che siano tali da generare G stesso, visto che, per definizione, ne è assicurato *almeno uno*.

Proposizione 2.17

Sia G un gruppo ciclico di n elementi; allora ci sono esattamente $\phi(n)$ generatori.

Dimostrazione. Sia $g \in G$ un generatore; allora gli elementi di G sono della forma $g^i,\ 0 \leq i < n$. Indicando con d l'ordine di g^i, si sa per il teorema di Lagrange che $d \mid n$ e si osserva che $(g^i)^d = g^{id} = e$, quindi n divide di, visto che n è l'ordine di g. Se fosse $\gcd(i,n) = 1$, allora si dovrebbe avere che $n \mid d$, ossia che $n = d$, visto che n è l'ordine di G e d del sottogruppo generato da g^i. Questo permette di concludere che tutti gli elementi della forma g^i con $\gcd(i,n) = 1$ sono generatori di G, visto che hanno ordine n.

Se, invece, fosse $\gcd(i,n) > 1$, allora g^i non sarebbe un generatore perché non sarebbe possibile ottenere g come potenza di g^i; infatti, se $(g^i)^s = g \Rightarrow g^{is-1} = e$, allora risulterebbe che $n \mid is - 1$, cioè

$$is \equiv 1 \pmod{m}$$

Però questo non è possibile perché l'equazione

$$ix \equiv 1 \pmod{m}$$

non ha soluzione, essendo che $\gcd(i,n) > 1$. □

Lemma 2.1

Per ogni intero $n \in \mathbb{N}^{>0}$, si ha:

$$\sum_{d|n} \phi(d) = n$$

Dimostrazione. Si considera la seguente lista di n frazioni:

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$$

Si riducono queste frazioni ai minimi termini e si riportano in una lista separata; il numero di queste frazioni che rimane intatta è ottenuto dal numero di interi coprimi con n, quindi è esattamente $\phi(n)$.

Sia, ora, d un divisore di n: il numero di frazioni che, ridotte ai minimi termini, saranno della forma $\frac{j}{d}$ sono tutte quelle in cui $\gcd(j,d) = 1$, quindi sono $\phi(d)$.

Questo significa che le frazioni della lista originaria possono essere suddivise ed essere contate a gruppi a seconda del denominatore: per ogni gruppo

individuato dal denominatore d, il numero di frazioni di questo gruppo è $\phi(d)$, il che vuol dire che n, cioè il numero totale di frazioni, è proprio ottenuto da $\sum_{d|n} \phi(d)$. □

Proposizione 2.18

Sia G un gruppo ciclico di n elementi; in G, ci sono esattamente $\phi(d)$ elementi di ordine d, con d intero che divide n.

Dimostrazione. Il caso $d = n$ è già stato mostrato precedentemente. Sia, allora, $d < n$; se g è un generatore di G, si considera l'elemento $g^{n/d}$ (con $d \mid n$ per assunzione). Il sottogruppo generato da $g^{n/d}$ è, evidentemente, di ordine d: $(g^{n/d})^d = g^n = e$; per la proposizione 2.17, questo sottogruppo ha esattamente $\phi(d)$ elementi di ordine d.

Questa procedura si può ripetere per ogni $d < n : d \mid n$, arrivando a scrivere un numero di elementi di G pari a $\sum_{d|n} \phi(d)$; per il lemma precedente, si sa che questa somma è pari proprio a n, quindi si sono elencati tutti gli elementi di G. Questo significa che se d divide n, il numero di elementi di ordine d in G sono esattamente quelli ottenuti dallo studio del sottogruppo $g^{n/d}$, cioè non ve ne sono altri. □

La seguente proposizione, invece, permette una caratterizzazione anche dei gruppi ciclici infiniti.

Proposizione 2.19

Sia G un gruppo ciclico e sia $H \subset G$ un suo sottogruppo; allora H è ciclico.

Dimostrazione. Sia $\langle g \rangle = G$ e sia k il minimo intero positivo tale che $g^k \in H$; allora, dato $g^a \in H$, per qualche $a \in \mathbb{Z}$, si ha $a = qk + r$ per divisione euclidea. Si nota che: $(g^k)^{-q} g^a = (g^k)^{-q} g^{qk} g^r = g^r \in H$, visto che H è un sottogruppo. Questo, però, è assurdo perché $r < k$ e $g^r \in H$, quindi deve essere $r = 0$, da cui $\forall a \in \mathbb{Z} : g^a \in H$, si ha $a = qk$, per qualche intero q. Sostanzialmente: $\langle g^k \rangle = H$. □

Ora si torna a studiare i gruppi ciclici finiti con la seguente proposizione.

Proposizione 2.20

Sia G un gruppo ciclico di n elementi; allora $\forall d$ divisore di n, esiste esattamente un sottogruppo di cardinalità d in G.

Dimostrazione. Sia $\langle g \rangle = G$ e $d \mid n$; il sottogruppo K generato da $g^{n/d}$ si sa avere esattamente d elementi e si sa contenere esattamente $\phi(d)$ elementi di ordine d. Sia, ora, H un sottogruppo di G con proprio d elementi; per la precedente proposizione, si sa che H è ciclico, quindi $\exists h \in G : \langle h \rangle = H$, con h di ordine d. Questo, però, significa anche che $h \in K$ e, quindi $H \subseteq K$, visto che K contiene

tutte le potenze di h, essendo un sottogruppo. Visto che $H \subseteq K$ e hanno lo stesso numero di elementi, allora deve essere $H = K$. □

Proposizione 2.21

Sia G un gruppo ciclico con n elementi e sia g un suo generatore; allora $\forall k \in \mathbb{Z}$ si ha $\langle g^k \rangle = \langle g^{\gcd(k,n)} \rangle$.

Dimostrazione. Sia $d = \gcd(k,n)$ e $k = cd$, per qualche $c \in \mathbb{Z}$; per il teorema di Bézout, esistono $x, y \in \mathbb{Z}$ tali che

$$d = xk + yn$$

Per semplicità di notazione, sia $K = \langle g^k \rangle$ e sia $D = \langle g^d \rangle$. Visto che $g^k = (g^d)^c$, si ha $g^k \in D \implies K \subseteq D$; inoltre:

$$g^d = (g^k)^x (g^n)^y = \left((g^k)^x e^y\right) = (g^k)^x$$

quindi $g^d \in K$, da cui $D \subseteq K$. Complessivamente, si deve avere $D = K$. □

Si riassumono tutte le proprietà dimostrate sui gruppi ciclici finiti.

- In un gruppo ciclico di n elementi, si hanno $\phi(n)$ generatori.
- In un gruppo ciclico di n elementi, ci sono $\phi(d)$ elementi di ordine d, con $d \mid n$.
- Ogni sottogruppo di un gruppo ciclico è anch'esso ciclico.
- In un gruppo ciclico di n elementi, per ciascun d divisore di n, esiste un unico sottogruppo di ordine d.
- Dato g il generatore di un gruppo G di n elementi, il sottogruppo ciclico generato da g^k è lo stesso di quello generato da $g^{\gcd(k,n)}$.

Di seguito, una proposizione che permette di collegare la ciclicità di un gruppo finito con la sua immagine attraverso un omomorfismo.

Proposizione 2.22

Siano G, G' due gruppi e $\alpha : G \to G'$ un omomorfismo. Se $g \in G$ è un elemento di ordine finito $o(g) = n$, allora $o(\alpha(g))$ è finito e divide n.

Dimostrazione. Visto che α è un omomorfismo, $\forall k \in \mathbb{Z}$ si ha $\alpha(g^k) = \alpha(g)^k$. Questo vuol dire che $\alpha(g)^n = \alpha(g^n) = \alpha(e_G) = e_{G'}$. Questo significa che $o(\alpha(g)) \leq n$ e $o(\alpha(g))$ deve dividere n. □

2.8 Sottogruppi normali e I teorema di omomorfismo

Definizione 2.25 (Sottogruppo normale)

Sia G un gruppo e sia H un suo sottogruppo. Si dice che H è *normale* se soddisfa una delle due, equivalenti, condizioni:

NOR 1. $\forall x \in G,\ xH = Hx$, cioè $xHx^{-1} = H$;

NOR 2. H è il kernel di qualche omomorfismo di G in qualche altro gruppo.

Per indicare che H è un sottogruppo normale di G si scrive $H \lhd G$.

Intanto si nota che la condizione NOR 1 non coincide con la condizione $xhx^{-1} = h,\ \forall h \in H$ quando G non è commutativo. Nel caso di G commutativo, ogni sottogruppo H è normale e soddisfa la condizione più forte di NOR 1, cioè proprio $x^{-1}hx = h,\ \forall h \in H$.

Ora si dimostra che NOR 1 $\iff$ NOR 2. L'implicazione NOR 2 $\implies$ NOR 1 si vede di seguito.

Dimostrazione. Sia $H \equiv \mathrm{Ker}(f)$, con $f : G \to G'$ un omomorfismo di gruppi; allora:

$$f(xHx^{-1}) = f(x)f(H)f(x)^{-1} = e' \in G'$$

Da questo, segue che $xHx^{-1} \subset H,\ \forall x \in G$, quindi vale anche $x^{-1}Hx \subset H$[1], da cui (moltiplicando a sinistra per x e a destra per x^{-1}) si ha $H \subset xHx^{-1}$. □

L'altra implicazione si dimostra nel seguente teorema e nel successivo corollario.

Teorema 2.9

Sia G un gruppo e sia H un sottogruppo tale che $xH = Hx,\ \forall x \in G$. Se aH, bH sono due classi laterali di H, allora il prodotto $(aH) * (bH)$ è ancora una classe laterale. Inoltre, l'insieme delle classi laterali è esso stesso un gruppo, il cui prodotto è quello appena descritto.

Dimostrazione. La prima affermazione è immediata: $(aH) * (bH) = aHbH = abHH = abH$, usando che $xH = Hx$.

L'assioma GR 1 è osservata all'inizio di §2.6; GR 2 è soddisfatto da $eH = H$; GR 3, infine, è soddisfatto da $a^{-1}H$ come inverso di aH. □

Il gruppo delle classi laterali G/H è chiamato **gruppo quoziente** e si dice anche G **modulo** H. Il poter trattare questo come un gruppo è dovuto all'assunzione $xH = Hx$.

> **Osservazione 2.4.** Parlando di gruppo quoziente G/H si assumerà sempre che H è un sottogruppo normale di G.
> È chiaro che per essere vero che G/H è un gruppo quoziente, H deve per forza essere

[1] Visto che tale condizione vale $\forall x \in G$, si può mandare $x \to x^{-1}$ e, conseguentemente, $x^{-1} \to x$ e ottenere $x^{-1}Hx \subset H$.

un sottogruppo normale di G, da qui il motivo per cui lo si sottintende.

Esempio 2.8. Si considera il gruppo $(\mathbb{Z}, +)$ e il suo sottogruppo $\langle m \rangle = m\mathbb{Z}$, per qualche intero $m \in \mathbb{Z}$. Il relativo gruppo quoziente è $\mathbb{Z}/m\mathbb{Z}$; questo è l'insieme delle classi laterali della forma $\{z + km : k \in \mathbb{Z}\}$ al variare di $z \in \mathbb{Z}$, cioè ogni classe laterale corrisponde agli interi che hanno resto z quando divisi per m. Questo gruppo quoziente è, pertanto, isomorfo a $\mathbb{Z}_m$: partendo dal gruppo infinito $\mathbb{Z}$, tramite quoziente si è ottenuto un gruppo finito $\mathbb{Z}_m$.

Corollario 2.5 (Omomorfismo canonico)

Sia G un gruppo e sia H un suo sottogruppo normale. Sia G/H il gruppo quoziente e $\pi : G \to G/H$ la mappa che, ad ogni $a \in G$, associa la classe laterale aH, cioè $\pi(a) = aH$. Allora π è un omomorfismo e $\mathrm{Ker}(\pi) \equiv H$.

Dimostrazione. È evidente che π sia un omomorfismo dalla definizione di prodotto di classi laterali. Per il kernel, si vede che ogni elemento di H è automaticamente in $\mathrm{Ker}(\pi)$ perché se $h \in H \Rightarrow \pi(h) = hH \equiv H$. Sia, invece, $x \in G : \pi(x) = xH$ sia l'elemento unità di G/H, quindi coincidente con il laterale H stesso: $xH = H$. Questo vuol dire che $xe = x$ è un elemento di H. Quindi H coincide con il kernel di π. □

Proposizione 2.23

Dati $K \subset H \subset G$ sottogruppi normali di G, la mappa $xK \mapsto xH$, con $x \in G$ è un omomorfismo suriettivo $f : G/K \to G/H$; il suo kernel è H/K.

Dimostrazione. Intanto è ben definito: se $xK = yK \Rightarrow xH = yH$ perché $y^{-1}xK = K \Rightarrow f(y^{-1}xK) = y^{-1}xH = f(K) = H$, da cui $y^{-1}xH = H \Rightarrow xH = yH$.

Ora si verifica che è suriettivo; $\forall xH \in G/H$, si può prendere $f(xK) = xH$. Poi si verifica che è un omomorfismo; dati comunque $x, y \in G$:

$$f(xKyK) = f(xyK) = xyH = xHyH = f(xK)f(yK)$$

Il kernel è, infine, composto dagli elementi di G/K che vengono mappati in H, quindi

$$\mathrm{Ker}(f) = \{xK \in G/K : f(xK) = H\} = \{xK \in G/K : x \in H\} = H/K$$

La forma del Kernel è anche il motivo per cui questo non è un isomorfismo (cioè perché non è iniettivo). □

Sia $f : G \to G'$ un omomorfismo. Dato $x \in G$, allora, $\forall k \in \mathrm{Ker}(f)$:

$$f(xk) = f(x)f(k) = f(x) \implies f(x\mathrm{Ker}(f)) = f(x)$$

Quindi, ogni elemento in un laterale di $\mathrm{Ker}(f)$ ha la stessa immagine sotto f.

Teorema 2.10 (Primo teorema di omomorfismo)

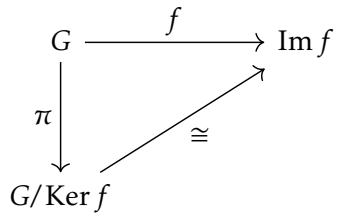
Sia $f : G \to G'$ un omomorfismo e sia $H = \mathrm{Ker}(f)$; allora la mappa $x\mathrm{Ker}(f) \mapsto f(x\mathrm{Ker}(f))$ è un isomorfismo del gruppo quoziente G/H con l'immagine di f, cioè $G/H \xrightarrow{\approx} \mathrm{Im}(f)$. In questo caso, si dice che l'isomorfismo $\overline{f}$ è **indotto** da f.

Dimostrazione. Si definisce $\overline{f} : G/H \to G'$ t.c. $xH \mapsto f(xH)$. Ora si verifica che è un isomorfismo usando il teorema 2.2. Intanto si ha che $\overline{f}$ è un omomorfismo, infatti:

$$\overline{f}(xHyH) = \overline{f}(xyH) = f(xy) = f(x)f(y) = \overline{f}(xH)\overline{f}(yH)$$

È anche iniettiva perché il suo nucleo sono quei laterali xH tali che $f(xH) = e'$, quindi solamente H, che è l'unità di G/H. Infine si ha $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ per definizione di f. Quest'ultima considerazione permette di concludere che $G/H \cong \mathrm{Im}(f)$. □

Il primo teorema di omomorfismo si può esprimere in termini di un diagramma commutativo che permette di evidenziare le implicazioni del teorema.



In questo modo, si ha $f = \overline{f} \circ \pi$.

Esempio 2.9. Si considera, come esempio, $\mathbb{Z}$ come sottogruppo del gruppo additivo $(\mathbb{R}, +)$; il gruppo quoziente $\mathbb{R}/\mathbb{Z}$ è chiamato **gruppo circolare**.
Dati due numeri reali $x, y \in \mathbb{R}$, si dice che $x \equiv y \pmod{\mathbb{Z}}$ se $x - y \in \mathbb{Z}$; questa definisce una relazione di equivalenza, le cui classi di equivalenza sono esattamente i laterali di $\mathbb{Z}$ in $\mathbb{R}$. Se è vero che $x \equiv y \pmod{\mathbb{Z}}$, allora $e^{2\pi ix} = e^{2\pi iy}$ e la mappa $x \mapsto e^{2\pi ix}$ definisce un isomorfismo di $\mathbb{R}/\mathbb{Z}$ nel gruppo moltiplicativo dei numeri complessi che hanno modulo unitario.

Esempio 2.10. Siano $\mathbb{C}^*$ e $\mathbb{R}^+$, rispettivamente, il gruppo moltiplicativo dei numeri complessi non-nulli e il gruppo moltiplicativo dei reali positivi.
Dato $\alpha \in \mathbb{C}^*$, vale $\alpha = ru$, con $r \in \mathbb{R}^+$ e $|u| = 1$ (si prende $u = \alpha/|\alpha|$). L'espressione di u è sempre determinata e la mappa $\alpha \mapsto \alpha/|\alpha|$ è un omomorfismo di $\mathbb{C}^*$ in $\mathbb{C}_1 := \{x \in \mathbb{C} : |x| = 1\}$. Essendo il nucleo di questo omomorfismo proprio $\mathbb{R}^+$, allora $\mathbb{C}^*/\mathbb{R}^+ \cong \mathbb{C}_1$.

Dal primo teorema di omomorfismo, seguono immediatamente i due seguenti corollari.

Corollario 2.6

Sia $f : G_1 \to G_2$ un omomorfismo suriettivo; allora

$$G_1/\mathrm{Ker} f \cong G_2$$

Corollario 2.7

Sia $f : G_1 \to G_2$ un omomorfismo iniettivo; allora

$$G_1 \cong \mathrm{Im} f$$

2.9 Approfondimenti sui gruppi

2.9.1 Il gruppo simmetrico e il gruppo alterno

Data una permutazione $\sigma \in S_n$, si indica con la tupla $\lambda(\sigma) = (\lambda_1, \dots, \lambda_k)$ la lunghezza di ciascuno dei k cicli disgiunti in cui si decompone σ. Usando l'equazione 2.5.1, si può riscrivere l'orbita di σ come:

$$\mathrm{Orb}(\sigma) = \{\tau \in S_n \mid \lambda(\tau) = \lambda(\sigma)\}$$

Secondo la formula in equazione 2.5.1, infatti, ciascuna permutazione in $\mathrm{Orb}(\sigma)$ si decompone nello stesso numero di cicli di stessa lunghezza di σ. Si introduce, poi, il numero $m_i(\sigma)$ che indica il numero di cicli di lunghezza i in cui si decompone σ; in notazione insiemistica, questo si scrive come:

$$m_i(\sigma) = \left|\left\{j \mid \lambda_j = i,\ \forall \lambda_j \text{ ciclo di } \sigma\right\}\right|$$

Proposizione 2.24

Per ogni permutazione $\sigma \in S_n$, sottintendendo $m_i = m_i(\sigma)$, vale la formula

$$|\mathrm{Orb}(\sigma)| = \frac{n!}{1^{m_1} 2^{m_2} \cdots n^{m_n} m_1! m_2! \cdots m_n!}$$

Dimostrazione. Fissate le lunghezze dei cicli in cui si decompone σ, si hanno $\binom{n}{\lambda_1}$ modi di scegliere elementi nel primo ciclo, $\binom{n-\lambda_1}{\lambda_2}$ elementi nel secondo e così via fino a $\binom{\lambda_k}{\lambda_k}$ per l'ultimo ciclo. Questo restituisce un numero possibile di scelte dato da:

$$\binom{n}{\lambda_1}\binom{n-\lambda_1}{\lambda_2}\cdots\binom{\lambda_k}{\lambda_k} = \frac{n!}{\lambda_1!\lambda_2!\cdots\lambda_k!}$$

Tutto questo va moltiplicato, ancora, per le possibili scelte all'interno di un singolo ciclo λ_i; cioè per ciascun λ_i, fissati gli elementi al suo interno, si hanno $(\lambda_i - 1)!$ possibili cicli diversi perché bisogna escludere quelli equivalenti fra loro (relativi a tutte le possibili rotazioni dello stesso ciclo). Così facendo, si rimane

con:

$$\frac{n!}{\lambda_1 \cdots \lambda_k} = \frac{n!}{1^{m_1} 2^{m_2} \cdots n^{m_n}}$$

Così facendo, però, si stanno contando più volte le permutazioni che hanno cicli della stessa lunghezza; se, infatti, fosse $\lambda_i = \lambda_j$, per qualche coppia i, j, non importa se si prende prima λ_i o prima λ_j (per esempio, la permutazione $(1,2)(3,4) = (3,4)(1,2)$). Per risolvere, bisogna dividere per le possibili permutazioni dei cicli di stessa lunghezza, quindi si rimane con:

$$\frac{n!}{1^{m_1} \cdots n^{m_n} m_1! \cdots m_n!}$$

che coincide proprio col numero di possibili permutazioni con cicli di stessa lunghezza di σ, quindi con $|\mathrm{Orb}(\sigma)|$. □

Come già accennato, ogni permutazione è scomponibile in trasposizioni; per esempio

$$(2,6,3,7,5,9,10) \in S_{10}$$

si può scrivere come

$$\begin{aligned}(2,6,3,7,5,9,10) &= (2,6)(6,3)(3,7)(7,5)(5,9)(9,10) \\ &= (2,10)(2,9)(2,5)(2,7)(2,3)(2,6)\end{aligned}$$

da cui si osserva anche che la decomposizione non è unica, come non lo è neanche il numero di trasposizioni utilizzabili:

$$(1,2) = (2,3)(1,3)(2,3) \in S_3$$

Quello che non cambia, però, è la parità del numero di trasposizioni usate, che permette di definire il concetto di **parità** di una permutazione.

