Lezione 1

1. Principi di buon ordinamento e induzione

Iniziamo ricordando i due principi seguenti, che sono logicamente equivalenti:

Principio di Buon Ordinamento. *Sia $\mathbb{N}$ l'insieme degli interi non-negativi e S un sottoinsieme di $\mathbb{N}$. Se S è non-vuoto, allora S ha un elemento minimo.*

Principio d'Induzione. *Sia S un sottoinsieme di $\mathbb{N}$ con le seguenti proprietà:*

(i) $0 \in S$;
(ii) $n \in S \implies n+1 \in S$.

Allora $S = \mathbb{N}$.

Siano A e B interi. Diciamo che A divide B se esiste un intero C tale che $AC = B$. In questo caso scriviamo $A|B$. Altrimenti scriviamo $A \nmid B$. Sia $\mathbb{N}^*$ l'insieme degli interi positivi. Una semplice applicazione del principio di buon ordinamento è:

Definizione 1.1. Siano a e b interi diversi da zero. Allora, l'insieme $S = \{c \in \mathbb{N}^* \mid a|c,\ b|c\}$ è non-vuoto perchè $\pm ab \in S$. L'elemento più piccolo di S si chiama il minimo comune multiplo di a e b, scritto $\mathrm{mcm}(a, b)$.

L'applicazione standard di questi due principi è:

Dimostrazione per Induzione. *Sia $P(n)$ una proposizione per ogni $n \in \mathbb{N}$. Supponiamo che $P(0)$ sia vera e che $P(k)$ sia vera implica che $P(k+1)$ sia vera. Allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.*

Dimostrazione. (Utilizzando il principio del buon ordinamento): Supponiamo che l'insieme

$$S = \{\, k \in \mathbb{N} \mid P(k) \text{ è falsa} \,\}$$

è non-vuoto. Allora, S ha un elemento più piccolo s. Per ipotesi, 0 non è un elemento di S. Quindi $s \geq 1$. In particolare, $s-1$ non è un elemento di S, poiché s è il più piccolo elemento di S e $s \geq 1$. Pertanto, $P(s-1)$ è vera. Per ipotesi, ciò implica che $P(s)$ è vera, e quindi s non è un elemento di S. Questa è una contraddizione e quindi S deve essere vuoto.

Dimostrazione. (Utilizzando il principio d'induzione): Sia

$$S = \{\, k \in \mathbb{N} \mid P(k) \text{ è vera} \,\}$$

Allora, $0 \in S$ per ipotesi. Per ipostesi, $n \in S \implies n+1 \in S$. Quindi, $S = \mathbb{N}$.

C.V.D.

Nota 1.2. Si può anche iniziare l'induzione da $k = L$ invece che da $k = 0$. Si tratta solo di reindicizzare l'elenco delle proposizioni: $Q(k) = P(k-L)$.

Nota 1.3. La forma completa del principio di induzione (vedi Esercizio 6 **??**) implica la seguente forma forte di induzione: Sia $P(n)$ una proposizione per ogni $n \in \mathbb{N}$. Supponiamo che

- $P(0)$ sia vera;
- $P(0), \ldots, P(k)$ siano vere implica che $P(k+1)$ sia vera.

Allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

La verifica della "dimonstrazione per induzione" con il principio del buon ordinamento illustra un altro strumento fondamentale:

Dimostrazione per Assurdo. *Un modo per dimostrare che una proposizione P è vera è mostrare che assumere che $\neg P$ sia vero porta a una contraddizione. Più precisamente, esiste una proposizione Q tale che*

$$\neg P \implies Q \wedge (\neg Q) \quad \text{è vera}$$

Poiché $Q \wedge (\neg Q)$ è sempre falsa, ne segue che P è vera.

Definizione 1.4. Un numero primo p è un intero maggiore di 1 che non ha divisori interi positivi diversi da 1 e p.

Teorema 1.5 (Euclide)**.** *Esistono infiniti numeri primi.*

Dimostrazione. Sia S l'insieme di tutti i numeri primi. Supponiamo che S sia finito e che m sia il prodotto degli elementi di S. Chiaramente nessun elemento di S può dividere $m+1$. Quindi, $m+1$ è primo o ha un fattore primo che non è contenuto in S. Ma questo contraddice l'ipotesi che S sia l'insieme di tutti i numeri primi.

C.V.D.

Esercizi

Esercizio 1. Dimostrare che $n > 3$ implica $n! > 2^n$.

Esercizio 2. Si ricorda che:

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

Verificare la regola di Pascal:

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

Questo puó essere fatto con l'algebra pura, senza induzione.

Esercizio 3. Dimostrare il teorema binomiale utilizzando l'induzione e la regola di Pascal:

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

Esercizio 4. Verificare:

Teorema 1.6 (Teorema fondamentale dell'aritmetica, versione debole)**.** *Ogni intero positivo $n > 1$ è un prodotto di numeri primi.*

Esercizio 5. Dimostrare che il principio di buon ordinamento implica il principio d'induzione.

Esercizio 6. Verifica del principio dell'induzione finita completa: Sia S un sottoinsieme di $\mathbb{N}$ con le seguenti proprietà:

(i) $0 \in S$;
(ii) $0, \ldots, n \in S \implies n+1 \in S$.

Allora $S = \mathbb{N}$. (Utilizzare il principio di buon ordinamento o il principio di induzione)

2. Teorema della divisione

Questa parte si basa sulla sezione (3.A) di *A Concrete Introduction to Higher Algebra* di L. Childs.

Teorema 2.1 (Teorema della Divisione)**.** *Siano a e b interi non-negativi tale che $a > 0$. Allora, existono interi $q \geq 0$ e $0 \leq r < a$ tale che $b = qa + r$.*

Dimostrazione. Sia

$$S = \{b - ax \mid x \text{ è un intero non-negativo e } b - ax \geq 0\}$$

Allora, S non è vuoto perchè $b - ax = b \geq 0$ se $x = 0$. Allora, il principio del buon ordinamento implica che S ha un elemento minimo r. Per costruzione, $r = b - qa$ per qualche $q \geq 0$. Dobbiamo dimostrare che $0 \leq r < a$. Supponiamo che $r \geq a$. Allora, $r - a = b - qa - a \geq 0$ che contraddice la proprietà di minimalità di r. Quindi,

$$b = qa + r, \qquad 0 \leq r < a$$

C.V.D.

Proposizione 2.2 (Unicità)**.** *Siano a e b interi non-negativi tale che $a > 0$. Sia $b = qa + r$ dove $q \geq 0$ e $0 \leq r < a$. Allora la coppia (q,r) è unica.*

Dimostrazione. Supponiamo che (q', r') sia un'altra coppia di interi tale che $b = q'a + r'$ dove $q' \geq 0$ e $0 \leq r' < a$. Dopo aver scambiato (q, r) e (q', r'), se necessario, si supponga che $r \geq r'$. Allora

$$0 = b - b = a(q - q') + (r - r')$$

e quindi $a(q' - q) = (r - r') \geq 0$. Però, $0 \leq r' \leq r < a$ implica che $0 \leq r - r' < a$. Dunque,

$$q' - q = (r - r')/a, \qquad 0 \leq (r - r')/a < 1$$

Poiché $q' - q$ è un numero intero, ne consegue che $q' - q = 0$, cioè $q = q'$. Di conseguenza, $r' = b - q'a = b - qa = r$.