Teorema 2.11
Sia $\sigma \in S_n$, con $n \geq 2$; se σ si decompone sia in k trasposizioni che k' trasposizioni, allora $k \equiv k' \pmod 2$.

Dimostrazione. Si fa *agire* S_n su $\mathbb{R}[x_1, \ldots, x_n]$, cioè l'insieme dei polinomi a coefficienti reali in n variabili nel seguente modo: presa $\sigma \in S_n$ e dato $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ si ha:

$$\sigma f(x_1, .., x_n) = f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)$$

Si nota che l'identità $e \in S_n$ è quella che lascia il polinomio invariato e si nota anche che $\forall \sigma, \tau \in S_n,\ f \in \mathbb{R}[x_1, \ldots, x_n]$:

$$(\sigma \circ \tau) f(x_1, \ldots, x_n) = \sigma\left[\tau f(x_1, \ldots, x_n)\right]$$

Questo è un esempio di *azione di gruppo su un insieme*. In questo caso particolare, si considera il polinomio

$$p(x_1,\dots,x_n) = \prod_{1\le i<j\le n} (x_i - x_j)$$

Per esempio, se $n = 3$, si ha $p(x_1,x_2,x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. Si considera la trasposizione $\tau = (a,b)$, $1 \le a < b \le n$ e si studia il risultato di $\tau p(x_1,\dots,x_n)$. Si nota che l'azione di τ non modifica i fattori $x_i - x_j$ in cui $i,j \neq a,b$, mentre per gli altri che contengono almeno a o b:

- $\forall i : 1 \le i < a$, l'azione di τ scambia $(x_i - x_a)$ e $(x_i - x_b)$;
- $\forall i : b < i \le n$, l'azione di τ scambia $(x_a - x_i)$ e $(x_b - x_i)$;
- $\forall i : a < i < b$, l'azione di τ scambia i fattori $(x_a - x_i)$ e $(x_i - x_b)$, ma scambiandone anche il segno, quindi il segno del prodotto rimane invariato;
- infine, l'azione di τ sul fattore $(x_a - x_b)$ ne cambia il segno.

Ne segue, dunque, che $\tau p(x_1,\dots,x_n) = -p(x_1,\dots,x_n)$, $\forall \tau \in S_n$, con τ trasposizione. Sfruttando che ogni $\sigma \in S_n$ permutazione generica è scrivibile in termini di k trasposizioni:

$$\sigma p(x_1,\dots,x_n) = (-1)^k p(x_1,\dots,x_n)$$

Ma allora, se σ si decompone anche in k' trasposizioni, significa che

$$\sigma p(x_1,\dots,x_n) = (-1)^{k'} p(x_1,\dots,x_n)$$

il che implica che $(-1)^{k'} = (-1)^k \implies k \equiv k' \pmod 2$. □

Questo teorema permette di dividere le permutazioni in due classi, a seconda della loro parità, definita di seguito.

Definizione 2.26 (Parità di una permutazione)

Si dice che $\sigma \in S_n$ è **pari** se può essere scritta come prodotto di un numero pari di trasposizioni, altrimenti verrà detta **dispari** se potrà essere scritta come prodotto di un numero dispari di trasposizioni.

Da questo teorema e dalla definizione di parità di una permutazione, si intende caratterizzare l'insieme delle permutazioni esclusivamente pari.

Definizione 2.27 (Gruppo alterno)

Si definisce l'insieme delle permutazioni pari $A_n \subset S_n$ come *gruppo alterno*.

Corollario 2.8

Per $n \geq 2$, il gruppo alterno A_n è un sottogruppo normale di S_n. Inoltre, vale che $|A_n| = n!/2$.

Dimostrazione. Si considera la funzione segno definita come $\text{sgn} : S_n \to \{-1, +1\}$, dove $\text{sgn}(\sigma) = 1 \Rightarrow \sigma$ è pari, mentre $\text{sgn}(\sigma) = -1 \Rightarrow \sigma$ è dispari. Come conseguenza del teorema 2.11, si ha che la funzione segno è un omomorfismo tra S_n e il gruppo moltiplicativo $\{-1, +1\}$ (il quale è, a sua volta, isomorfo a $\mathbb{Z}_2$). Allora il suo nucleo, che coincide proprio con A_n, è un sottogruppo normale di S_n.

Circa la cardinalità, invece, si nota che la mappa $\sigma \mapsto (1,2)\sigma$ che va da S_n in se stesso è una biezione e cambia di segno a σ; essendo una biezione e mandando le permutazioni pari in quelle dispari e viceversa (cioè ad ogni permutazione dispari se ne associa una pari e viceversa), significa che in S_n ci sono tante permutazioni pari quante dispari, il che vuol dire che $|A_n| = n!/2$. □

Si nota che la classe laterale $(1,2)A_n$ è composta da tutte le permutazioni dispari.

Inoltre, ricordando che in questa sezione si è trovato un algoritmo per scrivere ciascun ciclo di lunghezza j in termini del prodotto di $j-1$ trasposizioni, si riesce a capire immediatamente, data la decomposizione in cicli disgiunti di una permutazione, se essa è pari o dispari. Infatti, se σ è una permutazione che si decompone in r cicli di lunghezza dispari e s di lunghezza pari, allora questa è pari se e solo se s è pari.

2.9.2 Centralizzatore di un elemento

Si ricorda che $Z(G)$ è il sottogruppo di G costituito da tutti gli elementi che commutano con tutti gli altri ed è anche facile convincersi che questo sia un suo sottogruppo normale per definizione. Fissato $\gamma \in G$, si considera, adesso, l'insieme di tutti gli elementi che commutano con tale γ.

Definizione 2.28 (Centralizzatore)

Sia G un gruppo e sia $\gamma \in G$; si indica il centralizzatore di γ con $C(\gamma)$ ed è l'insieme definito come

$$C(\gamma) = \{g \in G \mid g\gamma = \gamma g\}$$

Si nota che, equivalentemente, si sarebbe potuto definire come

$$C(\gamma) = \left\{g \in G \mid g\gamma g^{-1} = \gamma\right\}$$

Osservazione 2.5. Si nota che la seconda definizione permette di individuare il centralizzatore di γ come quell'insieme i cui elementi g soddisfano $C_g(\gamma) = \gamma$.

Si vede subito che se $\gamma \in Z(G)$, allora $G(\gamma) = G$.

Proposizione 2.25

Sia G un gruppo con $\gamma \in G$; vale $C(\gamma) < G$ (cioè $C(\gamma)$ è un sottogruppo di G).

Dimostrazione. L'identità vi appartiene perché l'identità commuta con tutti gli elementi di G, in particolare con γ. Successivamente, se $g_1, g_2 \in C(\gamma)$, allora:

$$g_1 g_2 \gamma = g_1 \gamma g_2 = \gamma g_1 g_2 \implies g_1, g_2 \in C(\gamma)$$

Infine, se $g \in C(\gamma)$, allora $g^{-1} \in C(\gamma)$ perché

$$\gamma = g^{-1} g \gamma = g^{-1} \gamma g \implies \gamma g^{-1} = g^{-1} \gamma$$

□

Teorema 2.12

Sia G un gruppo e sia $\gamma \in G$; allora esiste una biezione tra $G/C(\gamma)$ e $\mathrm{Orb}(\gamma)$.

Dimostrazione. Si definisce la funzione

$$\begin{aligned} f : G/C(\gamma) &\longrightarrow \mathrm{Orb}(\gamma) \\ gC(\gamma) &\longmapsto g\gamma g^{-1} \end{aligned}$$

f è ben definita perché se $kC(\gamma) = gC(\gamma)$, allora $k = gs$, per qualche $s \in C(\gamma)$, per cui:

$$f\Big(kC(\gamma)\Big) = k\gamma k^{-1} = (gs)\gamma(gs)^{-1} = gs\gamma s^{-1} g^{-1} = g\gamma g^{-1}$$

Questo mostra che la mappa è ben definita.

Per la suriettività, invece, si nota che per $g_1 \gamma g_1^{-1} \in \mathrm{Orb}(\gamma)$, basta prendere $g_1 C(\gamma)$ nel dominio.

Infine, per l'iniettività, si assume che $f\Big(gC(\gamma)\Big) = f\Big(hC(\gamma)\Big)$, cioè $g\gamma g^{-1} = h\gamma h^{-1}$; questo, però, implica che $h^{-1} g \gamma g^{-1} h = \gamma$, da cui segue che $h^{-1} g \in C(\gamma) \implies hC(\gamma) = hh^{-1} gC(\gamma) = gC(\gamma)$, cioè stessi elementi dell'immagine corrispondono a stessi elementi nel dominio. □

Corollario 2.9

Sia G un gruppo; allora $\forall \gamma \in G$:

$$|\mathrm{Orb}(\gamma)| = \frac{|G|}{|C(\gamma)|}$$

2.9.3 Quoziente di un gruppo ciclico

Si considera un gruppo ciclico C (finito o infinito) generato da un elemento x, cioè $C = \langle x \rangle$. Un suo sottogruppo H sarà per forza normale, visto che C è commutativo; si vuole studiare il gruppo quoziente C/H.

A questo proposito, si considera l'omomorfismo canonico $\pi : C \to C/H$; visto che x genera C, allora $\pi(x) = xH$ genera C/H.

Dimostrazione. Usando che π è una mappa suriettiva e il fatto che $\pi(x^j) = \pi(x)^j$, visto che è un omomorfismo, si ottiene che una qualunque classe laterale $bH = x^kH$, per qualche intero k, è l'immagine di $\pi(x^k) = \pi(x)^k$, quindi si ottiene la tesi perché ogni classe laterale si ottiene tramite elevazione a potenza di $\pi(x)$. □

Questo dimostra anche che C/H è ciclico. In quanto tale, si analizzano i vari scenari possibili.

(a). Se $H = \{e\}$, allora π è una mappa sia iniettiva che suriettiva, pertanto è un isomorfismo e vale $C \cong C/H$.

(b). Se $H = C$ (che equivale a dire che $x \in H$), allora C/H contiene la sola classe laterale eH.

(c). Se $\{e\} \subsetneq H \subsetneq C$, allora necessariamente $x \notin H$; si considera m come il più piccolo intero positivo tale che $x^m \in H$. Usando quanto trovato sopra, cioè che C/H è ciclico ed è generato da xH, e aggiungendo anche l'informazione per cui $x^mH = H$ perché, per definizione, $x^m \in H$, si conclude che l'ordine di xH è proprio m, quindi C/H ha cardinalità m e i suoi elementi sono:

$$H,\ xH,\ x^2H,\ldots,\ x^{m-1}H$$

3 Teoria degli anelli

3.1 Definizioni preliminari

Definizione 3.1 (Anello)

Un insieme R è detto *anello con unità* se possiede due operazioni, $+$ (addizione) e $\cdot$ (moltiplicazione), che soddisfano le seguenti proprietà:

(r1). R è un gruppo commutativo rispetto a $+$;

(r2). $\forall a, b, c \in R$, vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associatività rispetto al prodotto);

(r3). $\exists 1 \in R : \forall a \in R,\ a \cdot 1 = 1 \cdot a = a$;

(r4). $\forall a, b, c \in R,\ (a + b) \cdot c = a \cdot c + b \cdot c$ e $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributività).

Per anello, si intederà sempre un anello con unità, nonostante sia possibile una definizione anche senza unità.

Osservazione 3.1. La definizione ammette un anello della forma $A = \{0\}$, in cui tutte le operazioni sono quelle banali e lo 0 funziona sia da elemento neutro per la somma, che per la moltiplicazione.

Definizione 3.2 (Anello commutativo)

Un anello R tale che $\forall a, b \in R$

$$a \cdot b = b \cdot a$$

è detto commutativo.

Definizione 3.3 (Divisore dello zero)

Sia R un anello commutativo. Si dice che $a \in R$ è un *divisore dello zero* se $\exists b \in R,\ b \neq 0$ tale che $ab = 0$.

In particolare, 0 è sempre un divisore dello zero. Inoltre, un anello commutativo R in cui $0 \neq 1$ e in cui l'unico divisore dello zero è 0 si dice **dominio** (o dominio di integrità).

Definizione 3.4 (Elemento invertibile)

Sia $u \in R$; u si dice *invertibile* se esiste $v \in R$ tale che $u \cdot v = v \cdot u = 1$. Si indica con R^* l'insieme degli elementi invertibili in R.

Proposizione 3.1

Sia R un anello; l'insieme R^* è un gruppo rispetto alla moltiplicazione.

Dimostrazione. L'associatività è soddisfatta dall'assioma (r2) degli anelli, visto che $R^* \subset R$. Evidentemente esiste l'elemento neutro perché esso è invertibile, infatti $1 \cdot 1 = 1$. Infine, l'elemento inverso deve essere contenuto nell'insieme per-

ché $\forall a \in R^*$, $\exists a^{-1} \in R : a \cdot a^{-1} = a^{-1} \cdot a = 1$, ma a^{-1} è invertibile con inverso proprio a. □

Definizione 3.5 (Elementi associati)
Siano $a, b \in R$ anello commutativo; questi si dicono *associati* se $a = bu$, per $u \in R^*$.

Definizione 3.6 (Corpo)
Un anello R in cui $0 \neq 1$ e in cui $\forall \in R \setminus \{0\}$ è invertibile è detto *corpo*.

Definizione 3.7 (Campo)
Un corpo è detto *campo* se è commutativo.

Alcuni esempi di *anelli commutativi* sono $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_m$ con $m > 1$. Gli anelli $\mathbb{Q}$ e $\mathbb{R}$ sono anche dei *campi*, mentre $\mathbb{Z}$ no perché non possiede gli inversi rispetto alla moltiplicazione degli elementi diversi da $-1, 1$. Tuttavia, $\mathbb{Z}$ è un esempio di *dominio*. Se R è un anello commutativo, anche l'*insieme dei polinomi a coefficienti in R*, $R[x]$, è un anello commutativo. Inoltre, se R è un dominio, anche $R[x]$ è un dominio.

Un anello non commutativo è l'anello $\mathcal{M}_n(K)$ delle matrici $n \times n$, $n \geq 2$ a coefficienti in un campo K.

3.1.1 I quaternioni

Un esempio di corpo che non è un campo sono i quaternioni $\mathbb{H}$. Per descriverlo, si parte dal gruppo dei quaternioni, dato da $(Q_8, \cdot)$

$$Q_8 = \{1, -1, \mathbf{i}, (-1)\mathbf{i}, \mathbf{j}, (-1)\mathbf{j}, \mathbf{k}, (-1)\mathbf{k}\} \tag{3.1.1}$$

dove il prodotto è definito nel seguente modo:

- 1 è l'elemento neutro;
- valgono le seguenti relazioni:

$$(-1)^2 = 1 \qquad i^2 = j^2 = k^2 = -1 \qquad \mathbf{ij} = (-1)\mathbf{ji} = \mathbf{k}$$
$$\mathbf{jk} = (-1)\mathbf{kj} = \mathbf{i} \qquad \mathbf{ki} = (-1)\mathbf{ik} = \mathbf{j}$$

Si può verificare che, con questo prodotto, Q_8 è un gruppo non-commutativo nel quale sono presenti tre elementi di ordine 4; questo implica anche che non è isomorfo al gruppo diedrale di 8 elementi D_4 perché quest'ultimo ha solo due elementi di ordine 4.

Il corpo dei quaternioni è un'estensione del campo dei complessi. Per la sua costruzione, si parte dallo spazio vettoriale reale di dimensione 4 con base $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

dove la somma è data da

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = (a + a') + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$$

Per conferirgli una struttura di anello, si deve definire una moltiplicazione; questa è definita distribuendo ciascun termine dei due fattori e usando le relazioni stabilite dal prodotto per Q_8. In questo modo, $\mathbb{H}$ ha una struttura di anello con unità ed è evidentemente non commutativo, visto che Q_8 non lo è.

Si nota che ogni elemento di $\mathbb{H} \setminus \{0\}$ ha un inverso; infatti, dato $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, con a, b, c, d non tutti nulli, il suo inverso è dato da:

$$\frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}$$

Se ne conclude, dunque, che $\mathbb{H}$ è un corpo, ma non un campo.

3.1.2 Gli anelli $\mathbb{Z}_m$

Si nota che se m non è primo, allora $\mathbb{Z}_m$ ha dei divisori dello zero che sono diversi da $[0]_m$, per cui non è un dominio. Se m non fosse primo, infatti, si potrebbe fattorizzare come $m = k \cdot s$, con $1 < k, s < m$ e varrebbe:

$$[k]_m[s]_m = [ks]_m = [m]_m = [0]_m$$

Ne segue che se m non è primo, allora $\mathbb{Z}_m$ non è un campo perché, come si mostrerà, un campo è automaticamente un dominio. È facile vedere, però, che non esiste un inverso di $[k]_m$ e $[s]_m$.

Dimostrazione. Prendendo d'esempio k, la condizione che deve verificare per avere inverso modulo m è $\gcd(k, m) = 1$, ma chiaramente non sono coprimi perché m è, per definizione, un suo multiplo. □

Teorema 3.1
Se p è un numero primo, allora $\mathbb{Z}_p$ è un campo.

Dimostrazione. Sia $[a]_p \neq [0]_p$ in $\mathbb{Z}_p$; visto che p non divide a, allora $\gcd(a, p) = 1$, per cui $ax \equiv 1 \pmod{p}$ ha soluzione, cioè a ha un inverso modulo p; sia questo b. Conseguentemente, $[a]_p[b]_p = [ab]_p = [1]_p$, il che vuol dire che $\exists [b]_p \in \mathbb{Z}_p$ inverso di $[a]_p$. Pertanto, ogni elemento di $\mathbb{Z}_p$ ha inverso. □

3.2 Anelli di polinomi e algoritmo di Euclide

Sia K un campo; si considera l'insieme $K[x]$ dei polinomi a coefficienti in K. Un generico $f(x) \in K[x]$ è della forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

con $a_i \in K, \forall i = 0, 1, \ldots, n$. In questa notazione, dire che $f(x)$ è non-nullo equivale a richiedere che almeno $a_n \neq 0$, dove a_n è chiamato *coefficiente direttore* di $f(x)$ e n è il grado del polinomio, indicato con $\deg f$.

Osservazione 3.2. Per convenzione, il polinomio costante 0 ha grado $-\infty$.

Proposizione 3.2

Dati $f, g \in K[x]$, vale

$$\deg fg = \deg f + \deg g$$

Dimostrazione. Il grado di un polinomio è dato dal massimo esponente di x; evidentemente, il termine di massimo grado del prodotto è ottenuto dal prodotto dei termini di grado massimo, cioè da $x^{\deg f} \cdot x^{\deg g} = x^{\deg f + \deg g}$, da cui segue la tesi. □

Teorema 3.2 (Algoritmo di Euclide)

Siano $f, g \in K[x]$ due polinomi e sia $\deg g \geq 0$; allora esiste un'unica coppia di polinomi $q(x), r(x) \in K[x]$ tali che

$$f(x) = q(x)g(x) + r(x)$$

con $\deg r < \deg g$.

Dimostrazione. Sia $m = \deg g \geq 0$; i polinomi f, g sono della forma

$$f(x) = a_n x^n + \ldots + a_0$$
$$g(x) = b_m x^m + \ldots + b_0$$

con $b_m \neq 0$. Se $n < m$, allora si prende $q = 0$ e $r = f$ e il teorema è dimostrato. Si considera, ora, il caso $n \geq m$; sia, allora:

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) \implies \deg f_1 < \deg f$$

Ripetendo il procedimento finché non ci si trova nel caso $\deg f_k < \deg g$, caso in cui si prende $q = 0$ e $r = f_k$, si trovano dei polinomi q_1, r tali che

$$f_1(x) = q_1(x)g(x) + r(x), \ \deg r < \deg g$$

Allora:

$$\begin{aligned} f(x) &= a_n b_m^{-1} x^{n-m} g(x) + f_1(x) \\ &= a_n b_m^{-1} x^{n-m} g(x) + q_1(x) g(x) + r(x) \\ &= \Big(a_n b_m^{-1} x^{n-m} + q_1(x)\Big) g(x) + r(x) \end{aligned}$$

Ora manca da mostrare l'unicità di questa decomposizione. Si suppone, allora, che valga

$$f = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

con $\deg r_1, \deg r_2 < \deg g$. Ma quindi si ha

$$(q_1 - q_2)g = r_2 - r_1$$

Questo vuol dire che o il grado del membro di sinistra è $\geq \deg g$, oppure è nullo e, contemporaneamente, o il mmebro di destra è nullo, oppure è $< \deg g$. Se ne conclude che l'unica possibilità è che siano entrambi nulli, quindi $q_1 = q_2$ e $r_1 = r_2$. □

Definizione 3.8 (Polinomio monico)

Un polinomio $f(x) \in K[x]$, con $\deg f(x) = n$, si dice *monico* se $a_n = 1$.

3.2.1 Il massimo comune divisore e il teorema di Bézout

Usando l'algoritmo di Euclide si può definire il **massimo comune divisore** per un polinomio, cioè dati $f(x), g(x) \in K[x]$, si costruisce $\gcd(f(x), g(x))$.

Si deve dimostrare che questo è ben definito; intanto, dati due polinomi e dato l'insieme dei loro divisori monici, se ne può sicuramente scegliere unico di grado maggiore; rimane da mostrare che questa scelta è unica.

Si prendono due polinomi $f(x), g(x) \in K[x]$; per l'algoritmo di Euclide, esistono unici $r_1(x), q_1(x) \in K[x]$ tali che

$$f(x) = q_1(x)g(x) + r_1(x), \ \deg g > \deg r_1$$

Se $r_1 = 0$, ci si ferma perché $\gcd(f, g) = g(x)$, altrimenti $\exists! q_2, r_2 \in K[x]$ tali che

$$g(x) = q_2(x)r_1(x) + r_2(x), \ \deg r_1 > \deg r_2$$

Se $r_2 = 0$, ci si ferma perché $\gcd(f, g) = r_1(x)$, altrimenti si reitera. In generale, identificando $f = r_{-1}$ e $g = r_0$, si possono trovare delle sequenze uniche di polinomi in $K[x]$ tali che

$$r_{i-2}(x) = q_i r_{i-1}(x) + r_i(x)$$

con $\deg r_i \leq \deg r_{i-1}$, $\forall i$; proprio perché $\forall i$, il grado di r_i è minore strettamente di quello di r_{i-1}, allora esiste il più piccolo $k \geq 0 : r_{k+1}(x) = 0$. Conseguentemente, $r_k(x)$ differirà da $\gcd(f,g)$ a meno di un multiplo perché, ad ogni passaggio, ogni divisore comune di r_{i-2}, r_{i-1} deve esserlo anche di r_i, quindi, un divisore comune di f e g lo sarà anche di r_k. In particolare, quindi, $\gcd(f,g) \mid r_k(x)$.

Per quanto detto sopra, nell'asunzione che $r_{k+1} = 0$, si ha $r_{k-1}(x) = q_{k+1}(x)r_k(x) \Rightarrow r_k(x)$ divide $r_{k-1}(x)$. Inoltre si nota che $r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x)$, quindi r_k divide anche r_{k-2}; iterando, si conclude che $r_k(x)$ divide tutti gli $r_i(x)$, quindi anche $r_{-1}(x) = f(x)$ e $r_0(x) = g(x)$.

Sia, ora, γ il coefficiente direttore di $r_k(x)$; questo vuol dire che $r_k(x)/\gamma$ ha coefficiente direttore unitario e divide $f(x)$ e $g(x)$. Allora, per definizione di massimo comune divisore, si ha

$$\deg \frac{r_k(x)}{\gamma} \leq \deg(\gcd(f,g))$$

ma, allo stesso tempo, deve valere anche che

$$\deg \frac{r_k(x)}{\gamma} \geq \deg(\gcd(f,g))$$

perché il m.c.d. divide $r_k(x)$, quindi anche $r_k(x)/\gamma$. Allora, visto che i polinomi $\gcd(f,g)$ e $r_k(x)/\gamma$ sono entrambi monici e hanno stesso grado; inoltre, il primo divide il secondo, pertanto devono essere uguali.

Per finire, bisogna dimostrare che tutti i polinomi che dividono $f(x), g(x)$ e hanno grado massimale sono associati fra loro, quindi differiscono per il prodotto per un valore di K, e che ne esiste uno solo che è monico. Per la prima, assumendo che $p(x), q(x)$ siano due divisori di grado massimale di f e g, si ha, per esempio

$$f = ap(x) = bq(x) \implies p(x) = \frac{b}{a}q(x)$$

perché $a^{-1} \in K$ (visto che K è un campo), per cui $b/a \in K$ per chiusura sotto moltiplicazione, quindi $p(x)$ e $q(x)$ sono associati. Assumendo, ora, che siano entrambi monici, le costanti a e b devono essere uguali perché, altrimenti, il termine di grado massimo nei due avrebbe due coefficienti diversi e non sarebbero uguali. Questo dimostra l'unicità, quindi la buona definizione, del massimo comune divisore per polinomi.

Anche per i polinomi, si ha un analogo del *teorema di Bézout*; infatti, partendo dall'ultima relazione dell'algoritmo di Euclide, si trovano due polinomi $y(x), z(x) \in K[x]$ tali che

$$y(x)f(x) + z(x)g(x) = r_k(x)$$

A questo punto, dividendo per il coefficiente direttore γ di $r_k(x)$, si trova proprio:

$$\lambda(x)f(x) + \mu(x)g(x) = \gcd(f,g) \tag{3.2.1}$$

con $\lambda(x) = y(x)/\gamma$ e $\mu(x) = z(x)/\gamma$.

Esempio 3.1. Siano $f(x) = 2x^4 + 5x^3 + 10x^2 + 10x + 3$ e $g(x) = 2x^3 + x^2 + 4x + 2$ due polinomi. Si nota che, per l'algoritmo di Euclide:

$$f_1(x) = f(x) - xg(x) = 4x^3 + 6x^2 + 8x + 3$$

Essendo ancora $\deg f_1 \geq \deg g$, si reitera:

$$f_2(x) = f_1(x) - 2g(x) = f(x) - (x+2)g(x) = 4x^2 - 1$$

Visto che $\deg f_2 < \deg g \Rightarrow f_2$ è il resto; infatti:

$$f_2(x) = f(x) - (x+2)g(x) \implies f(x) = (x+2)g(x) + f_2(x) = q_1(x)g(x) + r_1(x)$$

con $q_1(x) = x + 2$ e $r_1(x) = 4x^2 - 1$. Applicando, ora, lo stesso algoritmo per scrivere $g(x) = q_2(x)r_1(x) + r_2(x)$, si trovano

$$q_2(x) = \frac{2x+1}{4} \qquad r_2(x) = \frac{9(2x+1)}{4}$$

Applicando nuovamente l'algoritmo per scrivere $r_1(x) = q_3(x)r_2(x) + r_3(x)$, si trovano $q_3(x) = (8x - 4)/9$ e $r_3(x) = 0$. Ne segue che

$$\gcd(f, g) = \frac{4}{18} r_2(x) = \frac{2x+1}{2}$$

Ora, a partire dalla relazione

$$\begin{aligned} r_2(x) &= g(x) - q_2(x)r_1(x) = g(x) - q_2(x)\Big[f(x) - q_1(x)g(x)\Big] \\ &= -q_2(x)f(x) + \Big(1 + q_1(x)q_2(x)\Big)g(x) \end{aligned}$$

Si trovano

$$\lambda(x) = -\frac{4}{18} q_2(x) = -\frac{2x+1}{18} \qquad \mu(x) = \frac{4}{18}\Big(1 + q_1(x)q_2(x)\Big) = \frac{2x^2 + 5x + 6}{18}$$

3.2.2 Radici di un polinomio

Definizione 3.9 (Radice di un polinomio)

Sia K un campo; una *radice* di un polinomio

$$f(x) = a_n x^n + \dots a_1 x + a_0 \in K[x]$$

è un $x_0 \in K$ tale che $f(x_0) = 0$.

Lemma 3.1

Sia K un campo e sia $f(x) \in K[x]$, con $x_0 \in K$ una sua radice; allora

$$f(x) = (x - x_0)g(x)$$

con $g(x) \in K[x]$ e tale che $\deg g = \deg f - 1$.

Dimostrazione. Per l'algoritmo di Euclide, dividendo per $x - x_0$, si trovano unici $q(x), r(x) \in K[x]$ tali che

$$f(x) = q(x)(x - x_0) + r(x)$$

con $\deg r < \deg(x - x_0) = 1$. Quest'ultima disuguaglianza implica che $r(x)$ è un polinomio costante. Inoltre, si nota che, valutando tale espressione in $x = x_0$:

$$0 = q(x_0)(x_0 - x_0) + r(x_0) \implies r(x_0) = r(x) = 0$$

pertanto $g(x) = q(x)$ è il polinomio cercato. □

Teorema 3.3

Sia L un campo e sia $f(x) \in L[x]$ un polinomio di grado $n > 0$; allora f ha, al più, n radici distinte in L.

Dimostrazione. Se $f(x)$ non ha radici, allora l'enunciato è verificato. Se $f(x)$ ha radice $\alpha_1 \in L$, allora si sa che

$$f(x) = (x - \alpha_1)f_1(x)$$

Continuando questa decomposizione finché non si arriva ad un polinomio $h(x)$ tale che

$$f(x) = \prod_{i=1}^{t}(x - \alpha_i)h(x)$$

con $h(x)$ che non ha radici in L, con $t \leq n$ per questioni di grado e con eventuali ripetizioni, si è sicuri che non vi siano altre radici; infatti, se vi fosse una diversa scomposizione con β_1 radice diversa da tutte le precedenti, il che porterebbe alla fattorizzazione

$$f(x) = \prod_{i=1}^{s}(x - \beta_i)\gamma(x)$$

con $\gamma(x) \in L[x]$ polinomio senza radici, questo risulterebbe in un assurdo: valutando $f(x)$ in β_1, che si è assunta essere diversa da tutte le $\alpha_i, i = 1, \ldots, t$, si ha una fattorizzazione per cui $f(x) = 0$ e un'altra (quella con le α_i) per cui $f(x) \neq 0$. □

3.2.3 Ciclicità dei sottogruppi moltiplicativi finiti di un campo

Il teorema 3.3 appena dimostrato permette di concludere il seguente.

Teorema 3.4

Sia K un campo e sia G un sottogruppo di K^* (quindi è un sottogruppo moltiplicativo), con $|G| < \infty$; allora G è ciclico.

Dimostrazione. Sia $|G| = n$; se $n = 1$, l'enunciato è banale, quindi si assume $n > 1$. Visto che $\forall n \in \mathbb{Z}^{>0}$ vale

$$\sum_{d|n} \phi(d) = n$$

con $d \in \mathbb{Z}^{>0}$, prendendo

$$X_d = \{a \in G \mid o(a) = d\}$$

con $d \mid n$, vale anche che

$$\sum_{d|n} |X_d| = n$$

Se G non fosse ciclico, allora $|X_n| = 0$, per cui dovrebbe esistere un intero $d > 0$ tale che $d \mid n \Rightarrow d < n$ e tale che $|X_d| > \phi(d) \geq 1$. Sia, allora, $g \in X_d$, per cui $o(g) = d$ e tutti gli elementi di $\langle g \rangle$ (sottogruppo ciclico di G generato da g) sono radici di $x^d - 1$. In $\langle g \rangle$, ci sono esattamente $\phi(d)$ elementi di ordine d, quindi, essendo $|X_d| > \phi(d)$, si trova $h \in X_d : h \notin \langle g \rangle$, con h radice di $x^d - 1$. A questo punto, però, $x^d - 1$ avrebbe $d + 1$ radici in K, il che è assurdo. □

Corollario 3.1

Per ogni $p \in \mathbb{Z}$ numero primo, il gruppo $\mathbb{Z}_p^*$ è ciclico, visto che è un sottogruppo moltiplicativo del campo $\mathbb{Z}_p$.

3.3 Proprietà di base degli anelli

Lemma 3.2

Sia A un anello; allora $\forall a, b \in A$ vale:

(a). $a \cdot 0 = 0 \cdot a = 0$;

(b). $\exists! - a \in A : a + (-a) = -a + a = 0$ e $-(-a) = a$;

(c). $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ e, in particolare, $(-1) \cdot a = a \cdot (-1) = -a$;

(d). $(-a) \cdot (-b) = a \cdot b$ e, in particolare, $(-1) \cdot (-1) = 1$.

Dimostrazione. Si dimostrano i vari punti.

(a). Si nota che

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Sottraendo $a \cdot 0$ ad ambo i membri, si rimane con $a \cdot 0 = 0$. L'altra si dimostra analogamente.

(b). Già mostrato per i gruppi.

(c). Per mostrare che $a \cdot (-b) = -(a \cdot b)$, si mostra che $a \cdot b + a \cdot (-b) = 0$. Per la proprietà distributiva:

$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$$

(d). Si applica due volte il punto (c):

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$$

dove l'ultima deriva dal punto (b).

□

Osservazione 3.3. Si nota che, per la proprietà (a) appena dimostrata, nel momento in cui in un anello A si verifichi $1 = 0$, allora $\forall a \in A,\ 0 = a \cdot 0 = a \cdot 1 = a$. Questo vuol dire che A è l'anello banale.

Proposizione 3.3

Un campo è automaticamente anche un dominio.

Dimostrazione. Sia K un campo; se, per assurdo, fosse $br = 0$ per $b, r \in K,\ b, r \neq 0$, allora si possono moltiplicare ambo i membri per l'inverso di b, per esempio, e trovare che $r = 0$, il che è assurdo. □

Proposizione 3.4 (Legge di cancellazione)

In ogni dominio R vale la legge di cancellazione, cioè $\forall a \in R,\ a \neq 0$:

$$ab = ac \implies b = c$$

Dimostrazione. È sufficiente notare che $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0$. Usando il fatto che $a \neq 0$ e che si è in un dominio, deve risultare $b - c = 0 \Rightarrow b = c$. □

La legge di cancellazione non vale in generale per qualunque anello, infatti, in $\mathbb{Z}_{12}$, $[3][4] = [3][8] \nRightarrow [4] = [8]$.

Definizione 3.10 (Sottoanello)

Sia R un anello; un suo sottoinsieme $T \subseteq R$ è detto *sottoanello* se:

(sr 1). $1 \in T$;

(sr 2). T è un sottogruppo di R rispetto a $+$;

(sr 3). $\forall a, b \in T \Rightarrow ab \in T$.

3.3.1 Omomorfismi di anelli

Definizione 3.11 (Omomorfismo di anelli)

Siano R, S due anelli; una mappa $\phi : R \to S$ è detta *omomorfismo di anelli* se $\forall a, b \in R$:

(or 1). $\phi(a+b) = \phi(a) + \phi(b)$;

(or 2). $\phi(ab) = \phi(a)\phi(b)$;

(or 3). $\phi(1_R) = 1_S$.

Se ϕ è biettiva, allora è un isomorfismo di anelli.

Definizione 3.12 (Kernel di un omomorfismo)

Il nucleo di $\phi : R \to S$ omomorfismo di anelli è definito come l'insieme

$$\operatorname{Ker}\phi = \{a \in R \mid \phi(a) = 0_S\}$$

Essendo gli omomorfismi di anelli un caso particolare di omomorfismo di gruppi, vale la seguente proposizione esattamente come valeva per i gruppi.

Proposizione 3.5

Il nucleo di un omomorfismo di anelli $\phi : R \to S$ è un sottogruppo additivo di R.

In aggiunta a questa, il nucleo di un omomorfismo di anelli soddisfa anche la seguente proprietà, che lo renderà quello che sarà noto come **ideale**.

Proposizione 3.6

Sia $\phi : R \to S$ un omomorfismo di anelli; allora $\forall a \in \operatorname{Ker}\phi$, si ha $ar \in \operatorname{Ker}\phi$ e $ra \in \operatorname{Ker}\phi$, $\forall r \in R$.

Dimostrazione. Visto che $a \in \operatorname{Ker}\phi \Rightarrow \phi(a) = 0_S$; allora

$$\phi(ar) = \phi(a)\phi(r) = 0_S\phi(r) = 0_S \implies ar \in \operatorname{Ker}\phi$$

Analogamente si verifica l'altro. □

Sempre perché un omomorfismo di anelli è un caso particolare di omomorfismo di gruppi, vale che $\phi : R \to S$ è iniettiva se e solo se $\operatorname{Ker}\phi = \{0_R\}$. Si nota, comunque, che il nucleo non è un sottoanello di R in generale; infatti, dovendo soddisfare $\phi(1_R) = 1_S \Rightarrow 1_R \notin \operatorname{Ker}\phi$, quindi non ha una struttura di anello perché non ha l'elemento neutro rispetto al prodotto. Tuttavia, vale la seguente.

Proposizione 3.7

Sia $\phi : R \to S$ un omomorfismo di anelli; allora $\phi(R)$ è un sottoanello di S.

Dimostrazione. Evidentemente $1_S \in \phi(R)$ per definizione di omomorfismo. È anche verificato che $\phi(R)$ è un sottogruppo additivo di S per quanto dimostrato sui gruppi. Infine, $\forall a, b \in \phi(R) \Rightarrow ab \in \phi(R)$ perché se $a = \phi(\alpha),\ b = \phi(\beta)$

$$ab = \phi(\alpha)\phi(\beta) = \phi(\alpha\beta) \implies ab \in \phi(R)$$

□

Proposizione 3.8

Dati $\phi : R \to S$, $\psi : S \to T$ due omomorfismi di anelli, la loro composizione $\psi \circ \phi : R \to T$ è ancora un omomorfismo di anelli.

3.3.2 Ideali e generatori

Definizione 3.13 (Ideale)

Un sottoinsieme $I \subseteq R$, con R anello, è detto *ideale* se:

(D1). I è un sottogruppo additivo di R;

(D2). $\forall r \in R, \forall h \in I$ si ha $hr \in I$ e $rh \in I$.

La proprietà moltiplicativa che caratterizza gli ideali, quindi, è tale da *assorbre* a destra e a sinistra gli elementi dell'anello di riferimento.

Osservazione 3.4. Si nota che la definizione data è riferita in particolare all'oggetto noto come **ideale bilatero**; avendo solamente a che fare con anelli commutativi per il resto della trattazione, non si farà differenza con il concetto di ideale non-bilatero.

Osservazione 3.5. Si nota che un ideale I non è un sottoanello di R a parte il caso in cui $I = R$. Infatti, se $1 \in I \Rightarrow I = R$ per la proprietà di assorbimento.

Definizione 3.14 (Ideale generato)

Dato R un anello commutativo e dato $a \in R$ un suo elemento, si definisce l'ideale generato da a come l'insieme

$$\langle a \rangle = \{ra \mid r \in R\}$$

Più in generale, se $a_1, \ldots, a_k \in R$ sono k suoi elementi, l'ideale da loro generato è:

$$\langle a_1, \ldots, a_k \rangle = \{r_1 a_1 + \ldots + r_k a_k \mid r_1, \ldots, r_k \in R\}$$

Definizione 3.15 (Ideale principale)

Sia $I \subseteq R$ un ideale di un anello R; si dice che I è un *ideale principale* se $\exists a \in R : I = \langle a \rangle$.