C.V.D.

Definizione 2.3. Siano a e b interi non negativi tali che $a > 0$. Sia $b = qa + r$ dove $q \geq 0$ e $0 \leq r < a$. Allora, q è detto il quoziente della divisione di b per a e r è detto il resto.

Esercizi

Esercizio 7. Sia

$$S = \{s \in \mathbb{N}^* \mid s = au + bv, \quad u, v \in \mathbb{Z}\}$$

Sia d il elemento minimo di S. Dimostrare che $d|a$ e $d|b$.

3. Basi

Sia $n \in \mathbb{N}$. Esiste allora una sequenza di numeri interi $\{a_0, \ldots, a_k\}$ tale che ogni $a_j \in \{0, ..., 9\}$ e

$$n = a_k 10^k + \cdots + a_1 10 + a_0$$

La stringa "$a_k \cdots a_0$" si chiama la rappresentazione in base 10 dell'intero n.

Nota 3.1. Se $k > 0$, si assume che $a_k \neq 0$ per evitare di aggiungere una serie di zeri eccessiva.

(*) $216 = 2 \cdot 108 + 0$
$108 = 2 \cdot 54 + 0$
$54 = 2 \cdot 27 + 0$
$27 = 2 \cdot 13 + 1$
$13 = 2 \cdot 6 + 1$
$6 = 2 \cdot 3 + 0$

$3 = 2 \cdot 1 + 1$
$1 = 2 \cdot 0 + 1$

$216_{10} = 11011000_2$

Siano $n \geq 0$ e $b \geq 2$ interi. Allora, si dice che n ha una rappresentazione di base b se esiste una sequenza $\{a_0, \ldots, a_k\}$ tale che ogni $a_j \in \{0, \ldots, b-1\}$ e

$$n = a_k b^k + \cdots + a_0$$

La stringa "$a_k \cdots a_0$" si chiama rappresentazione in base b dell'intero n.

(*) **Esempio 3.2.** La rappresentazione di 216 in base 2 è 11011000.

$$216 = 2^7 + 2^6 + 2^4 + 2^3 = 128 + 64 + 16 + 8$$

La rappresentazione di 216 in base 3 è 22000

$$216 = 2 * 3^4 + 2 * 3^3 = 2 * 81 + 2 * 27$$

La rappresentazione di 216 in base 60 è (3,36) – usiamo le virgole quando $b > 10$,

$$216 = 3 * 60 + 36$$

Teorema 3.3. *Fissato un intero $b \geq 2$, ogni intero $n \geq 0$ può essere rappresentato in base b: cioè, n può essere scritto univocamente come*

$$n = a_k b^k + \cdots + a_0$$

dove $a_j \in \{0, \ldots, b-1\}$ per $j = 0, \ldots, k$.

Dimostrazione. Sia $P(n)$ la proposizione che n ha una rappresentazione di base b. Allora, $P(0)$ è ovviamente vera. Supponiamo che $P(0), \ldots, P(k)$ siano vere. Allora,

$$k + 1 = bq + r, \qquad 0 \leq r < b$$

Inoltre, poichè $b > 1$ sappiamo che $q < k + 1$. Per ipotesi,

$$q = q_m b^m + \cdots + q_0$$

Ne segue che

$$k + 1 = bq + r = b(q_m b^m + \cdots + q_0) + r = q_m b^{m+1} + \cdots + q_0 b + r$$

è una rappresentazione di n in base b.

Per dimostrare che un numero ha un'unica rappresentazione in base b, sia S l'insieme di tutti gli interi non negativi che non hanno a rappresentazione unica in base b. Se S non è vuoto, ha un elemento più piccolo n. È chiaro che $n \geq b$ (perché?). Siano,

$$n = a_k b^k + \cdots + a_1 b + a_0, \qquad n = c_\ell b^k + \cdots + c_1 b + c_0$$

due diverse rappresentazioni di n in base b. Allora,

$$n = (a_k b^{k-1} + \cdots + a_1)b + a_0 = Aq + a_0, \qquad n = (c_\ell b^{\ell-1} + \cdots + c_1)b + c_0 = Cq + c_0$$

dove $0 \leq a_0 < b$ e $0 \leq c_0 < b$. Per il teorema della divisione, $a_0 = c_0$, e quindi $A = C$ ha due diverse rappresentazioni in base b. Ma $A < n$, contraddizione.

C.V.D.

Nota 3.4. La dimostrazione fornisce anche un algoritmo per calcolare la rappresentazione in base b del numero n:

$$n = bq_0 + r_0, \quad q_0 = bq_1 + r_1, \cdots q_k = b(0) + r_k$$

dove "$r_n r_{n-1} \ldots r_0$" è la rappresentazione di n base b.

Esercizi

♉ **Esercizio 8.** Scrivi 1984 in base 2, 3, 5.

♉ **Esercizio 9.** Le operazioni di addizione, sottrazione, moltiplicazione e divisione funzionano esattamente allo stesso modo in base b che in base 10. Calcola:

- $(1001110110000)_2/(11000)_2$.
- $(1100)_2^3 - (1010)_2^3 - (1001)_2^3$.

♉ **Esercizio 10.** Ricordiamo che ci sono 60 secondi in un minuto, 60 minuti in un grado e 180 gradi è uguale a π radianti. Usando l'approssimazione $\pi \sim 3.14$, cos'è un radiante in gradi, minuti, secondi?

ESERCIZIO 1

Dimostrare che $n > 3 \Rightarrow n! > 2^n$

$n = 4 \Rightarrow 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 > 2^4 = 16$ ✓

$n+1 \Rightarrow (n+1)! = (n+1)(n)(n-1)\dots(1) = (n+1)n!$

$$(n+1)n! > 2^{(n+1)}$$

$$(n+1)n! > 2^n \cdot 2$$

$$\frac{(n+1)n!}{2} > 2^n$$

poiché $n! > 2^n$ per ipotesi resta da dim.:

$\frac{n+1}{2} > 1 \quad \forall n > 3$ ✓

$\Rightarrow (n+1)! > 2^{(n+1)} \Rightarrow n! > 2^n \quad \forall n > 3$

ESERCIZIO 2

Si ricorda che: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Verificare la regola di Pascal: $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)!}{k!(n-k)!} = (n-1)!\left[\frac{n-k}{k!(n-k)!} + \frac{k}{k!(n-k)!}\right] =$$

$$= \frac{(n-1)!\,\cancel{(n-k)}}{k!\,\cancel{(n-k)}(n-k-1)!} + \frac{(n-1)!\,\cancel{k}}{\cancel{k}(k-1)!(n-k)!} = \binom{n-1}{k} + \binom{n-1}{k-1} \checkmark$$

ESERCIZIO 3

Dimostrare il teorema binomiale utilizzando l'induzione e la regola di Pascal:

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

Per induzione:

- $n=0$: $(x+y)^0 = 1$ ✓

- $n+1$: $(x+y)^{n+1} = (x+y)^n (x+y) = \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right)(x+y) =$

$$= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k} =$$

$$= x^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} y^{n-k} + y^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} =$$

$$= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k}\right] x^k y^{n+1-k}$$

$$= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \underbrace{\binom{n+1}{k}}_{} x^k y^{n+1-k}$$

PERCHÉ, PER LA REGOLA DI PASCAL

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$$\Rightarrow \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n-k+1}$$

ESERCIZIO 4

Verificare il th fondamentale dell'aritmetica (versione debole):

<u>TH</u> Ogni intero positivo $n>1$ é un prodotto di num. primi

$P(n) = \{n$ é un prodotto di numeri primi$\}$

$P(2)$ vera (2 é primo)

Supponiamo $P(2), \dots, P(n)$ vere

$P(n+1)$:

- CASO 1: $n+1$ é primo
- CASO 2: $n+1$ é composto $\Rightarrow n+1 = ab$ con $1<a,b<n+1$

  ma $P(a), P(b)$ vere $\Rightarrow a = p_1^{u_1} \cdots p_k^{u_k}$

  con $p_1, \dots, p_k$ primi

  $\Rightarrow b = q_1^{v_1} \cdots q_k^{v_k}$

  con $q_1, \dots, q_k$ primi

ESERCIZIO 5

Dimostrare che il principio di buon ordinamento implica il principio d'induzione.