Osservazione 3.6. In generale, non è detto che ogni ideale di un anello R sia principale; infatti in $\mathbb{Z}[x]$, l'ideale $\langle 3, x \rangle$ non è principale.

Osservazione 3.7. Come accennato precedentemente, il nucleo di un omomorfismo $\phi : R \to S$ è un ideale bilatero di R.

Proposizione 3.9

Se I e J sono due ideali di R anello, allora anche $I + J = \{i + j \mid i \in I, j \in J\}$ e $I \cap J$ sono ideali di R.

Dimostrazione. Si è già dimostrato che somma ed intersezione di gruppi abeliani (ogni sottogruppo di un gruppo abeliano è ancora abeliano) restituisce ancora un gruppo. Per finire, si nota che $\forall r \in R,\ \forall i \in I, \forall j \in J$

$$r(i + j) = ri + rj = i' + j' \in I + J$$

dove $ri \in I$ e $rj \in J$ perché I, J sono ideali. Per l'intersezione, questa proprietà segue dalla definizione di intersezione stessa. □

Proposizione 3.10

Se I e J ono due ideali dell'anello R, allora anche

$$IJ = \left\{ i_1 j_1 + \ldots + i_n j_n \mid i_1, \ldots, i_n \in I,\ j_1, \ldots, j_n \in J \right\}$$

è un ideale di R, con $IJ \subset I \cap J$. Inoltre, tale inclusione può essere stretta.

Dimostrazione. Sia $h = \sum_{k=1}^{n} i_k j_k$; evidentemente $\forall r \in R$

$$rh = r \sum_{k=1}^{n} i_k j_k = \sum_{k=1}^{n} r i_k j_k = \sum_{k=1}^{n} i'_k j_k$$

con $i'_k \in I,\ \forall k = 1, \ldots, n$ perché I è un ideale, quindi $rh \in IJ$. È verificato che IJ è un sottogruppo perché I e J lo sono, infatti l'identità è ottenuta dal prodotto delle identità, l'elemento inverso di $ij \in IJ$ è dato da $-(ij) = (-i)j = i(-j)$ e la chiusura rispetto alla somma segue per costruzione di IJ. □

3.3.3 Anelli quoziente

Sia I un ideale di un anello R; si indica con R/I l'insieme delle classi laterali di I in R, considerando I come sottogruppo additivo di R. Allora gli elementi di R/I saranno insiemi (classi laterali) della forma $a + I$ al variare di $a \in R$.

Visto che I è un sottogruppo additivo di R, che è anche normale perché R è un gruppo additivo abeliano, allora R/I ha sicuramente una struttura da gruppo additivo, con somma data da

$$(a+I)+(b+I)=(a+b)+I$$

Per parlare di *anello quoziente*, è necessario dotare R/I di un prodotto; la scelta più naturale è:

$$(a+I)(b+I)=ab+I$$

Per verificare che sia un'operazione ben definita, si mostra che se $a+I=a'+I$ e $b+I=b'+I$, allora $ab+I=a'b'+I$.

Dimostrazione. Il fatto che $a+I=a'+I$ significa che $a'=a+i,\ i\in I$; analogamente $b+I=b'+I\Rightarrow b'=b+j,\ j\in I$. Allora

$$a'b'+I=(a+i)(b+j)+I=ab+aj+bi+ij+I$$

Ricordando che I è un ideale e che, quindi, possiede la proprietà di assorbimento, i termini $aj, bi, ij\in I$, quindi la classe laterale risultante è proprio $ab+I$. □

Rimane da dimostrare che, con tali operazioni, R/I è un anello.

Dimostrazione. La parte della somma si è già fatta per il gruppo quoziente in quanto I è un sottogruppo additivo di R anello commutativo. Rimane da verificare che il prodotto appena definito rispetti le condizioni di prodotto per un anello.

- La proprietà associativa del prodotto è verificata da

$$\Big((a+I)(b+I)\Big)(c+I)=(ab+I)(c+I)=abc+I=(a+I)\Big((b+I)(c+I)\Big)$$

- L'elemento neutro è dato da $1+I$, infatti:

$$(a+I)(1+I)=a+I$$

- La distributività deriva da

$$(a+I)\Big[(b+I)+(c+I)\Big]=(a+I)\Big[(b+c)+I\Big]=a(b+c)+I=(ab+ac)+I=(ab+I)+(ac+I)$$

□

A questo punto, è possibile riportare in teoria degli anelli il primo teorema di omomorfismo.

Teorema 3.5 (Primo teorema di omomorfismo)
Sia $\phi : R \to S$ un omomorfismo di anelli; allora

$$R/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$$

Dimostrazione. La dimostrazione è analoga al caso dei gruppi. □

Anche in questo caso è possibile definire l'omomorfismo canonico $\pi : R \to R/I$, con R anello e $I \subseteq R$ un suo ideale; questo permette la costruzione di un diagramma commutativo analogo al caso dei gruppi. La costruzione di tale omomorfismo canonico permette anche di riportare ogni ideale come nucleo di un omomorfismo in base alla seguente.

Proposizione 3.11
Sia R un anello; ogni suo ideale I può essere visto come il nucleo di un omomorfismo.

Dimostrazione. Si considera la proiezione $\pi : R \to R/I$, cioè la mappa che ad ogni $r \in R$, associa la classe laterale di I, $r + I$. Si verifica che π è un omomorfismo di anelli e che $\operatorname{Ker}\pi = I$. □

3.3.4 Omomorfismi di valutazione

Sia R un anello tale che $\exists A \subset R$ con A sottoanello commutativo di R. Allora, $\forall r \in R$ si può definire la mappa

$$V_r : A[x] \to R \qquad V_r[f(x)] = f(r),\ \forall f(x) \in A[x]$$

Questo è un omomorfismo di anelli.

Dimostrazione. Evidentemente

$$\begin{aligned} &V_r[f(x)g(x)] = f(r)g(r) = V_r[f(x)]V_r[g(x)] \\ &V_r[f(x) + g(x)] = f(r) + g(r) = V_r[f(x)] + V_r[g(x)] \\ &V_r[u(x)] = V_r[1_A] = 1_A \end{aligned}$$

□

Gli omomorfismi di valutazione possono aiutare la comprensione dei quozienti di anelli. Per capirne l'utilità, si considera il seguente esempio.

Esempio 3.2. Si prendono $K = \mathbb{R}$ e $i \in \mathbb{C}$. Successivamente si considera l'omomorfismo di valutazione $V_i : \mathbb{R}[x] \to \mathbb{C}$. È evidente che tale omomorfismo è suriettivo perché ogni numero complesso $a + ib \in \mathbb{C}$ è raggiunto da $V_i[f(x)]$ con $f(x) = a + bx$. Ora se ne studia il nucleo; intanto è ovvio che $x^2 + 1 \in \mathbb{R}[x]$ viene mappato in 0 per

costruzione, quindi $x^2+1 \in \operatorname{Ker} V_i$. Conseguentemente, ogni multiplo di x^2+1 è anch'esso contenuto nel nucleo, quindi

$$\langle x^2+1\rangle \subseteq \operatorname{Ker} V_i$$

È possibile mostrare che $\langle x^2+1\rangle \supseteq \operatorname{Ker} V_i$; per farlo, si prende un generico $f(x) \in \operatorname{Ker} V_i$ (cioè un polinomio tale che $f(i)=0$) e se ne considera la divisione euclidea per x^2+1:

$$f(x) = (x^2+1)q(x) + r(x)$$

dove $r(x)=0$, oppure è un polinomio di grado ≤ 1, quindi, in generale, avrà la forma $r(x)=a+bx$, con $a,b \in \mathbb{R}$. Applicando l'omomorfismo di valutazione a questa relazione, si trova

$$f(i) = 0 \cdot q(x) + a + ib = a + ib = 0 \implies a = b = 0$$

visto che a,b sono reali. Questo mostra che $f(x)$ è multiplo di x^2+1, quindi $f(x) \in \langle x^2+1\rangle$, pertanto $\operatorname{Ker} V_i = \langle x^2+1\rangle$.
Per il primo teorema di omomorfismo, segue che

$$\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$$

3.4 Quozienti di anelli di polinomi

3.4.1 Il quoziente $K[x]/\langle f(x)\rangle$

Si studiano i quozienti della forma $K[x]/\langle f(x)\rangle$, con K campo e $f(x) \in K[x]$. Se $f(x) = 0 \Rightarrow \langle f(x)\rangle = \{0\}$, quindi $K[x]/\langle f(x)\rangle \cong K[x]$. Se, invece, $f(x) = a \in K$ costante, con $a \neq 0$, si ha $\langle a\rangle = K[x]$, quindi il quoziente è banale perché è composto da una sola classe laterale coincidente con tutto l'anello.

Si assume, allora, che $\deg f = n \geq 1$; l'idea è che nel quoziente si sta imponendo $f(x)=0$ perché ciascun polinomio che è multiplo di $f(x)$ viene identificato con la classe di resto $[0]$. Per capirlo meglio, si considera il seguente esempio.

Esempio 3.3. Sia $K=\mathbb{R}$ e $f(x)=x^2+1 \in \mathbb{R}[x]$; allora in $\mathbb{R}[x]/\langle x^2+1\rangle$ vale la relazione $x^2+1=0$, cioè $x^2=-1$, perché ogni multiplo di x^2+1 viene mandato in 0 (o meglio, in $[0]$) dal quoziente, che si occupa di classificare in classi di resto separate i valori del resto per divisione euclidea dei vari polinomio di $K[x]$ con x^2+1. Considerando $p(x) = 3x^4 - 5x^3 + x - \sqrt{3} \in \mathbb{R}[x]$, la sostituzione porta a:

$$3x^4 - 5x^3 + x - \sqrt{3} = -5x(-1) + 3(-1)^2 + x - \sqrt{3} = 6x + (3 - \sqrt{3})$$

Questo vuol dire che $p(x) \equiv 6x + (3-\sqrt{3}) \pmod{x^2+1}$.

Il discorso appare più evidente se si considera il processo appena svolto come applicato alla divisione euclidea; dato $p(x) \in K[x]$, questo si scrive come $p(x) = q(x)f(x) + r(x)$, ma se $f(x) = 0$, allora si rimane con il rappresentante della classe di equivalenza $r(x)$.

Questo permette di concludere che ogni elemento di $K[x]/\langle f(x)\rangle$ è il laterale di un polinomio di grado minore di quello di $f(x)$, analogamente a quanto succedeva per $\mathbb{Z}/m\mathbb{Z}$.

Proposizione 3.12

Sia K un campo e R un anello contenente K come sottoanello; allora R è uno spazio vettoriale su K con le ovvie operazioni di somma e prodotto per scalare.

Dimostrazione. Per definizione, R ha la struttura di gruppo additivo abeliano, perciò gli assiomi legati alla somma sono automaticamente soddisfatti.

Riguardo al prodotto per scalare, questo è definito come $\cdot : K \times R \to R$. Essendo $K \subset R$, valgono tutte le proprietà richieste dagli assiomi perché R è un anello e contiene K. □

Proposizione 3.13

Sia K un campo e $f(x) \in K[x]$ un polinomio con $\deg f = n \geq 1$. Sia, poi, $K[x]/\langle f(x)\rangle \supset K' = \{c + \langle f(x)\rangle \mid c \in K\}$ il sottoinsieme delle classi laterali dei polinomi costanti; allora K' è un sottoanello di $K[x]/\langle f(x)\rangle$ che è isomorfo a K e $K[x]/\langle f(x)\rangle$ è uno spazio vettoriale su K' di dimensione n.

Dimostrazione. Si nota che la mappa $\phi : K' \to K$ tale che $\phi(c + \langle f(x)\rangle) = c$ è un omomorfismo. È, inoltre, possibile verificare che è suriettiva, in quanto $\forall c \in K$, $\phi(c + \langle f(x)\rangle) = c$, e che è iniettiva perché $\phi(c_0 + \langle f(x)\rangle) = 0 \iff c_0 = 0$ per definizione.

Visto che $K \cong K'$, significa che anche K' ha una struttura di campo, pertanto è un sottoanello di $K[x]/\langle f(x)\rangle$; allora, per la proposizione precedente, $K[x]/\langle f(x)\rangle$ è uno spazio vettoriale su K'. Quanto alla dimensione, si è dimostrato che in $K[x]/\langle f(x)\rangle$ ci sono polinomi di grado al massimo $n-1$ per l'algoritmo di Euclide; allora, visto che un polinomio di grado $n-1$ ha n gradi di libertà, la dimensione dello spazio è proprio n. □

Esempio 3.4. Sia $K = \mathbb{Z}_2$ e $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Per quanto appena dimostrato, $\mathbb{Z}[2]/\langle x^2 + x + 1\rangle$ è uno spazio vettoriale su $K = \left\{c + \langle x^2 + x + 1\rangle \mid c \in \mathbb{Z}_2\right\} \cong \mathbb{Z}_2$ ed è di dimensione 2. I suoi elementi sono $\overline{0}, \overline{1}, \overline{x}$ e $\overline{x+1}$; inoltre, è possibile verificare che

$$\overline{x}(\overline{x+1}) = \overline{1} \iff x(x+1) \equiv 1 \pmod{x^2 + x + 1}$$

Segue che $\mathbb{F}_4 = \mathbb{Z}_2/\langle x^2 + x + 1\rangle$ è un campo con 4 elementi.

Osservazione 3.8. Si scrive $\overline{g}(x)$ per indicare il laterale $g(x) + \langle f(x)\rangle \in K[x]/\langle f(x)\rangle$. Si

nota che $f(\overline{x}) = 0 \in K[x]/\langle f(x)\rangle$, infatti:

$$\begin{aligned} f(\overline{x}) &= a_n\overline{x}^n + \ldots + a_1\overline{x} + a_0 \\ &= a_n(x^n + \langle f(x)\rangle) + \ldots + a_1(x + \langle f(x)\rangle) + a_0(1 + \langle f(x)\rangle) = \sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{n} a_j \langle f(x)\rangle \\ &= \sum_{i=0}^{n} a_i x^i + \langle f(x)\rangle = \overline{a_n x^n + \ldots + a_1 x + a_0} \\ &= \overline{f(x)} = \overline{0} \in K[x]/\langle f(x)\rangle \end{aligned}$$

Questo vuol dire che l'anello costruito, cioè $K[x]/\langle f(x)\rangle$, contiene K[a] e ha una radice di $f(x) \in K[x]$.

[a] Come notato precedentemente, $K[x]/\langle f(x)\rangle$ contiene un sottoanello isomorfo a K, cioè quello delle classi laterali dei polinomi costanti.

3.4.2 Polinomi irriducibili

Definizione 3.16 (Polinomio irriducibile)

Sia K un campo e $f(x) \in K[x]$ un polinomio di grado ≥ 1. Si dice che $f(x)$ è *irriducibile* se gli unici divisori di $f(x)$ sono i polinomi costanti diversi da 0 e i polinomi associati a $f(x)$.

Una maniera equivalente per definire l'irriducibilità è dire che, quando in $K[x]$ si ha una relazione della forma

$$f(x) = a(x)b(x)$$

significa che uno fra $a(x)$ e $b(x)$ è un polinomio costante diverso da 0.

Teorema 3.6

Sia K un campo e $f(x) \in K[x]$; allora il quoziente $K[x]/\langle f(x)\rangle$ è un campo se e solo se $f(x)$ è un polinomio irriducibile.

Dimostrazione. Si mostra l'implicazione $\Leftarrow$; siano, allora, $f(x) \in K[x]$ irriducibile e $I = \langle f(x)\rangle$. Per mostrare che $K[x]/I$ è un campo, è sufficiente mostrare che se $a(x) + I$ è un elemento di $K[x]/I$ diverso da $0 + I$, allora ammette un inverso. Si nota che $\gcd(a, f) = 1$ perché, essendo irriducibile, $f(x)$ ha 1 e $f(x)$ come unici divisori, a meno di associati; di questi, solo 1 divide anche $a(x)$, altrimenti $a(x) \equiv 0 \pmod{f(x)}$ e $a(x) \in 0 + I$, contrario a quanto assunto. Per Bézout

$$\lambda(x)a(x) + \mu(x)f(x) = 1$$

Questa relazione, permette di concludere che $\lambda(x) + I$ è l'inverso di $a(x) + I$ in

$K[x]/I$ perché

$$(a(x)+I)(\lambda(x)+I) = a(x)\lambda(x)+I = a(x)\lambda(x)+\mu(x)f(x)+I = 1+I$$

visto che $\mu(x)f(x)+I = 0+I$.

Per l'implicazione $\Rightarrow$, invece, si assume che $f(x)$ non sia irriducibile e si nota che ci si trova in uno dei seguenti casi.

- $f(x) = 0$, quindi $K[x]/\langle 0\rangle \cong K[x]$, quindi non è un campo.
- $\deg f = 0 \Rightarrow f(x) = k \in K^*$, quindi $\langle f(x)\rangle = K[x] \Rightarrow K[x]/\langle f(x)\rangle \cong \{0\}$, che non è un campo.
- $f(x)$ si fattorizza come $f(x) = g_1(x)g_2(x)$, con $1 \leq \deg g_1, \deg g_2 < \deg f$; in questo caso, le classi $g_1(x)+I$ e $g_2(x)+I$ sono entrambe diverse da $0+I$ per questioni di grado. Inoltre

  $$(g_1(x)+I)(g_2(x)+I) = f(x)+I = 0+I$$

  Visto che in $K[x]$ ci sono dei divisori di 0 diversi da 0, $K[x]/I$ non solo non è un campo, ma non è neanche un dominio.

□

3.4.3 Anelli euclidei

L'anello $K[x]$ permette una divisione con resto in analogia con quanto possibile in $\mathbb{Z}$ con la divisione euclidea. L'idea, ora, è di trovare una struttura per tutti quegli anelli che condividono tale analogia.

Definizione 3.17 (Anello euclideo)

Un dominio D è detto *anello euclideo* se esiste una mappa $g : D \setminus \{0\} \to \mathbb{N}$, detta *grado*, tale che

(a). $\forall a, b \in D$, con $a, b \neq 0$, vale $g(a) \leq g(ab)$;

(b). $\forall a, b \in D$, con $b \neq 0$, esistono $q, r \in D : a = qb+r$, dove $r = 0$, oppure $g(r) < g(b)$.

Evidentemente, il grado per gli interi $\mathbb{Z}$ è la funzione valore assoluto (dove si ignora il fatto che è ben definita anche per 0, mentre la funzione grado generica non lo è), mentre per i polinomi di $K[x]$, tale funzione, è il relativo grado.

Lemma 3.3

In un anello euclideo D, per $a, b \in D$ con $a, b \neq 0$, se $b \mid a$ e $a \nmid b$, allora $g(b) < g(a)$.

Dimostrazione. Visto che $b \mid a$ per assunzione, sia $a = bc$. Se $a \nmid b$, allora $b = qa + r$,

con $r \neq 0$ e $g(r) < g(a)$. D'altra parte, $r = b - aq = b - bcq = b(1 - cq) \Rightarrow g(r) \geq g(b)$, per cui $g(a) > g(b)$. □

Proposizione 3.14

Sia D un dominio; allora $b \in D^* \iff \langle b \rangle = D$.

Dimostrazione. Si divide la dimostrazione nelle due implicazioni.

- ($\Rightarrow$) Sia b invertibile, cioè $b \in D^*$; allora $\forall d \in D,\ d = db^{-1}b = rb$, per $r = db^{-1} \in D$.
- ($\Leftarrow$) Sia $\langle b \rangle = D$; allora $\exists a \in D : ab = 1 \Rightarrow b$ è invertibile.

□

Lemma 3.4

In un anello euclideo D, vale $g(1) \leq g(b),\ \forall b \in D$ e $g(b) = g(1) \iff b \in D^*$.

Dimostrazione. Per la prima affermazione, si nota che $\forall b \in D,\ g(b) = g(1b) \geq g(1)$.
Per la seconda parte, invece, si usa che b è invertibile $\iff \langle b \rangle = D$.

- ($\Rightarrow$) Sia $g(b) = g(1)$ e sia $a \in D$; allora $a = qb + r$, con $r = 0$ o $g(r) < g(b)$, ma b ha grado minimo, quindi $r = 0$. Ne segue che $a \in \langle b \rangle,\ \forall a \in D \implies D = \langle b \rangle$.
- ($\Leftarrow$) Sia $b \in D^*$; allora $\langle b \rangle = D$, quindi $\forall a \in D$, si trova $r \in D$ tale che $a = rb$. Da questo, segue che $\forall a \in D,\ g(a) \geq g(b)$, quindi $g(b)$ ha il grado minore fra tutti, per cui $g(b) = 1$.

□

3.5 Fattorizzazione negli anelli euclidei

3.5.1 Proprietà di base

Definizione 3.18 (PID)

Un dominio è detto *a ideali principali* (PID) se tutti i suoi ideali sono principali.

Esempio 3.5. L'anello dei polinomi a coefficienti costanti $K[x, y]$, con K campo, non è a ideali principali perché l'ideale $I = \langle x, y \rangle$ non può essere generato da un solo elemento.

Dimostrazione. Sia $f \in K[x, y] : \langle f \rangle = I$. Questo significa che f divide ogni elemento di I, in particolare $x = gf$ e $y = hf$, per qualche coppia $g, h \in K[x, y]$. Quindi f divide contemporaneamente sia x, che y, ma questi due polinomi sono coprimi; allora f deve essere al massimo una costante (cioè un elemento di K), il che significherebbe che è invertibile e, conseguentemente, che $1 \in I \Rightarrow I = K[x, y]$.

Tuttavia, quanto appena dimostrato è un assurdo perché $\langle x, y\rangle \neq K[x, y]$, visto che $1 \notin \langle x, y\rangle$. □

Teorema 3.7

Sia D un anello euclideo; allora D è un dominio a ideali principali.

Dimostrazione. Sia I un ideale di D; se $I = \{0\}$, la tesi è vera perché $I = \langle 0\rangle$, quindi si considera solo il caso $I \neq \{0\}$.

Si considera l'insieme $S = \{g(c) \mid c \in I \setminus \{0\}\}$, con g la funzione grado definita su D. Questo insieme è non vuoto, quindi, per il principio del minimo, ne ammette uno; sia questo m.

Sia, quindi, $b \in I : g(b) = m$; si vuole dimostrare che $I = \langle b\rangle$. Per farlo, si osserva che $\forall \gamma \in I$, si può usare la divisione euclidea per scrivere $\gamma = bq + r$, dove $r = 0$, oppure $g(r) < g(b)$. Però si vede che $r = \gamma - bq \in I$ perché $\gamma \in I$ e $bq \in I$ per assorbimento, quindi $r = 0$ perché altrimenti esisterebbe un elemento di I di grado inferiore a b, il che sarebbe un assurdo. Questo significa che ogni elemento di I è multiplo di b. □

Definizione 3.19 (Massimo comune divisore per anelli euclidei)

Sia D un anello euclideo e siano $a, b \in D$ due elementi non entrambi nulli. Si definisce *massimo comune divisore* di a e b come quell'elemento $d \in D$ tale che:

- $d \mid a$ e $d \mid b$;
- $\forall c \in D : c \mid a$ e $c \mid b$, si ha $c \mid d$.

Al contrario del caso di $\mathbb{Z}$ e $\mathbb{K}[x]$, qui il massimo comune divisore non è unico in generale e non c'è un modo privilegiato di sceglierlo. Se a, b sono non entrambi nulli, il procedimento per trovare operativamente un massimo comune divisore è eseguire l'algoritmo di Euclide fino ad arrivare all'ultimo resto non-nullo: questo sarà un massimo comune divisore di a e b. Questo è dovuto al fatto che è possibile dimostrare un lemma analogo a quanto visto per $\mathbb{Z}$, dove l'insieme dei divisori comuni di a, b è uguale a quello di $d, 0$.

Inoltre, ripercorrendo indietro l'algoritmo, si può esprimere $d = \lambda a + \mu b$, con $\lambda, \mu \in D$. Per questa ragione, d è nell'ideale $\langle a, b\rangle$ e ne è un generatore, visto che divide ogni suo elemento.

Sia, ora, d' un altro MCD di a, b; visto che sono entrambi dei massimi comuni divisori, deve valere contemporaneamente $d \mid d'$ e $d' \mid d$, per cui, rispettivamente

$$\begin{cases} d' = sd \\ d = td' \end{cases} \implies d' = sd = std' \Rightarrow d'(1 - st) = 0$$

Visto che D è un dominio, deve valere $1 - st = 0$, da cui s, t sono invertibili. Questo implica che d e d' sono elementi associati. Visto che ciascun massimo comune divisore

di a, b è associato ad un altro e genera l'ideale $\langle a, b \rangle$, si può dare la seguente, equivalente, definizione di MCD.

Definizione 3.20 (Massimo comune divisore per anelli euclidei)
Sia D un anello euclideo e siano $a, b \in D$ due elementi non entrambi nulli. Sia, poi, d un generatore dell'ideale $\langle a, b \rangle$; allora si dirà che d è un massimo comune divisore di a, b.

Osservazione 3.9. Riprendendo quanto visto per i polinomi, cioè che dati $f(x), g(x) \in \mathbb{K}[x]$ su un campo $\mathbb{K}$, il loro MCD è l'unico polinomio monico che li divide e genera l'ideale $\langle f, g \rangle$ che, quindi, è principale. Per quanto visto, ogni altro generatore di questo ideale è associato a $\gcd(f, g)$.

Dalle considerazioni tratte finora, è possibile arrivare al seguente enunciato del teorema di Bézout.

Teorema 3.8 (Teorema di Bézout per anelli euclidei)
Sia D un anello euclideo. Dati $a, b \in D$ non entrambi nulli, sia $\gcd(a, b)$ un loro massimo comune divisore; allora esistono $\lambda, \mu \in D$ tali che

$$\gcd(a, b) = \lambda a + \mu b$$

Osservazione 3.10. Più in generale, è possibile usare la definizione di MCD data in 3.20 anche per PID e vale un analogo del teorema di Bézout. Se il dominio non è euclideo, però, non esiste, in generale, un algoritmo di Euclide per calcolare concretamente un MCD.

3.5.2 Elementi irriducibili ed elementi primi

Definizione 3.21 (Elemento irriducibile)
Sia D un dominio e sia $\pi \in D$ un suo elemento. Si dirà che π è irriducibile se $\pi \neq 0$, $\pi \notin D^*$ e se $\forall \gamma, \delta \in D : \pi = \gamma\delta \Rightarrow \gamma \in D^*$ o $\delta \in D^*$.

Esempio 3.6. Per $D = \mathbb{Z}$, gli irriducibili sono gli elementi della forma $\pm p$, con p primo. In $D = \mathbb{R}[x]$, invece, sono i polinomi di grado 1 e i polinomi di grado 2 che non hanno radici reali: questo è diretta conseguenza del teorema fondamentale dell'algebra.

Definizione 3.22 (Elemento primo)
Un elemento π di un dominio di integrità D si dice *primo* se $\pi \neq 0$, $\pi \notin D^*$ e se $\forall \gamma, \delta \in D : \pi \mid \gamma\delta \Rightarrow \pi \mid \gamma$, o $\pi \mid \delta$.

Per i domini, la condizione di essere primo è una condizione più forte di essere irriducibile.

Proposizione 3.15

Sia D un dominio; se $\pi \in D$ è primo, allora è irriducibile.

Dimostrazione. Siano $\gamma, \delta \in D : \pi = \gamma\delta$; allora $\pi \mid \gamma\delta$, perciò $\pi \mid \gamma$, o $\pi \mid \delta$. Senza perdita di generalità, si può assumere che $\pi \mid \gamma$; allora $\exists \nu \in D : \gamma = \pi\nu \Rightarrow \pi\gamma\delta = \pi\nu\delta$. Essendo D un dominio, si può cancellare π e ottenere che $1 = \nu\delta \Rightarrow \delta$ è invertibile. □

In generale, il viceversa è falso, ma non nei dominio euclidei.

Proposizione 3.16

Sia D un dominio euclideo; se $\pi \in D$ è irriducibile, allora è anche primo.

Dimostrazione. Siano $\gamma, \delta \in D : \pi \mid \gamma\delta$, quindi $\exists \kappa \in D : \gamma\delta = \pi\kappa$. Assumendo senza perdita di generalità che π non divida γ, si dimostra che $\pi \mid \delta$.

Visto che π è irriducibile, i suoi divisori sono tutti e soli gli elementi associati a 1 (cioè gli invertibili) e a se stesso (ossia gli elementi della forma $\nu\pi$ con $\nu \in D^*$) (da dimostrare). Per questo, gli MCD di π e γ sono gli associati di 1 (da dimostrare), quindi, per Bézout, $\exists y, z \in D : y\gamma + z\pi = 1$. Moltiplicando per δ:

$$\delta = y\gamma\delta + z\pi\delta = y\pi\kappa + z\pi\delta = \pi(y\kappa + z\delta)$$

quindi $\pi \mid \delta$. □

Teorema 3.9 (Esistenza e unicità della scomposizione in fattori irriducibili)

Sia D un anello euclideo e $a \in D : a \neq 0$ e non invertibile; allora esistono $p_1, \dots, p_r \in D$ irriducibili tali che $a = p_1 p_2 \cdots p_r$.

Inoltre, se si trovano altri $q_1, \dots, q_s \in D$ irriducibili tali che $a = q_1 \cdots q_s$, allora $r = s$ e $\exists \tau \in S_r : p_i$ è associato a $q_{\tau(i)}$, $\forall i = 1, 2, \dots, r$.

Dimostrazione. Per l'esistenza, si fa uso della funzione grado come visto per $\mathbb{Z}$ (da dimostrare).

Per l'unicità, invece, sia $r < s$; si procede per induzione su r. Il passo base per $r = 1$ è il seguente: $s = 1$, altrimenti a sarebbe contemporaneamente irriducibile ($a = p_1$) e non irriducibile ($a = q_1 \cdots q_s$). A questo punto, segue direttamente che $a = p_1 = q_1$.

Per il passo induttivo, si suppone $r > 1$ e che l'enunciato sia vero quando la prima fattorizzazione ha $r - 1$ fattori irriducibili. Visto che $p_1 \mid a = q_1 q_2 \cdots q_s = q_1(q_2 \cdots q_s)$, deve valere $p_1 \mid q_1$, oppure $p_1 \mid (q_2 \cdots q_s)$; nel primo caso, essendo p_1, q_1 irriducibili e $p_1 \mid q_1$, segue che sono associati, quindi $q_1 = kp_1$, $k \in D^*$. Allora, dividendo a per p_1, si ottiene:

$$p_2 p_3 \cdots p_r = k q_2 \cdots q_s$$

A sinistra si ha il prodotto di $r-1$ fattori irriducibili e a destar il prodotto di $s-1$ fattori irriducibili[a]. Per ipotesi induttiva, si sa che $r-1=s-1$ e che queste due fattorizzazioni coincidono, quindi in questo caso il teorema è dimostrato.

Se, invece, valesse $p_1 \mid (q_2 \cdots q_s)$, si può iterare il ragionamento e, in un numero finito di passi, si trova un indice i tale che p_1 è associato a q_i: analogamente a prima, il teorema è dimostrato per induzione. □

[a] Il fattore k non invalida tale affermazione perché è invertibile e il teorema richiede che le due fattorizzazioni coincidano a meno di associati

3.6 Gli interi di Gauss

Definizione 3.23 (Anello degli interi di Gauss)

L'insieme $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ è chiamato *anello degli interi di Gauss*.

Proposizione 3.17

L'insieme $\mathbb{Z}[i]$ è un anello euclideo.

Dimostrazione. Dimostrare per esercizio che è un anello.

L'anello $\mathbb{Z}[i]$ è un dominio, visto che è un sottoanello del campo $\mathbb{C}$. Come funzione grado, si prende il modulo quadro:

$$g : \begin{array}{ccc} \mathbb{Z}[i]\setminus\{0\} & \longrightarrow & \mathbb{N} \\ a+ib & \longmapsto & |a+ib|^2 = a^2+b^2 \end{array}$$

Per $z, w \in \mathbb{Z}[i]\setminus\{0\}$, si ha $g(zw) \geq z$ perché $|zw|^2 \geq |z|^2$, essendo $|w| \geq 1$ (perché a, b sono interi).

Si considerano, ora, tutti i multipli di $w \in \mathbb{Z}[i]$, con $w \neq z$ e $w \neq 0$, per dimostrare che esiste la divisione euclidea di z per w. Questi, nel piano complesso, formano un reticolo composto dai vertici di quadrati di lato $|w|$ e ogni punto del piano è in uno di questi quadrati, o più di uno se si trova al bordo. In particolare, z starà sempre in uno di questi quadrarti. Ora, preso $Q = w_0 w$ un vertice che ha distanza minima da z, se ne può stimare la distanza nel caso peggiore in cui z è nel centro del quadrato:

$$|z - w_0 w| \leq \frac{|w|}{\sqrt{2}} \implies g(z-w_0 w) \leq \frac{g(w)}{2} < g(w)$$

Questo permette di prendere w_0 come quoziente e $z - w_0 w$ come resto della divisione, cioè $z = ww_0 + (z - w_0 w)$. □

3.6.1 Fattorizzazione in $\mathbb{Z}[i]$

Si vogliono studiare gli elementi irriducibili nell'anello $\mathbb{Z}[i]$.

Lemma 3.5

Sia $p \in \mathbb{Z}$ un numero primo dispari che non è irriducibile in $\mathbb{Z}[i]$; allora p si scrive come somma di due quadrati di numeri interi.

Dimostrazione. Sia, quindi, $p \in \mathbb{Z}$ un elemento non irriducibile in $\mathbb{Z}[i]$, per cui $p = (a+bi)(c+di)$, con $a+bi, c+di \in \mathbb{Z}[i]$ e non invertibili, quindi deve valere $g(a+ib) = a^2+b^2 > 1$ e $c^2+d^2 > 1$ per il lemma 3.4.

Visto che $p = \overline{p}$ (visto che è un intero), si ha $p = (a-bi)(c-di)$, quindi, moltiplicando ambo i membri per le due relazioni, si ottiene $p^2 = (a^2+b^2)(c^2+d^2)$. Dato che $a^2+b^2 > 1$ e $c^2+d^2 > 1$, allora $a^2+b^2 = p$ e $c^2+d^2 = p$. □

Lemma 3.6

Sia $p \in \mathbb{Z}$ un primo della forma $4n+1$; allora la congruenza $x^2 \equiv -1 \pmod{p}$ ammette soluzione in $\mathbb{Z}$.

Dimostrazione. Sia $x = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)/2$; visto che $p-1 = 4n$, nel prodotto precedente compare un numero pari di termini, quindi

$$x = (-1)(-2)\cdots\left(-\frac{p-1}{2}\right)$$

A questo punto, è sufficiente notare che

$$\begin{aligned} x^2 &= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2} \cdot (-1) \cdot (-2) \cdot \ldots \cdot \left(-\frac{p-1}{2}\right) \\ &\equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-1) \equiv (p-1)! \equiv -1 \pmod{p} \end{aligned}$$

dove l'ultima congruenza segue dal teorema di Wilson. □

Teorema 3.10

Sia $p \in \mathbb{Z}$ un numero primo della forma $4n+1$; allora p non è irriducibile in $\mathbb{Z}[i]$ ed esistono $a, b \in \mathbb{Z} : p = a^2+b^2$.

Dimostrazione. È sufficiente mostrare che p non è irriducibile in $\mathbb{Z}[i]$; il resto deriva direttamente dal primo dei due precedenti lemmi.

Sia, allora, $x \in \mathbb{Z} : x^2 \equiv -1 \pmod{p}$ (questo x esiste per il lemma precedente); allora $p \mid (x^2+1) = (x-i)(x+i)$. Se p fosse irriducibile in $\mathbb{Z}[i]$, allora dovrebbe valere $p \mid (x+i)$ per esempio, per quanto affermato dal proposizione 3.16. Questo, però, vorrebbe dire che esistono $c, d \in \mathbb{Z} : p(c+id) = x+i$ da cui, uguagliando le parti immaginarie, $pd = 1$, il che è assurdo. □

Teorema 3.11

Sia p un primo dispari della forma $4n+3$; allora p non può essere scritto come somma di due quadrati.

Dimostrazione. Sia $p = a^2+b^2$, con $a, b \in \mathbb{Z}$; dato che p è dispari, allora a e b devono

essere uno pari e l'altro dispari necessariamente.

Senza perdita di generalità, si assume che sia a pari e b dispari, per cui $a^2 \equiv 0 \pmod 4$ e $b^2 \equiv 1 \pmod 4$ (da verificare). Allora:

$$p = a^2 + b^2 \equiv 1 + 0 \equiv 1 \pmod 4$$

che è assurdo perché $p \equiv 3 \pmod 4$. □

Corollario 3.2

I primi della forma $4n+3$ sono irriducibili in $\mathbb{Z}[i]$.

Dimostrazione. Per il lemma 3.5, si sa che se un primo dispari non è irriducibile in $\mathbb{Z}[i]$, allora si scrive come somma di due quadrati. Visto che i primi della forma $4n+3$ non si possono scrivere in tal modo, segue che devono essere irriducibili in $\mathbb{Z}[i]$. □

Teorema 3.12

Tutti e i soli elementi irriducibili di $\mathbb{Z}[i]$ sono, a meno di associati, i primi di $\mathbb{Z}$ nella forma $4n+3$ e gli $z \in \mathbb{Z}[i] : g(z) = |z|^2$ è un primo di $\mathbb{Z}$.

Dimostrazione. Si divide la dimostrazione nelle due implicazioni.

- ($\Leftarrow$) Sia $p = 4n+3$ un primo; per il corollario precedente, si ha che è irriducibile in $\mathbb{Z}[i]$. Se $g(z) = p$, con p primo, allora z è irriducibile perché, scrivendo $z = w_1 w_2$ e considerando i quadrati delle norme, si ha $p = |w_1|^2 |w_2|^2$, da cui una delle due norme deve essere pari a 1, pertanto uno dei fattori di z è invertibile.

- ($\Rightarrow$) Sia $z \in \mathbb{Z}[i]$ irriducibile, quindi $z \mid z\bar{z} = g(z) = q_1 \dots q_s$, dove i q_i sono primi di $\mathbb{Z}$ (si è fattorizzato $g(z)$ in $\mathbb{Z}$). Per la prop. 3.16, si deve avere che $z \mid q_i$, per un certo i, pertanto $zw = q_i$, per $w \in \mathbb{Z}[i]$. Ma allora q_i è un primo della forma $4n+3$, quindi z, a meno di associati, è un primo di tale tipo. Se, invece, w non è invertibile, allora $|w|^2 \neq 1$ e, passando ai quadrati, si ha $|z|^2 |w|^2 = q_i^2$ e $|z|^2 = q_i$.

□

3.6.2 Fattorizzazione in $\mathbb{Z}[\sqrt{n}]$

Si studiano, ora, gli anelli della forma $\mathbb{Z}[\sqrt{n}]$, dove anche $\mathbb{Z}[\sqrt{-m}] = \mathbb{Z}[i\sqrt{m}]$, con $m > 0$ è ammesso. Gli interi di Gauss appena studiati fanno parte di questa famiglia di anelli.

Osservazione 3.11. Qualora n fosse un quadrato, si avrebbe $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$.

Per questa osservazione, si considereranno solo gli n detti *square free*, cioè dati dal prodotto di due primi distinti, tutti con esponente pari a 1.

È possibile dimostrare che degli anelli così definiti non sono euclidei, ma è comunque possibile definire una *seminorma* nel seguente modo:

$$\ell : \begin{array}{ccc} \mathbb{Z}[\sqrt{n}] & \longrightarrow & \mathbb{Z} \\ a+b\sqrt{n} & \longmapsto & a^2-nb^2 \end{array} \tag{3.6.1}$$

Lemma 3.7

L'applicazione ℓ è moltiplicativa.

Dimostrazione. Siano $a+b\sqrt{n}, c+d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$; si nota che:

$$\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right) = ac+bdn+(ad+bc)\sqrt{n}$$

Da questo, si ottiene che:

$$\begin{aligned} \ell\left[\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right)\right] &= (ac+bdn)^2 - n(ad+bc)^2 \\ &= a^2c^2 + 2abcdn + b^2d^2n^2 - a^2d^2n - 2abcdn - b^2c^2n \\ &= c^2(a^2-nb^2) - nd^2(a^2-nb^2) = (a^2-nb^2)(c^2-nd^2) \\ &= \ell\left(a+b\sqrt{n}\right)\ell\left(c+d\sqrt{n}\right) \end{aligned}$$

□

Lemma 3.8

Un elemento $z \in \mathbb{Z}[\sqrt{n}]$ è invertibile se e solo se $\ell(z) \in \{-1,1\}$.