PRINCIPIO DI INDUZIONE:

Sia $S \subseteq \mathbb{N}$ t.c $0 \in S, n \in S \Rightarrow n+1 \in S$. Allora $S = \mathbb{N}$

Sia R il complementare di S: $R = \mathbb{N} - S$

Allora $R = \emptyset$ (perché $S = \mathbb{N}$)

Supponiamo per assurdo $R \neq \emptyset$.

Allora, per il principio del buon ordinamento, R ha un elemento minimo d.

$0 \in S \Rightarrow 0 \notin R \Rightarrow d \geq 1 \Rightarrow d-1 \in S \Rightarrow d \in S \Rightarrow d \notin R$ ↯

ESERCIZIO 6

Verificare il principio di induzione completo:

Sia S un sottoinsieme di $\mathbb{N}$ con le seguenti proprietà:

i) $0 \in S$

ii) $0, \dots, n \in S \Rightarrow n+1 \in S$

Allora $S = \mathbb{N}$.

$S = \mathbb{N}$ ✓

$\Uparrow$

Tramite induzione:

$n=0 \Rightarrow 0 \in S \Rightarrow 1 \in S \Rightarrow 2 \in S \Rightarrow \dots \Rightarrow n \in S \Rightarrow n+1 \in S$

Supponiamo $P(0), \dots, P(n)$ vere

$0, \dots, n \in S \Rightarrow n+1 \in S \Rightarrow S = \mathbb{N}$

Tramite buon ordinamento:

$S = \{k \in \mathbb{N} : P(k) \text{ è falsa}\}$

Allora $S = \emptyset$ oppure S ha un elemento minimo m

$0 \in S \Rightarrow m \geq 1$

Supponiamo $P(0), \dots, P(m-1)$ vere

$\Rightarrow P(m)$ vera

ESERCIZIO 7

Sia $S = \{s \in \mathbb{N}^* : s = au + bv,\ u, v \in \mathbb{Z}\}$

Sia d l'elemento minimo di S.

Dimostrare che $d \mid a$ e $d \mid b$.

d È UN ELEM. DI S, QUINDI È DELLA FORMA $au + bv$

Per il th della divisione $a = qd + r$, $0 \leq r < d$

$\Rightarrow a = q(au + bv) + r \Rightarrow r = a - q(au + bv) \Rightarrow r = a(1 - qu) - qbv$

$\Rightarrow r \in S$ oppure $r = 0$

Ma $r \in S$ non è possibile in quanto $1 \leq r < d$, ma d è il minimo elemento di S $\lightning$

ESERCIZIO 8

Scrivere 1984 in base 2, 3, 5

$1984 = 2 \cdot 992 + 0$

$992 = 2 \cdot 496 + 0$

$496 = 2 \cdot 248 + 0$

$248 = 2 \cdot 124 + 0$

$124 = 2 \cdot 62 + 0$

$62 = 2 \cdot 31 + 0$

$31 = 2 \cdot 15 + 1$

$15 = 2 \cdot 7 + 1$

$7 = 2 \cdot 3 + 1$

$3 = 2 \cdot 1 + 1$

$1 = 2 \cdot 0 + 1$

$\Rightarrow 1984_{10} = 11111000000_2$

$1984 = 3 \cdot 661 + 1$

$661 = 3 \cdot 220 + 1$

$220 = 3 \cdot 73 + 1$

$73 = 3 \cdot 24 + 1$

$24 = 3 \cdot 8 + 0$

$8 = 3 \cdot 2 + 2$

$2 = 3 \cdot 0 + 2$

$\Rightarrow 1984_{10} = 2201111_3$

$1984 = 5 \cdot 396 + 4$

$396 = 5 \cdot 79 + 1$

$79 = 5 \cdot 15 + 4$

$15 = 5 \cdot 3 + 0$

$3 = 5 \cdot 0 + 3$

$\Rightarrow 1984_{10} = 30414_5$

ESERCIZIO 9

Calcolare $1001110110000_2 / 11000_2 = 5040_{10} / 24_{10} = 210_{10}$

```
1 0 0 1 1 1 0 1 1 0 0 0 0 | 1 1 0 0 0
  1 1 0 0 0               |----------
  ---------               |
  0 1 1 1 1 0             | 11010010
    1 1 0 0 0             |
    ---------             |
        1 1 0 1 1         |
        1 1 0 0 0         |
        ---------         |
            0 1 1 0 0 0   |
              1 1 0 0 0   |
              ---------   |
                    0 0   |
```

Calcolare $(1100)_2^3 - (101)_2^3 - (1001)_2^3 = 1728 - 125 - 729$
$= 874$

ESERCIZIO 10

$1 \text{ rad} = \frac{180°}{\pi} \simeq 57.3248°$

$57.3248 = 57 + 0.3248 =$
$= 57 + 0.3248 \cdot 60 =$
$= 57 + 19.488 =$
$= 57 + 19 + 0.488 \cdot 60 =$
$= 57° + 19' + 29''$

Lezione 2

Questa parte si basa sulla sezione (3.B) – (3.D) di *A Concrete Introduction to Higher Algebra* di L. Childs.

1. Il massimo comune divisore

Definizione 1.1. Sia S un sottoinsieme dei numeri reali, $\mathbb{R}$. Allora $m \in \mathbb{R}$ è un elemento massimo di S se (i) $m \in S$; (ii) $s \in S \implies s \leq m$.

In generale, un sottoinsieme di $\mathbb{R}$ non deve necessariamente avere un elemento massimo. Ad esempio, un sottoinsieme aperto di $\mathbb{R}$ non ha mai un elemento massimo.

Lemma 1.2. *Sia $S \subseteq \mathbb{R}$. Se S ha un elemento massimo m, allora S ha un unico elemento massimo.*

Dimostrazione. Siano m e m' elementi massimi di S. Allora $m \leq m'$ perché m' è massimo. Allo stesso modo, $m' \leq m$ perché m è massimo. Così $m = m'$.

Lemma 1.3. *Sia $S \subseteq \mathbb{R}$ un insieme finito e non-vuoto. Allora, S ha un elemento massimo.*

Dimostrazione. Sia $P(n)$ la proposizione che se S ha $n \geq 1$ elementi allora S ha un elemento massimo. La proposizione $P(1)$ è vera. Supponiamo che $P(n)$ è vera e S un insieme con $n+1$ elementi. Scegli un elemento $s \in S$ e sia $S' = S - \{s\}$. Quindi, $S' = S - \{s\}$ ha $n \geq 1$ elementi. Poiché $P(n)$ è vera, ne consegue che S' ha un elemento massimo, chiamalo s'. Chiaramente il massimo m di s e s', scritto $m = \max(s, s')$, è un elemento massimo di S. In particolare, $P(n+1)$ è vera.

C.V.D.

Se n è un intero, sia $D(n) = \{\, d \in \mathbb{Z} \mid d|n \,\}$. Nota che $D(0) = \mathbb{Z}$.

Proposizione 1.4. *Sia n un intero diverso da zero. Allora, $D(n) \subseteq \{-|n|, \ldots, |n|\}$. In particolare, $D(n)$ è un insieme finito.*

Dimostrazione. $m \in D(n) \implies$ esiste $k \in \mathbb{Z}$ tale che $n = km$. In particolare, $k \neq 0$ e $m \neq 0$ perché $n \neq 0$. Allora,

$$|n| = |km| = |k||m| \implies |k|, |m| \leq |n|$$

C.V.D.

Definizione 1.5. Siano a e b interi tale che $(a, b) \neq (0, 0)$. Il massimo comune divisore di a e b, scritto $\mathrm{mcd}(a, b)$ è il massimo elemento dell'insieme $D(a) \cap D(b)$.

Nota 1.6. Se $a = 0$, $b \neq 0$ allora $\mathrm{mcd}(a, b) = b$. , SE $a \neq 0, b = 0 \Rightarrow MCD(a, 0) = a$

La definizione di $\mathrm{mcd}(a, b)$ fornisce anche un algoritmo per calcolarlo:

```
int mcd(int a, int b) // Assumes a, b>0
{ int k, m;
  for(m=1, k=1; k<a+1; k++) // a % k = remainder of a/k
  if ( ((a % k)==0)) && ((b % k)==0) ) m=k;
  return m;
}
```

Nota 1.7. Si può anche trovare mcd fattorizzando gli interi.

(*) $MCD(256,60) = MCD(4\cdot 60+16,60) = MCD(60,16) =$
$= MCD(3\cdot 16+12,16) = MCD(16,12) =$
$= MCD(1\cdot 12+4,12) = MCD(12,4) =$
$= MCD(3\cdot 4,4) = MCD(4,0) = 4$

Esempio 1.8. $\mathrm{mcd}(60,256)$ [Ometto gli elementi negativi di $D(n)$ in questi esempi.]

$$D(60) = \{1,2,3,4,5,6,10,12,15,20,30,60\}$$
$$D(256) = \{1,2,4,8,16,32,64,128,256\}$$

$D(60)\cap D(256) = \{1,2,4\} \implies \mathrm{mcd}(60,256) = 4.$

2. Algoritmo di Euclide

Lemma 2.1. *Siano a e b interi diversi da zero. Allora* $\mathrm{mcd}(a+b,b) = \mathrm{mcd}(a,b)$. $= MCD(r+qb,b) =$
$= MCD(r,b) \Rightarrow$
$MCD(b,r)$

Dimostrazione. Siano $m = \mathrm{mcd}(a+b,b)$ e $\mu = \mathrm{mcd}(a,b)$. Allora

$$m = \mathrm{mcd}(a+b,b) \implies m|(a+b), \quad m|b \implies m|a, \quad m|b \implies m \le \mu$$

Allo stesso modo,

$$\mu = \mathrm{mcd}(a,b) \implies \mu|a, \quad \mu|b \implies \mu|(a+b), \quad \mu|b \implies \mu \le m$$

Quindi, $m = \mu$.

C.V.D.

Supponiamo che $a \ge b > 0$ e scrivi $a = qb + r$ dove $0 \le r < b$. Allora, il lemma precedente implica

$$\mathrm{mcd}(a,b) = \mathrm{mcd}(r+qb,b) = \mathrm{mcd}(r,b) = \mathrm{mcd}(b,r)$$

L'algoritmo si ferma quando $r = 0$. In questo modo, otteniamo un algoritmo ricorsivo per calcolare il mcd

```
int mcd_euclid(int a, int b)
{   if (b == 0)    // mcd(a,0)=a
      return a;
    if (b>a) ~~mcd(b,a)~~  // Switch roles of a and b   {c=b; b=a; a=c;}
     return mcd(b, a % b);
}
```

Esempio 2.2. 54%36

- $\mathrm{mcd}(54,36) = \mathrm{mcd}(36,18) = \mathrm{mcd}(18,0) = 18$
- $\mathrm{mcd}(133,27) = \mathrm{mcd}(27,25) = \mathrm{mcd}(25,2) = \mathrm{mcd}(1,0) = 1.$
- $\mathrm{mcd}(56,24) = \mathrm{mcd}(24,8) = \mathrm{mcd}(8,0) = 8.$
- (*) $\mathrm{mcd}(256,60) = \mathrm{mcd}(60,16) = \mathrm{mcd}(16,12) = \mathrm{mcd}(12,4) = \mathrm{mcd}(4,0) = 4.$

La forma originale di questo algoritmo appare negli elementi di Euclide:

Algoritmo euclideo. *Siano a e b interi diversi da zero. Applicare il teorema di divisione successivamente come segue:*

$$\begin{aligned} b &= aq_1 + r_1, \\ a &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ r_2 &= r_3q_4 + r_4, \\ &\vdots \quad \vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} + 0. \end{aligned}$$

L'algoritmo termina quando r_n divide r_{n-1}, a quel punto r_n è il massimo comune divisore di a e b.

Esempio 2.3.

- $\mathrm{mcd}(54, 36)$
$$\begin{aligned} 36 &= (0)(54) + 36, \qquad r_1 = 36 \\ 54 &= (1)(36) + 18, \qquad r_2 = 18 \end{aligned}$$
$r_2 | r_1 \implies \mathrm{mcd}(54, 36) = r_2 = 18.$
- $\mathrm{mcd}(256, 60)$
$$\begin{aligned} 60 &= (0)(256) + 60, \qquad r_1 = 60 \\ 256 &= (4)(60) + 16, \qquad r_2 = 16 \\ 60 &= (3)(16) + 12, \qquad r_3 = 12 \\ 16 &= (1)(12) + 4, \qquad r_4 = 4 \end{aligned}$$
$r_4 | r_3 \implies \mathrm{mcd}(256, 60) = r_4 = 4.$

Definizione 2.4. Siano a e b interi diversi da zero. Allora, a e b sono coprimi se $\mathrm{mcd}(a, b) = 1$.

Esercizi

Esercizio 1. Trova $\mathrm{mcd}(72, 42)$ e $\mathrm{mcd}(1024, 216)$

Esercizio 2. Scrivere un'implementazione non ricorsiva dell'algoritmo di Euclide.

Esercizio 3. Perché l'algoritmo euclideo termina dopo un numero finito di passi?

Esercizio 4. Sia p un numero primo. Mostra che se a è un intero e $\mathrm{mcd}(p, a) \neq 1$ allora p è un divisore di a.