Dimostrazione. Si divide la dimostrazione nelle due implicazioni.

- ($\Rightarrow$) Se $z \in \mathbb{Z}[\sqrt{n}]$ ed è invertibile, allora $zw = 1$ per qualche $w \in \mathbb{Z}[\sqrt{n}]$. Per il lemma precedente, si ha: $\ell(z)\ell(w) = \ell(1) = 1 \Rightarrow \ell(z) \in \{-1,1\}$.
- ($\Leftarrow$) Sia $z = a+b\sqrt{n}$, con $|\ell(z)| = 1$; allora $|a^2-nb^2| = 1$, per cui

  $$\left(a+b\sqrt{n}\right)\left(a-b\sqrt{n}\right) = 1 \text{ oppure } \left(a+b\sqrt{n}\right)\left(-a+b\sqrt{n}\right) = 1$$

  e, in ogni caso, z risulta invertibile.

□

Nello studio di anelli di questa forma, se ne possono trovare alcuni che non sono a fattorizzazione unica, come ad esempio $\mathbb{Z}[\sqrt{10}]$.

Proposizione 3.18

L'anello $\mathbb{Z}[\sqrt{10}]$ non è un dominio a fattorizzazione unica.

Dimostrazione. Si può direttamente osservare che 6 può essere scritto come

$$\left(4+\sqrt{10}\right)\left(4-\sqrt{10}\right) = 6 = 2\cdot 3$$

Per concludere che $\mathbb{Z}[\sqrt{10}]$ non è a fattorizzazione unica, però, è necessario mostrare che gli elementi che appaiono nelle due fattorizzazioni siano irriducibili.

Si mostra che 2 e 3 sono irriducibili. Se $2 = \left(a+b\sqrt{10}\right)\left(c+d\sqrt{10}\right)$ fosse una fattorizzazione senza invertibili, allora

$$\ell\left(a+b\sqrt{10}\right)\ell\left(c+d\sqrt{10}\right) = \ell(2) = 4$$

perciò le due seminorme a primo membro devono essere entrambe 2 o -2 (non può essere che una delle due sia uguale a ± 1, altrimenti l'elemento sarebbe invertibile). Questo, però, non è possibile perché $a^2 - 10b^2 = \pm 2$ non ha soluzioni intere. In maniera del tutto analoga, si vede che 3 è irriducibile, perché l'equazione $a^2 - 10b^2 = 3$ non ha soluzioni intere.

L'irriducibilità di $4+\sqrt{10}$ e $4-\sqrt{10}$ è diretta conseguenza dei conti già svolti; infatti, visto che tali elementi hanno seminorma pari a 6, perché $4+\sqrt{10}$ avesse una fattorizzazione senza invertibili, per esempio, dovrebbe avere fattori con seminorma pari a 2 e 3 rispettivamente, ma queste relazioni non sono possibili nell'anello, per quanto appena visto. □

Una conseguenza diretta di questa proposizione è che $\mathbb{Z}[\sqrt{10}]$ non è euclideo.

Osservazione 3.12. Si nota che in $\mathbb{Z}[\sqrt{10}]$, 2 è irriducibile, ma non è primo; infatti, si ha che $2 \mid (4+\sqrt{10})(4-\sqrt{10})$, ma non divide nessuno dei due fattori. Un modo per vederlo è che se fosse $2(a+b\sqrt{10}) = 4+\sqrt{10}$, allora $\ell(2) \mid \ell(4+\sqrt{10})$, che è falso perché $4 \nmid 6$.

3.7 Approfondimenti sull'irriducibilità

Si è visto che se K è un campo, allora tutti gli ideali di $K[x]$ sono della forma $\langle f(x)\rangle$, per qualche $f(x) \in K[x]$. Inoltre, se f è irriducibile, allora $K[x]/\langle f(x)\rangle$ è un campo contenente un sottoanello isomorfo a K (dato dalle classi dei polinomi costanti) ed è uno spazio vettoriale su K, la cui dimensione è uguale al grado di $f(x)$. Inoltre, in questo campo, il polinomio $f(x)$ ha una radice data dalla classe di x.

Il punto della sezione è affrontare le due seguenti domande.

(a). Cosa succede se $f(x)$ non è irriducibile? Si è già visto che, in questo caso, $K[x]/\langle f(x)\rangle$ non è un campo, ma si svilupperà più in dettaglio l'argomento.

(b). Che forma hanno i polinomi irriducibili di $K[x]$? Quanti sono e come si ricavano?

Tali domande sono piuttosto complicate e non saranno sviluppate del tutto, ma si getteranno le basi per tale approfondimento.

3.7.1 Il teorema cinese del resto

Sia K un campo e $f(x)$ un polinomio di $K[x]$. Si denota con $\overline{b(x)} := b(x) + \langle f(x)\rangle \in K[x]/\langle f(x)\rangle$ la classe di resto di $b(x) \in K[x]$.

Si assume che $f(x)$ sia irriducibile e si prendono $g(x), h(x) \in K[x]$ tali che $f(x) = g(x)h(x)$, con $\deg g, \deg h \geq 1$. In questo caso, g e h sono divisori non banali dello zero in $K[x]/\langle f(x)\rangle$. Per studiare meglio $K[x]/\langle f(x)\rangle$, si dà la seguente definizione e si studia un esempio analogo già affrontato.

Definizione 3.24 (Prodotto diretto di anelli)
Siano A_1, A_2 due anelli; il loro prodotto diretto $A_1 \times A_2$ è ottenuto definendo, su tale insieme, le operazioni

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2) \qquad (a_1, a_2) \cdot (b_1, b_2) := (a_1 b_1, a_2 b_2)$$

Con queste due operazioni, si può dimostrare che $A_1 \times A_2$ è un anello (da dimostrare). È, inoltre, possibile far vedere che se A_1 e A_2 sono non-banali, allora $A_1 \times A_2$ non è mai un campo (da dimostrare).

Esempio 3.7. Una situazione analoga è già stata affrontata: sia $n \in \mathbb{Z} : n = ab \geq 2$, con $a, b > 1$ due interi. Per studiare l'anello quoziente $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n\rangle$, si osserva l'esistenza di una mappa

$$f : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ [c]_n & \longmapsto & \left([c]_a, [c]_b\right) \end{array}$$

Dimostrare che f è ben definita e che è un omomorfismo di anelli.
Per il teorema cinese del resto, se $\gcd(a, b) = 1$, allora f è biettiva e, quindi, $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Tornando a $K[x]/\langle f(x)\rangle$, con $f(x) = g(x)h(x) : \deg g, \deg h \geq 1$, se $\gcd(h, g) = 1$, tramite ragionamenti analoghi, si può dimostrare che

$$\varphi : K[x]/\langle f(x)\rangle \longrightarrow K[x]/\langle g(x)\rangle \times K[x]/\langle h(x)\rangle \tag{3.7.1}$$

è un isomorfismo di anelli. Per mostrare l'analogo di quanto visto per $\mathbb{Z}/n\mathbb{Z}$, si deve ricavare l'analogo del teorema cinese del resto per i polinomi, tramite il teorema di Bézout e la divisione euclidea (da dimostrare).

Queste considerazioni, possono essere estese più in generale, come mostrato dai due seguenti teoremi.

Teorema 3.13 (Teorema cinese del resto generale)

Sia R un anello e siano I_1, I_2 due ideali tali che $I_1 + I_2 = R$; allora $I_1 I_2 = I_1 \cap I_2$ e l'omomorfismo

$$\Gamma : \begin{array}{ccc} R & \longrightarrow & R/I_1 \times R/I_2 \\ r & \longmapsto & (r + I_1, r + I_2) \end{array}$$

è suriettivo, quindi $R/I_1 I_2 \cong R/I_1 \times R/I_2$.

Teorema 3.14

Sia R un anello e siano $I_1, I_2, \ldots, I_n$ degli ideali tali che, per ogni coppia di indici (i, j), vale $I_i + I_j = R$; allora $I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \ldots \cap I_n$ e l'omomorfismo

$$\Gamma : \begin{array}{ccc} R & \longrightarrow & R/I_1 \times R/I_2 \times \ldots \times R/I_n \\ r & \longmapsto & (r + I_1, r + I_2, \ldots, r + I_n) \end{array}$$

è suriettivo, quindi

$$R/I_1 I_2 \ldots I_n \cong R/I_1 \times R/I_2 \times \ldots \times R/I_n$$

3.7.2 Irriducibilità in $\mathbb{Z}_p[x]$ e $\mathbb{Z}[x]$

In generale, stabilire l'irriducibilità di un polinomio è un problema difficile, ma c'è una classe di campi K in cui questo problema in $K[x]$ è più semplice: tali campi sono i **campi finiti**. L'obiettivo sarà studiare i campi $\mathbb{Z}_p[x]$.

La semplificazione è che, in questo campo, sono presenti un numero finito di polinomi monici di grado $d \in \mathbb{N}$, cioè p^d, e i possibili fattori propri di un polinomio di grado n in $\mathbb{Z}_p[x]$ sono da cercare proprio fra questi per $1 \leq d \leq n-1$.

Esempio 3.8. Si descrivono i polinomi irriducibili (monici) in $\mathbb{Z}_2[x]$ di grado piccolo. Oltre a x e $x+1$, per trovare quelli per grado ≤ 3 è sufficiente verificare che non abbiano radice in $\mathbb{Z}_2$, cosa che richiede due verifiche immediate: le valutazioni in $[0]_2$ e $[1]_2$ devono essere nulle.
In questo modo, si trovano i polinomi irriducibili di ordine 2 e 3, che sono

$$x^2 + x + 1 \qquad x^3 + x^2 + 1 \qquad x^3 + x + 1$$

Per quelli di grado 4, bisogna verificare anche che non ci siano fattori di grado 2; visto che esiste un solo irriducibile di grado due, non è difficile verificare che gli irriducibili di grado 4 in $\mathbb{Z}_2[x]$ sono

$$x^4 + x^3 + x^2 + x + 1 \qquad x^4 + x^3 + 1 \qquad x^4 + x + 1$$

Dimostrare i due seguenti punti.

(a). Sia $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio con $a_n \neq 0 \neq a_0$ e sia p/q una sua radice, con $p, q \in \mathbb{Z} : q \neq 0$ e $\gcd(p, q) = 1$; mostrare che $q \mid a_n$ e $p \mid a_0$.

(b). Descrivere un algoritmo che, in un numero finito di passi, decide se un dato polinomio in $\mathbb{Q}[x]$ ha una radice razionale e, in tal caso, ne calcola una.

Proposizione 3.19

Siano A_1, A_2 due anelli e $\varphi : A_1 \to A_2$ un omomorfismo di anelli; mostrare che

$$\hat{\varphi} : \begin{array}{ccc} A_1[x] & \longrightarrow & A_2[x] \\ f(x) & \longmapsto & \varphi(a_n)x^n + \ldots + \varphi(a_1)x + \varphi(a_0) \end{array}$$

definisce un omomorfismo di anelli.

Si usa questo omomorfismo nel caso della proiezione al quoziente $\varphi : \mathbb{Z} \to \mathbb{Z}_p$, con p primo.

Definizione 3.25 (Polinomio primitivo)

Un polinomio $f(x) \in \mathbb{Z}[x]$ è detto *primitivo* se il MCD dei suoi coefficienti è 1.

Proposizione 3.20

Sia p un primo e $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ la proiezione al quoziente. Sia, inoltre, $\hat{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ l'omomorfismo della proposizione precedente e sia $f(x) = a_n x^n + \ldots a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio primitivo con $n \geq 1$ tale che $p \nmid a_n$; allora, se $\hat{\varphi}(f(x))$ è irriducibile in $\mathbb{Z}_p[x]$, si ha che $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione. Si procede per controposizione. Sia, quindi, $f(x) = g(x)h(x)$ riducibile, con $g, h \in \mathbb{Z}[x]$; visto che f è primitivo, si deve avere per forza $\deg g, \deg h \geq 1$[a]. Si nota che

$$\hat{\varphi}(f(x)) = \hat{\varphi}(g(x))\hat{\varphi}(h(x))$$

e $\deg \hat{\varphi}(f(x)) = \deg f(x) = n$ perché, per ipotesi, $\varphi(a_n) \neq [0]_p$. Questo significa che deve anche valere $\deg \hat{\varphi}(g(x)), \deg \hat{\varphi}(h(x)) \geq 1$, il che dimostra che $\hat{\varphi}(f(x))$ è riducibile in $\mathbb{Z}_p[x]$. □

[a] Il fatto che i coefficienti siano in $\mathbb{Z}$, porta l'esistenza di irriducibili di grado 0; ad esempio 7 non è invertibile, quindi è irriducibile: il polinomio $7x + 7$ si fattorizza in 7 e $x + 1$, che sono due irriducibili.

Osservazione 3.13. L'ipotesi di primitività è necessaria perché, per esempio, se $p = 2$ e $f(x) = 3x + 3 = 3(x + 1)$, si avrebbe $\hat{\varphi}(f(x))$ irriducibile, ma non f irriducibile in $\mathbb{Z}[x]$.

Teorema 3.15 (Criterio di Eisenstein)

Sia $p \in \mathbb{N}$ un numero primo e $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio primitivo con $n \geq 1$ tale che:

(a). p non divide a_n;

(b). p divide $a_0, a_1, \ldots, a_{n-1}$;

(c). p^2 non divide a_0.

Allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione. Se $n = 1$, è verificato perché un polinomio primitivo di grado 1 è irriducibile.

Si procede per controposizione. Si assume che $f(x)$ abbia grado ≥ 2 e sia riducibile in $\mathbb{Z}[x]$, con $g, h \in \mathbb{Z}[x]$ non invertibili e tali che $f = g(x)h(x)$. Visto che f è primitivo, g e h saranno non-costanti; applicando l'omomorfismo $\hat{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, dalla precedente proposizione e dall'ipotesi (b), si ottiene che

$$[a_n]_p x^n = \hat{\varphi}(f(x)) = \hat{\varphi}(g(x))\hat{\varphi}(h(x))$$

dove l'ipotesi (a) assicura $[a_n]_p \neq [0]_p$. Si nota che, per polinomi a coefficienti in un campo, il prodotto di due polinomi è un monomio se e solo se entrambi i fattori sono monomi. Siccome $\deg \hat{\varphi}(f(x)) = \deg f(x) = n$, dovrà valere anche che $\deg \hat{\varphi}(g(x)) = \deg g(x) \geq 1$ e $\deg \hat{\varphi}(h(x)) = \deg h(x) \geq 1$, quindi $\hat{\varphi}(g(x))$ e $\hat{\varphi}(h(x))$ sono monomi di grado positivo e, in particolare, i termini costanti di g e h sono entrambi divisibili per p.

Visto che a_0 è il prodotto di questi due coefficienti, però, si dovrebbe avere che $p|^2 \mid a_0$, il che contraddice (c), quindi $f(x)$ non può essere riducibile in $\mathbb{Z}[x]$. □

Esempio 3.9. Per il criterio di Eisenstein, il polinomio $x^5 - 4x + 2$ è irriducibile in $\mathbb{Z}[x]$; infatti, $x^k - 4x + 2$ è irriducibile $\forall k \geq 2$, per cui in $\mathbb{Z}[x]$ ci sono polinomi irriducibili di ogni grado (a differenza di quello che succede in $\mathbb{C}[x]$, o in $\mathbb{R}[x]$).

3.7.3 Irriducibilità in $\mathbb{Q}[x]$

Lemma 3.9 (Teorema di Gauss)

Siano $f(x), g(x) \in \mathbb{Z}[x]$ due polinomi primitivi; allora il loro prodotto $f(x)g(x) \in \mathbb{Z}[x]$ è primitivo.

Dimostrazione. Siano

$$f(x) = \sum_i a_i x^i \qquad g(x) = \sum_j b_j x^j$$

con $a_i, b_j \in \mathbb{Z}$, $\forall i, j$. Si assume che $f(x)g(x)$ non sia primitivo. Sia, quindi, p un primo che divide tutti i coefficienti di tale prodotto e $a_s x^s$, $b_r x^r$ i due termini di grado più alto in $f(x)$ e $g(x)$ rispettivamente, che non siano divisibili per p; allora

il coefficiente di x^{r+s} di $f(x)g(x)$ è

$$\sum_{i+j=s+r} a_i b_j$$

che deve essere divisibile per p. Però p divide sicuramente tutti i termini della somma, ad eccezione di $a_s b_r$, quindi dunque dovrà dividere anche $a_s b_r$ e, in quanto primo, dividerà uno tra a_s e b_r. Questa è una contraddizione, quindi $f(x)g(x)$ deve essere primitivo. □

Corollario 3.3

Un polinomio in $\mathbb{Z}[x]$ di grado positivo è irriducibile in $\mathbb{Z}[x]$ se e solo se è primitivo e irriducibile in $\mathbb{Q}[x]$.

Dimostrazione. Se $f(x) \in \mathbb{Z}[x]$ è primitivo e irriducibile in $\mathbb{Q}[x]$, allora lo sarà anche in $\mathbb{Z}[x]$.

Per l'altra implicazione, invece, si nota che se $f(x) \in \mathbb{Z}[x]$ non è primitivo, non è irriducibile in $\mathbb{Z}[x]$, quindi si può assumere che $f(x) \in \mathbb{Z}[x]$ sia primitivo. Si assume che $f(x) = a(x)b(x)$, con $a(x), b(x) \in \mathbb{Q}[x]$ entrambi di grado positivo e si mostra che $f(x)$ è riducibile in $\mathbb{Z}[x]$.

Si possono trovare $\alpha, \beta \in \mathbb{Q}$ tali che $a'(x) = \alpha a(x) \in \mathbb{Z}[x]$ e $b'(x) = \beta b(x) \in \mathbb{Z}[x]$, con a', b' entrambi primitivi[a]. Per il lemma di Gauss, allora, anche $a'(x)b'(x) = \alpha\beta f(x) \in \mathbb{Z}[x]$ è primitivo. Visto che $f(x)$ è primitivo, si deve avere $\alpha\beta \in \mathbb{Z}$ e, visto che $\alpha\beta f(x)$ è primitivo, si deve anche avere $\alpha\beta = \pm 1$, per cui $f(x) = \pm a'(x)b'(x)$, che dimostra che $f(x)$ è riducibile in $\mathbb{Z}[x]$. □

[a] Ad esempio, α si può ottenere moltiplicando $a(x)$ per il mcm dei denominatori e, poi, si divide, eventualmente, per un intero per rendere il polinomio primitivo.

4 Teoria dei campi

4.1 Introduzione ed estensioni semplici di campi

Come già ripetuto, si è visto che dato un campo K e un polinomio $f(x) \in K[x]$ irriducibile e di grado ≥ 2, è possibile creare un nuovo campo $K[x]/\langle f(x)\rangle$ che contiene K e dove $f(x)$ ammette radice.

A volte, però, è già noto un campo in cui un polinomio ammette radice: nel caso di $x^3-2 \in \mathbb{Q}[x]$, si sa che questo non ammette radice in $\mathbb{Q}$, ma ne ammette in $\mathbb{R}$; si è, quindi, interessati a studiare che relazione sussiste tra il campo $\mathbb{Q}/\langle x^3-2\rangle$ e la presenza di una radice in $\mathbb{R}$. Per affrontare questo discorso, è necessario dare qualche definizione.

Definizione 4.1 (Sottocampo)
Sia E un campo e A un suo sottoanello; si dice che A è un sottocampo di E se $\forall a \in A,\ a \neq 0$, esiste $a^{-1} \in A$.

Sia K un campo e sia L un campo che è un'*estensione* di K, cioè vale $K \subseteq L$. Dato $\alpha \in L$, si considerano tutti i sottocampi di L che contengono sia K che α; la loro intersezione è ancora un sottocampo di L (da dimostrare). Per costruzione, questa intersezione rappresenta il più piccolo campo contenente K e α e, visto che questo è ben definito come sottocampo, ne segue la definizione.

Definizione 4.2 (Estensione semplice)
Siano K, L due campi tali che $K \subseteq L$ e sia α un elemento di L; si indicherà con $K(\alpha)$ il più piccolo sottocampo (rispetto all'inclusione) di L contenente sia K che α e lo si chiamerà *estensione semplice* di K.