Esercizio 5. Ricordiamo la successione di Fibonacci: $1, 1, 2, 3, 5, 8, 13, \ldots$ dove $f_{n+1} = f_n + f_{n-1}$. Verificare che $\mathrm{mcd}(f_{n+1}, f_n) = 1$.

Esercizio 6. Siano a e b numeri con n-cifre base 2. Formulare una congettura sul numero di iterazioni $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$, $a = bq + r$ necessarie per trovare $\mathrm{mcd}(a, b)$.

3. L'identitá di Bezout

.

Siano a e b interi tali che $(a, b) \neq (0, 0)$. Sia
$$S = \{au + bv \mid u,\, v \in \mathbb{Z}\} \cap \mathbb{N}^*$$
Allora, S è non-vuoto perché $|a|, |b| \in S$. Pertanto, S ha un elemento minimo m. In questa sezione mostreremo che $m = \mathrm{mcd}(a, b)$.

Come primo passo, mostriamo che $m | a$. Consideriamo il quoziente di a per m:
$$a = qm + r, \qquad 0 \leq r < m$$
D'altra parte, sappiamo che $m = au + bv$. Allora,
$$a = q(au + bv) + r \implies r = a - aqu - \overset{bqv}{\cancel{bv}} = a(1 - qu) - \overset{bqv}{\cancel{bv}} < m$$
che contraddice la minimalitá di m, a meno che $r = 0$ (ricorda che: $m \in \mathbb{N}^*$). Allo stesso modo, $m | b$.

Sia $\mu = \mathrm{mcd}(a, b)$. Allora, μ essendo il massimo comune divisore di a e b, ne consegue che $m \leq \mu$. D'altra parte, perchè $m = au + bv$ e μ è un divisore di a e b, ne consegue che $\mu | m$. Quindi $\mu = m$. Insomma, abbiamo:

Identità di Bézout . *Se a e b sono interi (non entrambi nulli) e il loro massimo comune divisore è d, allora esistono due interi u e v tale che $d = au + bv$.*

Per trovare gli interi u e v tali che $m = au + bv$ dove $m = \mathrm{mcd}(a, b)$, iniziamo con la seguente osservazione:

$$au + bv = m \implies m = (qb + r)u + bv = ru + b(v + qu)$$

Quindi, ricorda che questo processo di calcolo di $\mathrm{mcd}(a, b)$ per riduzione termina con $\mathrm{mcd}(m, 0)$. A quel punto, abbiamo $m = m(1) + 0(0)$. Pertanto, possiamo calcolare gli interi u e v utilizzando il seguente algoritmo esteso di Euclide:

$$\begin{aligned}\mathrm{mcd}(a, b|u, v) &= \mathrm{mcd}(qb + r, b|u, v) = \mathrm{mcd}(r, b|u, v + qu)\\ &= \mathrm{mcd}(b, r|v + qu, u) = \cdots = \mathrm{mcd}(m, 0|\ell_1(u, v), \ell_2(u, v))\end{aligned}$$

dove $\ell_1(u, v) = 1$, $\ell_2(u, v) = 0$ è un sistema lineare 2×2 di equazioni in u e v.x

Esempio 3.1.

- $\mathrm{mcd}(256, 60|u, v) = \mathrm{mcd}((4)(60)+16, 60|u, v) = \mathrm{mcd}(16, 60|u, v+4u) = \mathrm{mcd}(60, 16|v+4u, u)$.
- $\mathrm{mcd}(60, 16|v+4u, u) = \mathrm{mcd}((3)(16)+12, 16|v+4u, u) = \mathrm{mcd}(12, 16|v+4u, u+3(v+4u)) = \mathrm{mcd}(16, 12|3v + 13u, v + 4u)$.
- $\mathrm{mcd}(16, 12|3v + 13u, v + 4u) = \mathrm{mcd}((1)(12) + 4, 12|3v + 13u, v + 4u + (3v + 13u)) = \mathrm{mcd}(12, 4|4v + 17u, 3v + 13u)$.
- $\mathrm{mcd}(12, 4|4v + 17u, 3v + 13u) = \mathrm{mcd}((3)(4), 4|4v + 17u, 3v + 13u) = \mathrm{mcd}(0, 4|4v + 17u, 3v+13u+3(4v+17u)) = \mathrm{mcd}(0, 4|4v+17u, 15v+64u) = \mathrm{mcd}(4, 0|15v+64u, 4v+17u)$.

Quindi, dobbiamo risolvere il sistema lineare:

$$64u + 15v = 1, \qquad 17u + 4v = 0$$

A questo punto ricordiamo che le soluzioni di $\alpha u+\beta v = 0$ hanno la forma $(u, v) = c(\beta, -\alpha)$ dove c é uno scalare arbitrario. Cosí, $(u, v) = c(4, -17)$. Inserendo questo nell'altra equazione mostra che $c = 1$.

Questo può essere implementato ricorsivamente su un computer:

```
int mcd_esteso(int a, int b, int *u, int *v)
{   int d, x, y;
    if (b == 0) {
        *u = 1;
        *v = 0;
        return a;
    }
    d = mcd_esteso(b, a % b,&x,&y);
    *u = y;
    *v = x -y*(a/b);
    printf("%d,%d|%d,%d\n",b,a % b,*u,*v);   // Only for illustration
    return d;
```

}

Esempio 3.2. $\mathrm{mcd}(256, 60) = 4$.

```
mcm_esteso(256,60,&u,&v)
  4,0|0,1      // 4 = (12)(0)+(4)(1)
 12,4|1,-1     // 4 = (16)(1)+(12)(-1)
16,12|-1,4     // 4 = (60)(-1)+(4)(16)
60,16|4,-17    // 4 = (4)(256)-(17)(60)
```

Esempio 3.3. $\mathrm{mcd}(133, 27) = 1$.

```
mcm_esteso(133,27,&u,&v)
 1,0|0,1       // 1 = (0)(2)+(1)(1)
 2,1|1,-12     // 1 = (1)(25)+(2)(-12)
25,2|-12,13    // 1 = (27)(-12)+(25)(13)
27,25|13,-64   // 1 = (13)(133)+(27)(-64)
```

Il seguente lemma è di fondamentale importanza:

Lemma di Euclide. *Un intero $p > 1$ è un numero primo se e solo se $p \mid ab$ implica che $p \mid a$ o $p \mid b$, per tutti gli interi a e b.*

Dimostrazione. Supponiamo che p sia un primo. Ricordiamo che se $\mathrm{mcd}(a, p) \neq 1$ allora $p|a$. Allo stesso modo, se $\mathrm{mcd}(b, p) \neq 1$ allora $p|b$. Quindi, dopo aver cambiato a e b se necessario, possiamo supporre che $\mathrm{mcd}(a, p) = 1$.

Per il lemma di Bezout, esistono interi u, v tali che $pu + av = 1$. Dunque,

$$b = b(pu + av) = pbu + abv$$

Poiché $p \mid p$ e $p \mid ab$ (per ipotesi), $p \mid pbu + abv = b$, come desiderato.

Viceversa, se p non è primo allora esistono due interi a e b maggiori di uno tale che $p = ab$. In particolare, $p = ab$ e $a > 1 \implies b < p$. Quindi, $p \nmid b$. Allo stesso modo, $p \nmid a$.

C.V.D.

Esercizi

♉ **Esercizio 7.** Torniamo alla sequenza di Fibonacci: $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$. Sappiamo già che il mcd di coppie successive è sempre 1. Risolvi l'equazione $au + bv = 1$ per $(a, b) = (8, 13)$, $(13, 21)$, $(21, 34)$. C'è uno schema?

♉ **Esercizio 8.** Verificare: Se $a|bc$ e a e b sono coprimi allora $a|c$ (Usa l'identità di Bezout).

Esercizio 9. Scrivere un'implementazione iterativa di mcd_esteso. Un modo per farlo è codificare il sistema lineare in una matrice 2x2 e registrare come cambia la matrice ad ogni passaggio dell'algoritmo.

ESERCIZIO 1

Trovare MCD(72,42) e MCD(1024, 216)

$42 = 0 \cdot 72 + 42$

$72 = 1 \cdot 42 + 30$

$42 = 1 \cdot 30 + 12$

$30 = 2 \cdot 12 + 6$

$12 = 2 \cdot 6 + 0$

$\Rightarrow MCD(72,42) = 6$

$216 = 0 \cdot 1024 + 216$

$1024 = 4 \cdot 216 + 160$

$216 = 1 \cdot 160 + 56$

$160 = 2 \cdot 56 + 48$

$56 = 1 \cdot 48 + 8$

$48 = 6 \cdot 8 + 0$

$\Rightarrow MCD(1024, 216) = 8$

ESERCIZIO 2

Scrivere un'implementazione non ricorsiva dell'algoritmo di Euclide.

```
int MCD (int x, int y){
    while (y!=0){
        int k=x;
        x = y;
        y = k%y;
    }
    return x;
}
```

ESERCIZIO 3

Perché l'algoritmo di Euclide termina dopo un numero finito di passi?

Perché due numeri hanno sempre almeno un divisore in comune: 1.

ESERCIZIO 4

Sia p un numero primo. Mostrare che se a è un intero e $MCD(a,p) \neq 1$ allora $p|a$.

p primo, $MCD(a,p) \neq 1 \Rightarrow MCD(a,p) = p \Rightarrow p|a$

ESERCIZIO 5

Ricordiamo la successione di Fibonacci: 1, 1, 2, 3, 5, 8, 13...
dove $f_{n+1} = f_n + f_{n-1}$. Verificare $MCD(f_{n+1}, f_n) = 1$.

$P: MCD(f_{n+1}, f_n) = 1$

$P(0) \Rightarrow MCD(1,1) = 1$ ✓

Supponiamo $P(0), \dots, P(n)$ vere

$P(n+1) \Rightarrow MCD(\underbrace{f_{n+2}}_{= f_{n+1} + f_n}, f_{n+1}) = 1$

$MCD(f_{n+1} + f_n, f_{n+1}) = MCD(f_n, f_{n+1}) = 1$

PERCHÉ $MCD(a+b, b) = MCD(a,b)$

PER IPOTESI

ESERCIZIO 7

Sappiamo che il MCD di coppie successive è sempre 1.
Risolvere l'equazione $au + bv = 1$ per
$(a,b) = (8,13), (13,21), (21,34)$.
C'è uno schema?

$$EE(13,8) \to \langle 1, -3, 2+3\lfloor \tfrac{13}{8} \rfloor \rangle = \langle 1, \overset{u}{-3}, \overset{v}{5} \rangle$$
$$EE(8,5) \to \langle 1, 2, -1-2\lfloor \tfrac{8}{5} \rfloor \rangle = \langle 1, 2, -3 \rangle$$
$$EE(5,3) \to \langle 1, -1, 1+\lfloor \tfrac{5}{3} \rfloor \rangle = \langle 1, -1, 2 \rangle$$
$$EE(3,2) \to \langle 1, 1, 0-\lfloor \tfrac{3}{2} \rfloor \rangle = \langle 1, 1, -1 \rangle$$
$$EE(2,1) \to \langle 1, 0, 1 \rangle$$
$$EE(1,0) \to \langle 1, 1, 0 \rangle$$

$$EE(21,13) \to \langle 1, 5, -3-5\lfloor \tfrac{21}{13} \rfloor \rangle = \langle 1, \overset{u}{5}, \overset{v}{-8} \rangle$$
$$EE(13,8) \to \langle 1, -3, 5 \rangle$$

$$EE(34,21) \to \langle 1, -8, 5+8\lfloor \tfrac{34}{21} \rfloor \rangle = \langle 1, \overset{u}{-8}, \overset{v}{13} \rangle$$
$$EE(21,13) \to \langle 1, 5, -8 \rangle$$

ESERCIZIO 8

Verificare che se $a \mid bc$ e $MCD(a,b) = 1 \Rightarrow a \mid c$

$MCD(a,b) = 1 \Rightarrow \exists u, v$ t.c. $1 = au + bv$ per l'id. di Bezout
$c = 1 \cdot c = auc + bvc$
$a \mid bc \Rightarrow a \mid \underbrace{auc + bvc}_{c}$

Lezione 3

Questa parte si basa sulle sezioni (4.A) – (4.C) di *A Concrete Introduction to Higher Algebra* di L. Childs.

1. Teorema fondamentale dell'aritmetica

In questa sezione dimostriamo il seguente risultato:

Teorema fondamental dell'arithmetica. *Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica, se si prescinde dall'ordine in cui compaiono i fattori.*

La prima parte del teorema, riguardante l'esistenza di una fattorizzazione primo, era un esercizio a casa:

Dimostrazione. Sia $P(n)$ la proposizione che l'intero $n > 1$ è un numero primo oppure può essere espresso come prodotto di numeri primi. Allora, $P(2)$ è vera. Supponiamo che $P(2), \ldots, P(n)$ siano vere. Allora, anche $P(n+1)$ è vera:

- Se $n+1$ è primo, non c'è nulla da dimostrare.
- Se $n+1$ non è primo allora $n+1 = ab$, dove $1 < a, b < n+1$. Per l'ipotesi di induzione, a e b sono o primi o prodotti di primi.

C.V.D.

Per l'unicità della fattorizzazione, ricordiamo:

Lemma di Euclide. *Un intero $p > 1$ è un numero primo se e solo se $p \mid ab$ implica che $p \mid a$ oppure $p \mid b$, per tutti gli interi a e b.*

Dimostrazione. (Unicità) Sia S l'insieme degli interi > 1 per i quali la parte di unicità del teorema fondamentale dell'aritmetica fallisce. Se S non è vuoto, ha un elemento più piccolo n. Siano

$$n = p_1 \cdots p_k, \qquad n = q_1 \ldots q_\ell$$

due distinte fattorizzazioni prime di n. Allora, poiché $p_1 | n$, p_1 deve dividere qualche q_j per il lemma di Euclide. Dopo aver riordinato i fattori $q_1, \ldots, q_\ell$, possiamo assumere che $j = 1$. Poiché p_1 e q_1 sono entrambi primi, ne consegue che $p_1 = q_1$. Allora,

$$m = p_2 \cdots p_k = q_2 \cdots q_\ell$$

ha anche due fattorizzazioni distinte. Ma, $m < n$, che contraddice la minimalità di n.

C.V.D.