Dati $K \subseteq L$ e $\alpha \in L$ come sopra, si può considerare l'omomorfismo di valutazione $\psi : K[x] \to L$ tale per cui $\forall f(x) \in K[x],\ \psi(f(x)) = f(\alpha)$; si indicherà con $K[\alpha]$ l'immagine di ψ perché è effettivamente possibile vedere gli elementi di $\operatorname{Im}\psi$ come polinomi in α a coefficienti in K.

Si nota che il kernel di ψ è l'insieme di tutti i polinomi di $K[x]$ che hanno α come radice. Sapendo che $\operatorname{Ker}\psi$ è un ideale di $K[x]$ e che quest'ultimo è euclideo, segue che $\operatorname{Ker}\psi$ è un ideale principale, quindi:

$$\operatorname{Ker}\psi = \langle f(x)\rangle$$

per qualche $f(x) \in K[x]$. Ora, ci sono due casi: o il nucleo è $\operatorname{Ker}\psi = \{0\}$, relativo all'assenza di polinomi in $K[x]$ che abbiano α come radice (in tal caso si dirà che α è **trascendente** su K) e, per il primo teorema di omomorfismo, vale $K[x] \cong K[\alpha] = \operatorname{Im}\psi$[1], oppure $\operatorname{Ker}\psi = \langle f(x)\rangle \neq \{0\}$ e α si dice **algebrico** su K.

[1] In questo caso particolare, $K[\alpha]$ non è un campo, quindi $K[\alpha] \subsetneq K(\alpha)$.

Definizione 4.3 (Elemento algebrico e polinomio minimo)

Siano $K \subseteq L$ due campi e $\alpha \in L$ un suo elemento; si dice che α è *algebrico* su K se esiste $f(x) \in K[x] : f(x) \neq 0$ con α come radice. In altre parole, $\operatorname{Ker}\psi \neq \{0\}$. Un generatore di $\operatorname{Ker}\psi$ è detto *polinomio minimo* di α su K.

Osservazione 4.1. Per definizione, un polinomio minimo di α su K divide ogni altro polinomio di $K[x]$ che abbia α come radice; questo polinomio non è unico in senso stretto, ma lo è a meno di associati e l'aggettivo *minimo* è riferito al fatto che ha grado minore di tutti i polinomi di $K[x]$ che hanno α come radice.
A volte, viene usata la convenzione per cui IL polinomio minimo è quello che fra tutti i polinomi minimi ha coefficiente direttore unitario.

Si procede nello studio del caso in cui α sia algebrico su K, quindi $\operatorname{Ker}\psi = \langle f(x)\rangle \neq \{0\}$. In questo caso, si nota che f è irriducibile su $K[x]$: se $f(x) = h_1(x)h_2(x)$ fosse una fattorizzazione in $K[x]$, con h_1, h_2 non costanti, si avrebbe $f(\alpha) = h_1(\alpha)h_2(\alpha) = 0 \Rightarrow h_1(\alpha) = 0$ oppure $h_2(\alpha) = 0$, con $\deg f > \deg h_1, \deg h_2$, il che è assurdo perché $f(x)$ genera il nucleo, ma esistono polinomi di grado minore.

Quindi, visto che $\operatorname{Ker}\psi = \langle f(x)\rangle$, con f irriducibile, tramite il primo teorema di omomorfismo, si ottiene che $\operatorname{Im}\psi = K[\alpha]$ è un campo: più esattamente, è un sottocampo di L contenente α e K, quindi $K(\alpha)$.

Allo stesso tempo, si osserva che tutti polinomi in α devono appartenere a $K(\alpha)$, cioè $K[\alpha] \subseteq K(\alpha)$, quindi $K(\alpha) = K[\alpha]$.

Esempio 4.1. Si considera $K = \mathbb{Q}$ e $L = \mathbb{R}$, con $\alpha = \sqrt[3]{2}$. Per definizione, sia $1 + \sqrt[3]{2}$ che il suo inverso $1/(1 + \sqrt[3]{2})$ appartengono a $\mathbb{Q}(\sqrt[3]{2})$, ma si è appena visto che $\mathbb{Q}(\sqrt[3]{2}) = Q[\sqrt[3]{2}]$, perciò si vuole capire come può essere che $1/(1 + \sqrt[3]{2}) \in Q[\sqrt[3]{2}]$.
A questo scopo, si considera l'omomorfismo di valutazione $\psi : \mathbb{Q}[x] \to \mathbb{R}$ che valuta ogni polinomio in $\sqrt[3]{2}$. Si nota che il polinomio minimo di $\sqrt[3]{2}$ è $x^3 - 2$, ossia che $\operatorname{Ker}\psi = \langle x^3 - 2\rangle$, infatti $\langle x^3 - 2\rangle \subseteq \operatorname{Ker}\psi$, ma si vede anche che $x^3 - 2$ è irriducibile in $\mathbb{Q}[x]$[a], quindi genera $\operatorname{Ker}\psi$.
Sia, infatti, $g(x)$ un generatore di $\operatorname{Ker}\psi$; allora deve dividere $x^3 - 2$, ma $x^3 - 2$ è irriducibile, quindi, a meno di associati, si ha $g(x) = 1$, oppure $g(x) = f(x)$: il primo caso si esclude perché implica $\operatorname{Ker}\psi = \mathbb{Q}[x]$, che è assurdo visto che $\psi(1) = 1$. Allora:

$$Q[\sqrt[3]{2}] \cong \mathbb{Q}[x]/\langle x^3 - 2\rangle$$

Ora si studia il quoziente $\mathbb{Q}[x]/\langle x^3 - 2\rangle$. Ogni elemento di questo quoziente si scrive come

$$ax^2 + bx + c + \langle x^3 - 2\rangle,\ a, b, c \in \mathbb{Q}$$

Si considera $x+1+\langle x^3-2\rangle$; i polinomi $x+1$ e x^3-2 sono coprimi, quindi, per il lemma di Bézout, esiste una loro combinazione lineare pari a 1 a coefficienti in $\mathbb{Q}[x]$. Per

trovarla, si usa l'algoritmo di Euclide:

$$x^3-2=(x^2-x+1)(x+1)-3 \implies 1=-\frac{1}{3}(x^3-2)+\frac{1}{3}(x^2-x+1)(x+1)$$

A questo punto, si può verificare che le classi $x+1+\langle x^3-2\rangle$ e $\frac{1}{3}(x^2-x+1)+\langle x^3-2\rangle$ sono una l'inversa dell'altra in $\mathbb{Q}[x]/\langle x^3-2\rangle$.
D'altra parte, valutando l'uguaglianza precedente in $\sqrt[3]{2}$, si ha

$$\begin{aligned}1&=-\frac{1}{3}\left((\sqrt[3]{2})^3-2\right)+\frac{1}{3}\left((\sqrt[3]{2})^2-\sqrt[3]{2}+1\right)\left(\sqrt[3]{2}+1\right)\\ \Rightarrow 1&=\frac{1}{3}\left((\sqrt[3]{2})^2-\sqrt[3]{2}+1\right)\left(\sqrt[3]{2}+1\right)\end{aligned}$$

Questo permette di concludere che, in $\mathbb{R}$:

$$\frac{1}{\sqrt[3]{2}+1}=\frac{1}{3}\left((\sqrt[3]{2})^2-\sqrt[3]{2}+1\right)$$

In questo modo, si è mostrato che l'inverso di $\sqrt[3]{2}+1$ si può scrivere come polinomio in $\sqrt[3]{2}$ e appartiene, quindi, a $\mathbb{Q}[\sqrt[3]{2}]$.
Questo ragionamento, ripetuto per ogni elemento non-nullo, permette di capire perché $\mathbb{Q}[\sqrt[3]{2}]$ sia un campo e indica anche un modo per calcolare gli inversi.
Per finire, si nota che x^3-2 ammette $\sqrt[3]{2}\omega$ e $\sqrt[3]{2}\omega^2$ come radici in $\mathbb{C}$, con $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$.
Analogamente a quanto visto per $\mathbb{Q}[\sqrt[3]{2}]$, usando l'omomorfismo di valutazione

$$\begin{array}{rccc}\psi': & \mathbb{Q}[x] & \longrightarrow & \mathbb{C}\\ & g(x) & \longmapsto & \psi(g(x))=g(\sqrt[3]{2}\omega)\end{array}$$

si può concludere che $\mathbb{Q}[\sqrt[3]{2}\omega]\cong\mathbb{Q}[x]/\langle x^3-2\rangle$. In questo modo, si ha:

$$\mathbb{Q}[\sqrt[3]{2}]\cong\mathbb{Q}[x]/\langle x^3-2\rangle\cong\mathbb{Q}[\sqrt[3]{2}\omega]$$

Chiamando $\theta:\mathbb{Q}[\sqrt[3]{2}]\to\mathbb{Q}[\sqrt[3]{2}\omega]$ tale isomorfismo, si può notare che θ lascia fissi gli elementi di $\mathbb{Q}$ e $\theta(\sqrt[3]{2})=\sqrt[3]{2}\omega$, infatti nel primo isomorfismo, $\sqrt[3]{2}$ viene mappato in $\overline{x}$, e, nel secondo, $\overline{x}$ va in $\sqrt[3]{2}\omega$. Lo stesso discorso vale per $\mathbb{Q}[\sqrt[3]{2}\omega^2]$; in questo modo, si sono trovati tre sottocampi di $\mathbb{C}$ isomorfi tra loro.

[a] Questo si può vedere sia notando che, essendo di grado 3, dovrebbe avere un fattore di grado 1, cioè ammettere una radice razionale e si osserva subito che x^3-2 non ne ammette, oppure si usa il criterio di Eisenstein con $p=2$.

L'ultimo discorso si può generalizzare nel seguente teorema.

Teorema 4.1
Siano $K\subseteq L$ due campi e sia $f(x)\in K[x]$ un polinomio irriducibile che ha radici distinte α,β in L. Allora esiste un isomorfismo $\theta:K[\alpha]\to K[\beta]$ tale che $\theta(\alpha)=\beta$ e θ ristretto a K è l'identità.

Dimostrazione. Da dimostrare. □

I campi $K[\alpha]$ e $K[\beta]$ possono anche essere uguali, oltre che isomorfi, come succede nel caso di $K = \mathbb{Q}$ e $L = \mathbb{C}$, con $f(x) = x^2 + 1$, per cui si trova che $\mathbb{Q}(i) = \mathbb{Q}(-i)$. In generale, però, questi sono diversi.

4.2 Grado delle estensioni

Come già accennato, dati due campi $F \subseteq K$, K è un'estensione di F e si può vedere come spazio vettoriale su F stesso. Da questa struttura di spazio vettoriale, si possono ottenere alcune informazioni.

Definizione 4.4 (Dimensione)

Dati $F \subseteq K$ due campi, il grado di K su F è la dimensione di K come spazio vettoriale su F e viene indicato con $[K : F]$.

Questo grado può essere infinito, se la dimensione è infinita, e si scrive $[K : F] = \infty$; in questo caso, si dice che K è un'estensione infinita di F, altrimenti si dice che è un'estensione finita.

Teorema 4.2

Se L è un'estensione finita di K e K è un'estensione finita di F, allora L è un'estensione finita di F e

$$[L : F] = [L : K][L : F]$$

Dimostrazione. Un modo per calcolare $\dim_F L$ è quello di trovare una base di L su F e contarne gli elementi.

Sia, quindi, $\{v_1, \dots, v_m\}$ una base di L su K e sia $\{w_1, \dots, w_n\}$ una base di K su F; allora, l'enunciato del teorema segue dal fatto che l'insieme $\{v_1, \dots, v_m, w_1, \dots, w_n\}$ è una base di L su F composta da mn elementi.

Per vedere questo, si considera $v \in L$; allora $v = a_1 v_1 + \dots + a_m v_m$, con $a_i \in K$. Visto che ciascun coefficiente in K si può espandere tramite la base di K su F, cioè $a_i = b_{i1} w_1 + \dots + b_{in} w_n$, con $b_{ij} \in F$, allora si può scrivere che:

$$v = \sum_{\substack{i=1,\dots,m \\ j=1,\dots,n}} b_{ij} v_i w_j$$

il che dimostra che $\{v_i w_j\}_{i,j}$ genera L su F, quindi rimane da mostrare l'indipendenza lineare.

Considerando l'uguaglianza

$$\sum_{\substack{i=1,\dots,m\\ j=1,\dots,n}} b_{ij} v_i w_j = 0 = \sum_{i=1}^{m} (b_{i1} w_1 + \dots + b_{in} w_n) v_i$$

e notando che i $v_1, \dots, v_m$ è una base di L su K, si deduce che

$$b_{i1} w_1 + \dots + b_{in} w_n = 0$$

per ogni $i = 1, \dots, m$. Da questa relazione, usando l'indipendenza dei w_j, si ottiene che i b_{ij} sono tutti nulli. □

Corollario 4.1

Se L è un'estensione finita di F e $F \subseteq K \subseteq L$, allora K è un'estensione finita di F e L è un'estensione finita di K. Inoltre, $[L : F] = [L : K][K : F]$.

Dimostrazione. Si considera L come sottospazio vettoriale su F; visto che questo ha dimensione finita e che K è un suo sottospazio vettoriale, allora anche K ha dimensione finita su F.

Rimane da mostrare che L ha dimensione finita su K, ma questo segue direttametne dal fatto che una base di L su F è anche un insieme finito di generatori di L su K.

La dimostrazione è conclusa applicando il teorema precedente, visto che si è dimostrato che le estensioni $F \subseteq K$ e $K \subseteq L$ sono finite. □

4.3 Approfondimenti sulle estensioni di campi

L'obiettivo è la creazione di un campo con tutte le radici di un dato polinomio.

Si ricorda il teorema 3.3, per cui un polinomio di grado $n > 0$ in un campo L ha al più n radici distinte. Vista la possibilità di decomporre univocamente gli irriducibili negli anelli euclidei, se ne può dare una formulazione più forte.

Teorema 4.3

Sia L un campo e sia $f(x) \in L[x]$ un polinomio di grado $n > 0$; allora $f(x)$ ha al più n radici in L, contate con molteplicità.

Dimostrazione. Se $f(x)$ non ha radici, l'enunciato è vero. Se, invece, $f(x)$ ha una radice α_1, si può scrivere

$$f(x) = (x - \alpha_1) f_1(x)$$

Se $f_1(x)$ ha radice α_2, si può proseguire fino a trovare un polinomio $h(x) \in L[x]$ che non ha radici in L e, quindi, che non ha fattori di primo grado in $L[x]$. Questo

permette di scrivere

$$f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_t)h(x)$$

Per fattorizzare $f(x)$ in irriducibili, si deve fattorizzare $h(x)$, ma da questo non usciranno altri fattori di primo grado, per quanto detto prima.

Le t radici evidenziate presentano eventuali ripetizioni, quindi vale $t \leq n$; in ogni fattorizzazione in irriducibili di $f(x)$ compariranno queste radici come unici fattori di primo grado, perciò sono determinati univocamente a meno di associati.

Questo vuol dire che le $\alpha_k, k = 1,\dots,t$ sono le uniche radici di $f(x)$ e ciascuna di queste comparirà in ogni fattorizzazione con la stessa molteplicità. □

Si è visto che, dato un polinomio irriducibile di grado $\geq$ in $K[x]$, sia questo $f(x)$, questo non ha radici in K, ma ne ammette una in $K[x]/\langle f(x)\rangle$, campo che estende K.

Si può pensare, allora, che, iterando il procedimento che aggiunge una radice al polinomio, sia possibile costruire un campo E, che estende K, tale per cui $f(x)$ si fattorizzi nel prodotto di polinomio di grado 1 in $E[x]$.

Teorema 4.4

Sia K un campo e sia $f(x) \in K[x]$ un polinomio di grado $n \geq 0$; allora esistono un campo $E \supseteq K$ e elementi $e_1,\dots,e_n \in E$ (eventualmente con ripetizioni) tali che $f(x)$ si fattorizza, in $E[x]$, nel seguente modo:

$$f(x) = \lambda(x-e_1)\dots(x-e_n)$$

con $\lambda \in E$ costante.

Definizione 4.5 (Campo di spezzamento)

Siano $K \subseteq L$ due campi e sia $f(x) \in K[x]$ tale che $f(x)$ si fattorizza completamente in L come prodotto di fattori di primo grado; allora il più piccolo campo $E \subseteq L$ tale che $K \subseteq E$ e tale che $f(x)$ abbia tutte le radici in E si dice campo di spezzamento di f su K.

Osservazione 4.2. Visto che l'intersezione di campi è ancora un campo, si può dimostrare che, in L, esiste ed è unico il campo di spezzamento di f su K.

Esempio 4.2. Si considera l'elemento $c = \sqrt{2} + \sqrt[3]{2} \in \mathbb{R}$; si dimostra che è algebrico su $\mathbb{Q}$ di grado 6, si trova il suo polinomio minimo e il suo campo di spezzamento.

Svolgimento. Si nota, preliminarmente, che $x^2 - 2$ non è riducibile in $\mathbb{Q}[x]$; infatti, se lo fosse, essendo di grado 2, dovrebbe avere una radice in $\mathbb{Q}$, ma visto che si conoscono già le due radici $\sqrt{2}$ e $-\sqrt{2}$, che appartengono a $\mathbb{R} \setminus \mathbb{Q}$, il polinomio dovrebbe averne una terza reale, che è assurdo.

Si osserva lo stesso per il polinomio x^3-2, che risulta irriducibile in $\mathbb{Q}[x]$; per quanto visto precedentemente, vale che:

$$\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/\langle x^2-2\rangle,\ \left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right] = 2 \qquad \mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[x]/\langle x^3-2\rangle,\ \left[\mathbb{Q}[\sqrt[3]{2} : \mathbb{Q}\right] = 3$$

Vista la catena di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, per il teorema 4.2, si ha che $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$; analogamente notando la catena $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, si ha che 3 divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. Considerando ancora l'ultima catena, visto che $\sqrt{2}$ è radice di x^2-2, il suo polinomio su $\mathbb{Q}(\sqrt[3]{2})$ ha grado ≤ 2; ancora per il teorema 4.2, si ha

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 6$$

Ne segue che $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ è ≤ 6 ed è divisibile sia per 2, che per 3; allora $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.
Ora si considera $c = \sqrt{2} + \sqrt[3]{2} \Rightarrow (c-\sqrt{2})^3 = 2$, da cui

$$c^3 + 6c - 2 = \sqrt{2}(3c^2+2)$$

Da questa uguaglianza si ottiene che $\sqrt{2} \in \mathbb{Q}(c)$; elevando al quadrato, poi, si ha che:

$$(c^3+6c-2)^2 = 2(3c^2+2)^2$$

Si è trovato, quindi, che c è radice di $p(x) = x^6-6x^4-4x^3+12x^2-24x-4$. Per capire se questo è irriducibile, quindi per capire se è polinomio minimo di c su $\mathbb{Q}$, si può fare un'osservazione sui gradi delle estensioni coinvolte; infatti, visto che per il teorema 4.2 vale

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

e che $\mathbb{Q}(c, \sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ (da dimostrare), si sa che

$$[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = 6$$

Inoltre, essendo che $\sqrt{2} \in \mathbb{Q}(c)$, si ha $[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)] = 1$, cioè $\mathbb{Q}(c, \sqrt{2}) = \mathbb{Q}(c)$. Ne segue che $[\mathbb{Q}(c) : \mathbb{Q}] = 6$, per cui il polinomio minimo di c su $\mathbb{Q}$ è di grado 6, e, pertanto, coincide con quello proposto sopra.
Per finire, si cerca il campo di spezzamento su $\mathbb{Q}$ di $p(x)$. Visto che $\sqrt[3]{2}+\sqrt{2}$ è ottenuto sommando una radice di x^3-2 ad una radice di x^2-2, è intuitivo pensare che le sue altre radici siano della stessa forma, cioè $\sqrt[3]{2}\omega^r \pm \sqrt{2}$, con $r = 0, 1, 2$ e ω radice dell'unità.
Per dimostrare che questo è vero, si inizia col notare che $\sqrt[3]{2}\omega+\sqrt{2}$ e $\sqrt[3]{2}\omega^2+\sqrt{2}$ soddisfano la stessa identità di $\sqrt[3]{2}+\sqrt{2}$, cioè $(c-\sqrt{2})^3 = 2$; sviluppando questa relazione allo stesso modo, si trova che sono radici di $p(x)$. Per quanto riguarda, invece, gli

elementi della forma $\sqrt[3]{2}\omega^r - \sqrt{2}$, invece, queste soddisfano

$$(c+\sqrt{2})^3 = 2 \implies c^3 + 6c - 2 = -\sqrt{2}(3c^2+2)$$

Elevando al quadrato, si ottiene nuovamente $(c^3+6c-2)^2 = 2(3c^2+2)^2$, per cui anche queste sono radici di $p(x)$. Visto che il polinomio è di grado 6, queste sono effettivamente tutte le sue radici.
Segue che il campo di spezzamento è contenuto in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}, \omega)$. Per mostrare l'inclusione inversa, si osserva che, dovendo il campo di spezzamento contenere tutte le radici, dovrà contenere anche gli elementi

$$\frac{1}{2}\left[(\sqrt[3]{2}+\sqrt{2}) - (\sqrt[3]{2}-\sqrt{2})\right] = \sqrt{2} \qquad \frac{1}{2}\left[(\sqrt[3]{2}+\sqrt{2}) + (\sqrt[3]{2}-\sqrt{2})\right] = \sqrt[3]{2}$$

$$\frac{(\sqrt[3]{2}\omega+\sqrt{2}) + (\sqrt[3]{2}\omega-\sqrt{2})}{(\sqrt[3]{2}+\sqrt{2}) + (\sqrt[3]{2}-\sqrt{2})} = \omega$$

■

4.4 Approfondimenti sui campi finiti

Si studiano i campi da un diverso punto di vista: si cerca di capire se contenogno un sottoanello isomorfo a $\mathbb{Z}$, o meno.