Nota 1.1. Sia $R = \mathbb{Z}$ e $\delta(n) = |n|$ per n diverso da zero, e $R = \mathbb{Z}$. Astrattamente, i due ingredienti che fanno funzionare questa dimostrazione sono:

(i) Se a, $b \in R$ e $b \neq 0$, allora esistono q, $r \in R$ tali che $a = bq + r$ e o $r = 0$ oppure $\delta(r) < \delta(b)$.

(ii) $\delta(ab) = \delta(a)\delta(b)$

Se guardi indietro tra le note, vedrai che abbiamo usato $|ab| = |a||b|$ in più luoghi. Un altro luogo in cui si verifica la fattorizzazione in pezzi "irriducibili" riguarda i polinomi. Anche in questo caso, abbiamo il teorema di divisione, con la funzione di grado al posto del valore assoluto: $\deg(pq) = \deg(p)\deg(q)$. Torneremo su questo argomento più avanti nel corso.

Come prima applicazione, abbiamo la seguente proposizione utile, che mostra che possiamo calcolare il mcm in modo efficiente usando l'algoritmo euclideo, invece di trovare i fattori primi di ogni intero:

Proposizione 1.2. *Siano a e b interi diversi da zero. Allora*

$$|ab| = \mathrm{mcm}(a, b)\,\mathrm{mcd}(a, b)$$

Dimostrazione. Senza perdita di generalità, possiamo assumere che a e b sono interi positivi. Sia A l'insieme dei fattori primi di a e B l'insieme dei fattori primi di b. Sia $P = \{p_1, \ldots, p_m\} = A \cup B$. Allora,

$$a = p_1^{a_1} \cdots p_m^{a_m}, \qquad b = p_1^{b_1} \ldots p_m^{b_m}$$

dove permettiamo agli esponenti a_j e b_j di essere zero. Allora,

$$\mathrm{mcm}(a, b) = p_1^{\max(a_1,b_1)} \cdots p_m^{\max(a_m,b_m)}$$
$$\mathrm{mcd}(a, b) = p_1^{\min(a_1,b_1)} \cdots p_m^{\min(a_m,b_m)}$$

Dunque,

$$\begin{aligned}\mathrm{mcm}(a, b)\,\mathrm{mcd}(a, b) &= p_1^{\max(a_1,b_1)+\min(a_1,b_1)} \cdots p_m^{\max(a_m,b_m)+\min(a_m,b_m)} \\ &= p_1^{a_1+b_1} \cdots p_m^{a_m+b_m} = ab\end{aligned}$$

C.V.D.

Esempio 1.3. Dalla lezione precedente,

$$\mathrm{mcd}(60, 256) = 4, \quad \mathrm{mcd}(54, 36) = 18, \quad \mathrm{mcd}(133, 27) = 1, \mathrm{mcd}(56, 24) = 8$$

Allora,

- $\mathrm{mcm}(60, 256) = (60)(256)/4 = 3840$
- $\mathrm{mcm}(54, 36) = (54)(36)/18 = 108$
- $\mathrm{mcm}(133, 27) = (133)(27)/1 = 3591$
- $\mathrm{mcm}(56, 24) = (56)(24)/8 = 168$.

Le fattorizzazioni prime sono:

$$24 = (2^3)(3), \quad 27 = 3^3, \quad 36 = (2^2)(3^2), \quad 54 = (2)(3^3)$$
$$56 = (2^3)(7), \quad 60 = (2^2)(3)(5), \quad 133 = (7)(19), \quad 256 = 2^8$$

Allora,

- $\mathrm{mcd}(60, 256) = 2^2 = 4$, $\mathrm{mcm}(60, 256) = (2^8)(3)(5) = 3840$.
- $\mathrm{mcd}(54, 36) = (2)(3^2) = 18$, $\mathrm{mcm}(54, 36) = (2^2)(3^3) = 108$.

(*) SULLA DENSITÁ DEI NUM. PRIMI:

$$\underbrace{\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}}_{\text{FUNZIONE ZETA DI REIMANN}} = \underbrace{\prod_{p:\,\text{primo}} \frac{1}{1-p^{-s}}}_{\text{EULERO}}, \quad s>1$$

$$\frac{1}{\zeta(\ )} = \prod_{p:\,\text{primo}} \left(1-\frac{1}{p^2}\right) \approx \frac{6}{\pi^3} \approx 0.19$$

PROBABILITÁ CHE PRESI DUE NUMERI A CASO QUESTI SIANO PRIMI

- $\mathrm{mcd}(133, 27) = 1$, $\mathrm{mcm}(133, 27) = (3^3)(7)(19)$.
- $\mathrm{mcd}(56, 24) = (2^3)$, $\mathrm{mcm}(56, 24) = (2^3)(3)(7) = 168$.

Dalla dimostrazione di Proposizione (1.2) vediamo che se definiamo il massimo comune divisore di tre interi diversi da zero scrivendo

$$a = p_1^{a_1} \cdots p_m^{a_m}$$
$$b = p_1^{b_1} \cdots p_m^{b_m}$$
$$c = p_1^{c_1} \cdots p_m^{c_m}$$

e ponendo

$$\mathrm{mcd}(a, b, c) = p_1^{\min(a_1,b_1,c_1)} \cdots p_m^{\min(a_m,b_m,c_m)}$$

allora

$$\mathrm{mcd}(a, b, c) = \mathrm{mcd}(\mathrm{mcd}(a, b), c)$$

perché $\min(a_j, b_j, c_j) = \min(\min(a_j, b_j), c_j)$.

Per qualsiasi insieme finito $\{s_1, \ldots, s_k\}$ di interi diversi da zero, possiamo definire il massimo comune divisore allo stesso modo e otteniamo la stessa formula:

$$\mathrm{mcd}(s_1, \ldots, s_k) = \mathrm{mcd}(\mathrm{mcd}(s_1, \ldots, s_{k-1}), s_k)$$

Allo stesso modo, si può definire

$$\mathrm{mcm}(a, b, c) = p_1^{\max(a_1,b_1,c_1)} \cdots p_m^{\max(a_m,b_m,c_m)}$$

in tal caso abbiamo la formula

$$\mathrm{mcm}(a, b, c) = \mathrm{mcm}(\mathrm{mcm}(a, b), c)$$

perchè $\max(a_i, b_i, c_i) = \max(\max(a_i, b_i), c_i)$. In generale, abbiamo

$$\mathrm{mcm}(s_1, \ldots, s_k) = \mathrm{mcm}(\mathrm{mcm}(s_1, \ldots, s_{k-1}), s_k)$$

Esercizi

Esercizio 1. Verifica le formule

$$\mathrm{mcm}(a, b) = p_1^{\max(a_1,b_1)} \cdots p_m^{\max(a_m,b_m)}$$
$$\mathrm{mcd}(a, b) = p_1^{\min(a_1,b_1)} \cdots p_m^{\min(a_m,b_m)}$$

usato in Proposizione (1.2). Per essere chiari, sebbene questo sia "ovvio", abbiamo definito mcm e mcd in modo diverso. Pertanto, dobbiamo verificare queste formule.

(*)

2. Teorema dei numeri primi

Come abbiamo visto nella lezione 1, Euclide conosceva l'esistenza di infiniti numeri primi. Detto questo, una domanda naturale è quanto densamente sono distrubiti i numeri primi?

Sia $\pi : (1, \infty) \to \mathbb{N}^*$ la funzione data dalla regola

$$\pi(x) = \text{numero di primi minori o uguali a } x$$

Sia $\log(x)$ il logaritmo naturale di x

Teorema dei numeri primi.