Si inizia col notare che, dato un campo F, c'è un solo omomorfismo di anelli $\phi : \mathbb{Z} \to F$ determinato dalla condizione $\phi(1) = 1$[1]. Visto, inoltre, che $\mathbb{Z}$ è un anello a ideali principali, si ha che $\operatorname{Ker}\phi = \langle d \rangle$, per qualche $d \geq 0$ intero. Per questo, si hanno i due seguenti casi possibili.

(a). Il nucleo è banale, cioè $d = 0$ e $\operatorname{Ker}\phi = \langle 0 \rangle$. In questo caso, $\operatorname{Im}\phi \cong \mathbb{Z}$, cioè F contiene un sottoanello isomorfo a $\mathbb{Z}$, che si chiamerà ancora $\mathbb{Z}$ per semplicità. Visto, poi, che F è un campo, questo deve contenere tutti gli inversi di $\mathbb{Z}$, perciò esisterà anche un sottocampo isomorfo a $\mathbb{Q}$ (che si chiamerà ancora $\mathbb{Q}$). In questo caso, si dice che F è un campo di *caratteristica* 0.

(b). Si ha $d = p$ primo[2]; allora $\operatorname{Ker}\phi = \langle p \rangle$, quindi, per il primo teorema di omomorfismo, si ha $\operatorname{Im}\phi \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$, per cui F contiene un campo isomorfo a $\mathbb{Z}_p$, che verrà ancora indicato con $\mathbb{Z}_p$. In questo caso, si dirà che F è un campo di *caratteristica* p.

Osservazione 4.3. Si nota che, nel caso di $d = p$ primo, la somma di p addendi

[1] Come preannunciato, si considerano esclusivamente anelli con unità.

[2] Se d non fosse primo, allora $d = rs$, per r, s interi con $1 < s, r < d$, per cui $\phi(r)$ e $\phi(s)$ sarebbero diversi da 0 nel campo K, ma $\phi(r)\phi(s) = \phi(rs) = \phi(d) = 0$, che è assurdo perché in K non ci sono divisori di 0 non banali.

unitari è nulla:

$$\underbrace{1+1+\ldots+1}_{p \text{ addendi}} = \phi(1)+\ldots+\phi(1) = \phi(1+\ldots+1) = \phi(p) = 0$$

Considerando F come spazio vettoriale su $\mathbb{Z}_p$, si nota che $\forall v \in F$, la somma di p addendi $v+\ldots+v$ è ancora nullo perché

$$v+\ldots+v = (1+\ldots+1)v = 0v = 0$$

Si considera, ora, un campo finito L (cioè con un finito numero di elementi); si nota, intanto, che L non può avere caratteristica 0, altrimenti conterrebbe un sottocampo isomorfo a $\mathbb{Q}$, quindi infinito.

Sia, allora, $d = p$ primo la caratteristica di L, per cui L contiene un sottocampo isomorfo a $\mathbb{Z}_p$. Inoltre, il grado di L su $\mathbb{Z}_p$ deve essere un numero finito, sia questo $n \in \mathbb{N}\setminus\{0\}$, altrimenti L avrebbe dimensione infinita come spazio su $\mathbb{Z}_p$, quindi avrebbe elementi infiniti.

Sia $\{v_1,\ldots,v_n\}$ una base di L su $\mathbb{Z}_p$, quindi ogni elemento di L si scrive, univocamente, come $\lambda_1 v_1+\ldots+\lambda_n v_n$, con $\lambda_i \in \mathbb{Z}_p$, $i = 1,\ldots,n$. Visto che, per questi coefficienti, ci sono p possibili scelte per ciascuno, si ottiene che gli elementi di L sono p^n; da questa osservazione, si ottiene la seguente.

Proposizione 4.1

La cardinalità di un capmo finito è un intero della forma p^n, per p primo e $n \in \mathbb{N}\setminus\{0\}$.

Esempio 4.3. Si considera $x^3+x+1 \in \mathbb{Z}_2[x]$[a]; questo è irriducibile (cioè non ha radici in $\mathbb{Z}_2$), pertanto $K := \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ è un campo.
Indicando, per ciascun $f(x) \in \mathbb{Z}_2[x]$, con $\overline{f(x)}$ il laterale $f(x)+\langle x^3+x+1\rangle$, si ha

$$K = \left\{\overline{0},\overline{1},\overline{x},\overline{x+1},\overline{x^2},\overline{x^2+1},\overline{x^2+x},\overline{x^2+x+1}\right\}$$

Quindi K ha 2^3 elementi. Si nota che il sottocampo di K che è isomorfo a $\mathbb{Z}_2$ è $\left\{\overline{0},\overline{1}\right\}$; chiamandolo, abusando della notazione, ancora $\mathbb{Z}_2$, si ha $\mathbb{Z}_2 \subset K$. Visto, infine, che una base di K su $\mathbb{Z}_2$ è, per esempio, $\left\{\overline{1},\overline{x},\overline{x}^2\right\} \subset K$, si ritrova proprio $|K| = 2^3$.

[a] Si sottintende che 0 e 1 siano identificati con le relative classi di equivalenza $[0]_2$, $[1]_2$.

Ora si dimostra l'esistenza di infiniti campi finiti. Per farlo, si inizia introducendo un importante omomorfismo.

Teorema 4.5 (Omomorfismo di Frobenius)

Sia p un numero primo e K un campo di caratteristica p; la funzione $\mathcal{F} : K \to K$, definita da $\mathcal{F}(a) = a^p$, $\forall a \in K$, è un omomorfismo iniettivo.

Dimostrazione. Si mostra intanto che $\mathcal{F}$ è un omomorfismo. Si ha $\mathcal{F}(1) = 1$ e, per

ogni $a, b \in K$, $\mathcal{F}(ab) = (ab)^p = a^p b^p = \mathcal{F}(a)\mathcal{F}(b)$.

Quanto alla somma, bisogna mostrare la relazione $(a+b)^p = a^p + b^p$; questa relazione segue per lo stesso motivo della seconda dimostrazione del piccolo teorema di Fermat: l'uguaglianza si ha perché è possibile sviluppare il primo membro tramite il binomio di Newton, per poi utilizzare che i coefficienti $\binom{p}{i}$, con $1 \leq i \leq p-1$, sono multipli di p, quindi sono nulli in un campo di caratteristica p.

Per l'iniettività, invece, si nota che $\operatorname{Ker}\mathcal{F}$ è un ideale proprio di K perché non può essere $\operatorname{Ker}\mathcal{F} = K$, visto che $\mathcal{F}(1) = 1$. Essendo K un campo, l'unico ideale proprio è $\langle 0 \rangle$. □

Osservazione 4.4. Per quanto appena dimostrato, anche tutte le potenze $\mathcal{F}^j$, $j \in \mathbb{Z}^{>0}$ sono omomorfismi iniettivi.

Teorema 4.6

Sia K un campo e sia $\psi : K \to K$ un omomorfismo; allora l'insieme

$$\operatorname{Fix}\psi = \{k \in K \mid \psi(k) = k\}$$

degli elementi che rimangono invariati sotto ψ forma un sottocampo di K.

Dimostrazione. Intanto si mostra che è un sottoanello di K. Si inizia con l'osservare che $0 \in \operatorname{Fix}\psi$; inoltre, per $r \in \operatorname{Fix}\psi$:

$$\psi(-r) = -\psi(r) = -r \implies -r \in \operatorname{Fix}\psi$$

Dati, poi, $r, s \in \operatorname{Fix}\psi$:

$$\psi(r+s) = \psi(r) + \psi(s) = r + s$$

Quindi $\operatorname{Fix}\psi$ è un sottogruppo rispetto alla somma.

Analogamente, si dimostra che $rs \in \operatorname{Fix}\psi$ perché $\psi(rs) = \psi(r)\psi(s) = rs$ e, per definizione, si ha $1 \in \operatorname{Fix}\psi$, quindi $\operatorname{Fix}\psi$ è un sottoanello di K.

Rimane da dimostrare l'esistenza dell'inverso moltiplicativo. Sia, quindi $r \in \operatorname{Fix}\psi$, $r \neq 0$; allora

$$\psi(r^{-1}) = \psi(r)^{-1} = r^{-1}$$

quindi anche $r^{-1} \in \operatorname{Fix}\psi$, per cui è effettivamente un sottocampo di K. □

Sia L un campo finito con p^n elementi. Il suo gruppo moltiplicativo $L^* = L \setminus \{0\}$ ha, quindi, cardinalità $p^n - 1$, perciò, per un corollario del teorema di Lagrange, $\forall g \in L^*$: $g^{p^n-1} = 1$[1]. Considerando anche lo 0, per $g \in L$, si ha $g^{p^n} = g$.

Questo implica che il polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ ha esattamente p^n soluzioni in L. Più in particolare, tutti gli elementi di L sono radici di $x^{p^n} - x$ e, questo, si fattorizza come

[1] Questo perché l'ordine di un elemento di un gruppo divide l'ordine del gruppo stesso, cioè $g^{|G|} = g^{k \operatorname{ord} g} = (e)^k = e$.

prodotto di fattori di grado 1 in $L[x]$. Allora L è un capmo di spezzamento di $x^{p^n} - x$ su $\mathbb{Z}_p$.

Teorema 4.7

Ogni campo finito ha cardinalità p^n, con p numero primo e n intero positivo. Inoltre, $\forall p$ primo e $n \in \mathbb{Z}^{>0}$, esiste un campo finito di cardinalità p^n.

Dimostrazione. Avendo già dimostrato che questa è una condizione necessaria, cioè un campo, per essere finito, deve avere cardinalità p^n, si dimostra che questa è anche una condizione sufficiente. L'obiettivo è mostrare l'esistenza di un generico campo di p^n elementi, a partire da p primo e n intero positivo generici.

Per iniziare, si assume di avere un'estensione E di $\mathbb{Z}_p$, ottenuta tramite opportuni quozienti, dove $x^{p^n} - x$ ha tutte le radici. Questa estensione ha grado finito[a].

In E, si considera il campo di spezzamento R di $x^{p^n} - x$ su $\mathbb{Z}_p$; questo R ha caratteristica p e ha dimensione finita su $\mathbb{Z}_p$ (visto che è un sottocampo di E), quindi è, a sua volta, un campo finito.

Sia, ora, $L = \{r \in R \mid \mathcal{F}^n(r) = r\}$, con $\mathcal{F} : R \to R$ omomorfismo di Frobenius. Per quanto visto, l'insieme dei punti fissi di un omomorfismo è un sottocampo, di R in questo caso. Ricordando la definizione di omomorfismo di Frobenius, si osserva che gli elementi di L sono anche le radici di $x^{p^n} - x$. Queste sono p^n in quanto sono tutte distinte fra loro[b], da cui segue che L è un campo con p^n elementi. Si conclude, inoltre, che L coincide con R. □

[a] Seguendo il processo dei quozienti, si può stimare che il suo grado sarà $\leq n!$.

[b] Per vedere questo, si usa il criterio della derivata: la derivata di $x^{p^n} - x$ è -1, visto che R ha caratteristica p, quindi non ha radici in comune con $x^{p^n} - x$.

Corollario 4.2

Per ogni coppia di numeri p, n, con p primo e $n \in \mathbb{Z}^{>0}$, esiste un polinomio irriducibile di grado n in $\mathbb{Z}_p[x]$.

Dimostrazione. Sia K un campo finito con p^n elementi e sia α un generatore del gruppo moltiplicativo K^*, che è ciclico per il teorema 3.4; il campo $\mathbb{Z}_p(\alpha)$, allora, coincide con K perché $\mathbb{Z}_p(\alpha)$ è un sottoinsieme di K contenente 0 e tutte le potenze di α, cioè tutti gli elementi di K.

Ne segue che $\mathbb{Z}_p(\alpha) = K$ è un'estensione di grado n su $\mathbb{Z}_p$: chiamando $f(x)$ il polinomio minimo di α, visto che $\mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$, si ha che $\deg f = n$. □

Osservazione 4.5. Si è mostrato che se un campo L è finito, allora ha caratteristica p, ma il viceversa non è vero: esistono campi di caratteristica p che non sono finiti, come, per esempio

$$\mathbb{Z}_p(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Z}_p[x],\ g(x) \neq 0 \right\}$$

il campo delle funzioni razionali.

Teorema 4.8

Sia $f(x) \in \mathbb{Z}_p[x]$ irriducibile e di grado n; allora il campo $K = \mathbb{Z}_p[x]/\langle f(x)\rangle$ è un campo di spezzamento per $f(x)$ su $\mathbb{Z}_p$.

Dimostrazione. Si sa che il campo $K = \mathbb{Z}_p[x]/\langle f(x)\rangle$ ha p^n elementi; in questo campo, $f(x)$ ha una radice α, ma questa è anche radice di $x^{p^n} - x$, visto che ogni elemento di K è radice di tale polinomio. Quindi, essendo che $f(x)$ è irriducibile, questo è il polinomio minimo di α, quindi $f(x) \mid x^{p^n} - x$. Segue che le radici di $f(x)$ sono, in particolare, le radici di $x^{p^n} - x$, pertanto si trovano tutte in K.

Per concludere la dimostrazione, è sufficiente osservare che nessun sottocampo proprio di K può contenere, per ragioni di grado, tutte le radici di $f(x)$: se esistesse un sottocampo contenente α, questo conterrebbe anche $\mathbb{Z}_p(\alpha)$, che ha grado n su $\mathbb{Z}_p$, quindi coinciderebbe con K, anch'esso di grado n su $\mathbb{Z}_p$. □

Teorema 4.9

Sia p primo e $n \in \mathbb{Z}^{>0}$; allora $x^{p^n} - x$ è il prodotto di tutti i polinomi monici irriducibili di $\mathbb{Z}_p[x]$, il cui grado d è divisore di n.

Dimostrazione. Sia $q(x)$ irriducibile in $\mathbb{Z}_p[x]$ e di grado d tale che $d \mid n$. Si mostra che $q(x) \mid x^{p^n} - x$.

Si considera il campo $L = \mathbb{Z}_p[x]/\langle q(x)\rangle$, che è un campo con p^d elementi. Per quanto visto, ogni elementi di L soddisfa $y^{p^d} = y$ e, in L, si ha una radice α di $q(x)$. Per tale α, allora:

$$\alpha^{p^d} = \alpha$$

Visto che $d \mid n$, esiste un intero s tale che $sd = n$, quindi

$$\alpha^{p^n} = (\alpha^{p^d})^{p^{(s-1)d}} = \alpha^{p^{(s-1)d}}$$

A partire da questa, si può mostrare, per induzione su s, che $\alpha^{p^n} = \alpha$, per cui α è una radice di $x^{p^n} - x$. Se ne conclude che $q(x)$ e $x^{p^n} - x$ hanno una radice in comune, α, in L. Essendo $q(x)$ irriducibile, esso è il polinomio minimo di α su $\mathbb{Z}_p[x]$, quindi deve valere $q(x) \mid x^{p^n} - x$.

Ora si dimostra il viceversa, cioè che se $f(x)$ è un polinomio irriducibile di grado d che divide $x^{p^n} - x$, allora $d \mid n$.

A questo proposito, sia L un campo con p^n elementi; questo si è visto essere un campo di spezzamento di $x^{p^n} - x$ e, visto che $f(x) \mid x^{p^n} - x$, significa che L contiene anche tutte le radici di $f(x)$. Sia β una di queste radici; il polinomio minimo di β su $\mathbb{Z}_p$ è proprio $f(x)$, visto che è irriducibile. Allora, il sottocampo $K' = \mathbb{Z}_p(\beta)$ di L è isomorfo a $K = \mathbb{Z}_p[x]/\langle f(x)\rangle$, quindi K' ha p^d elementi e ha grado d su $\mathbb{Z}_p$. Però, K' è un sottocampo di L, che ha grado n su $\mathbb{Z}_p$, quindi, per il teorema 4.2,

segue che $d \mid n$.

Questo significa che, nella fattorizzazione in irriducibili di $x^{p^n} - x$ in $\mathbb{Z}_p[x]$, i fattori che compaiono sono, a meno di associati, tutti e soli i polinomi irriducibili monici di grado d che divide n. Considerando, per finire, il coefficiente del termine di grado massimo, si nota che il prodotto di tutti i polinomi irriducibili monici di grado d che divide n è esattamente pari a $x^{p^n} - x$ (non a meno di associati). □

Per terminare, è possibile far vedere che, a meno di isomorfismi, esiste un solo campo finito con p^n elementi.

Teorema 4.10

Due campi finiti con p^n elementi sono isomorfi.

Dimostrazione. Siano K_1, K_2 due campi con p^n elementi. Sia α_1 generatore di K_1^* e α_2 di K_2^* (che sono due gruppi moltiplicativi ciclici). Si nota che $K_1 = \mathbb{Z}_p(\alpha_1)$ e $K_2 = \mathbb{Z}_p(\alpha_2)$, come osservato in precedenza. Inoltre, se $f_1(x)$ è il polinomio minimo di α_1 su $\mathbb{Z}_p$ e $f_2(x)$ è il minimo di α_2 su $\mathbb{Z}_p$, allora

$$K_1 = \mathbb{Z}_p(\alpha_1) \cong \mathbb{Z}_p[x]/\langle f_1(x)\rangle \qquad K_2 = \mathbb{Z}_p(\alpha_2) \cong \mathbb{Z}_p[x]/\langle f_2(x)\rangle$$

e i due polinomi sono entrambi irriducibili e di grado n.

Si sa, anche, che entrambi dividono $x^{p^n} - x$ per il teorema precedente, quindi, pensando, per esempio, a K_1 e ricordando che i suoi p^n elementi sono tutte le radici di $x^{p^n} - x$, si conclude che $f_2(x)$ ha n radici in K_1, visto che le sue radici sono anche radici di $x^{p^n} - x$.

Sia β una tale radice; allora $\mathbb{Z}_p(\beta)$ è un sottocampo di K_1 e $\mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[x]/\langle f_2(x)\rangle$. Visto che $\mathbb{Z}_p(\beta)$ ha grado n, per ragioni dimensionali, deve coincidere con K_1, quindi $K_1 = \mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[x]/\langle f_2(x)\rangle$. Per finire, si sapeva che $K_2 \cong \mathbb{Z}_p[x]/\langle f_2(x)\rangle$; prendendo

$$\Gamma : K_1 \to \mathbb{Z}_p[x]/\langle f_2(x)\rangle \qquad \Theta : K_2 \to \mathbb{Z}_p[x]/\langle f_2(x)\rangle$$

i due isomorfismi in questione, si ha che $\Theta^{-1} \circ \Gamma : K_1 \to K_2$ è un isomorfismo. □

Osservazione 4.6. Si nota che l'isomorfismo utilizzato nella precedente dimostrazione, $\Theta^{-1} \circ \Gamma$, visto che manda 1 in 1, si comporta come l'identità sulla copia di $\mathbb{Z}_p$ contenuta in K_1 e K_2.