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\log(x)}\right)} = 1$$

Questo teorema non dice nulla sul limite della differenza delle due funzioni

$$\pi(x), \qquad \frac{x}{\log(x)}$$

all'aumentare di x senza limiti. Il teorema afferma invece che $x/\log(x)$ approssima $\pi(x)$ nel senso che l'errore relativo di approssimazione

$$\pi(x) \sim \frac{x}{\log(x)}$$

si avvicina a 0 al crescere di x senza limiti.

Sia p_n l'ennesimo numero primo. Allora, il teorema dei numeri primi è equivalente all'affermazione that

$$p_n \sim n\log(n)$$

nel senso che l'errore relativo di approssimazione si avvicina a 0 al crescere di x senza limiti.

Nota 2.1. Questo è un argomento subdolo del teorema della funzione inversa basato sull'osservazione che $\pi(p_n) = n$. Pertanto, dobbiamo solo capire la funzione inversa di $\frac{x}{\log(x)}$ è asintotico per $x\log(x)$.

L'ipotesi di Riemann irrisolta è equivalente alla seguente affermazione:

$$|\pi(x) - \mathrm{Li}(x)| < \sqrt{x}\log(x), \qquad x \geq 2.01$$

dove

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$

Non dimostreremo nessuno di questi risultati. Dimostreremo invece quanto segue:

Teorema 2.2 (Euler). *La somma*

$$\sum_{p:primo} \frac{1}{p}$$

è divergente. $(=\infty)$

Dimostrazione. (Erdős) Sia p_j il j'esimo numero primo. Se la somma converge, esiste un numero intero più piccolo k tale che

$$\sum_{j=k+1}^{\infty} \frac{1}{p_j} < \frac{1}{2} \tag{2.3}$$

Per ogni $\ell \in \mathbb{N}^*$, sia S_ℓ il sottoinsieme di $\{1, \ldots, \ell\}$ costituito da elementi che possono essere scritti come prodotti dei primi $\{p_1, \ldots, p_k\}$.

- Limite superiore per la cardinalità di S_ℓ: Ogni elemento di S_ℓ può essere scritto come un prodotto a^2b dove b è un intero privo di quadrati. Il numero di possibili scelte per b è quindi 2^k, poiché:

  $$b = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$$

  dove ogni $\epsilon_j \in \{0, 1\}$. Il numero di possibilità per a è delimitato da $\sqrt{\ell}$. Quindi,

  $$|S_\ell| < \sqrt{\ell}\, 2^k$$

- Limite inferiore per la cardinalità di S_ℓ: Sia $S'_\ell = \{1, \ldots, \ell\} - S_\ell$. Ogni elemento di S'_ℓ ha un fattore primo maggiore di p_k. Sia

$$S_\ell(j) = \{s \in S'_\ell \mid p_j | s\}$$

e nota che $S_\ell(j)$ è l'insieme vuoto non appena $p_j > \ell$. Allora,

$$S'_\ell = \cup_{j>k} S_\ell(j)$$

Inoltre, la cardinalità di $S_\ell(j)$ è al massimo ℓ/p_j. Allora,

$$|S'_\ell| < \sum_{j=k+1}^{\infty} |S_\ell(j)| < \sum_{j=k+1}^{\infty} \frac{\ell}{p_j} < \frac{\ell}{2}$$

per equazione (2.3). Ma $|S'_\ell| = \ell - |S_\ell|$. Così,

$$\ell - |S_\ell| < \frac{\ell}{2} \implies \frac{\ell}{2} < |S_\ell|$$

Combinando queste due disuguaglianze si ottiene:

$$\frac{\ell}{2} < |S_\ell| < \sqrt{\ell}\, 2^k$$

che è falso non appena $\ell > 2^{2k+2}$.

C.V.D.

Esercizi

Esercizio 2. Sia p_n l'ennesimo numero primo. Qual è il raggio di convergenza della serie di potenze:

$$\sum_{j=1}^{\infty} p_j x^j$$

(Ricordi il criterio del rapporto?)

Esercizio 3. Calcola la somma alternata

$$\frac{1}{2} - \frac{1}{3} + \frac{1}{5} - + \cdots$$

dei reciproci dei numeri primi con una precisione di $\frac{1}{1000}$. Un elenco dei primi 1000 numeri primi è qui, se si desidera utilizzare un foglio di calcolo. https://it.wikipedia.org/wiki/Lista_di_numeri
(Ricordi il criterio di Leibnitz/delle serie alternate)?

3. Piccolo teorema di Fermat

Ricordiamo il triangolo di Pascal:

$$\binom{3}{1} = 3$$

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & n=0 \\
 & & & 1 & & 1 & & & n=1 \\
 & & 1 & & 2 & & 1 & & n=2 \\
 & 1 & & 3 & & 3 & & 1 & n=3 \\
1 & & 4 & & 6 & & 4 & & 1 \quad n=4 \\
k & & k & & \text{ecc.} & & k & & k \\
\shortparallel & & \shortparallel & & k & & \shortparallel & & \shortparallel \\
0 & & 1 & & \shortparallel & & 3 & & 4 \\
 & & & & 2 & & & & \vdots
\end{array}$$

le cui voci sono i coefficienti binomiali

$$\text{binomial}(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}, \qquad n \geq k$$

Ricorda che $0! = 1$. In particolare, $\text{binomial}(n,0) = 1$ per ogni intero n non-negativo.

Ogni voce interna del triangolo è la somma delle due voci della riga precedente. Questa è una conseguenza di:

Regola di Pascal. *Siano n e $k \in \mathbb{N}^*$. Allora,*

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

Dimostrazione.

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= (n-1)!\left[\frac{n-k}{k!(n-k)!} + \frac{k}{k!(n-k)!}\right] \\
&= (n-1)!\frac{n}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}
\end{aligned}$$

C.V.D.

Teorema Binomiale. *Sia n un intero non-negativo. Allora,*

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

Dimostrazione. Sia $P(n)$ l'affermazione che per $(x+y)^n$ la formula è vera. Allora, $P(0)$ è vera perché:

$$1 = (x+y)^0 = \sum_{k=0}^{0} \binom{0}{0} x^0 y^0$$

Supponiamo che $P(n)$ sia vera. Allora,

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= x\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} + y\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} \\
&= \sum_{j=1}^{n+1} \binom{n}{j-1} x^j y^{n+1-j} + \sum_{\ell=0}^{n} \binom{n}{\ell} x^\ell y^{n+1-\ell} \\
&= x^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) x^k y^{n+1-k} + y^{n+1} \\
&= \sum_{m=0}^{n+1} \binom{n+1}{m} x^m y^{n+1-m}
\end{aligned}$$

utilizzando la regola di Pascal.

C.V.D.

Lemma 3.1. *Sia p un numero primo e k un intero tali che $0 < k < p$. Allora, p è un divisore di* $\mathrm{binomial}(p, k)$.

Dimostrazione. Esercizio per gli studenti. ☡

C.V.D.

Piccolo Teorema di Fermat. *Sia p un numero primo e n un intero. Allora, p è un divisore di $n^p - n$.*

Dimostrazione. Sia $P(n)$ l'affermazione che p è un divisore di $n^p - n$. Supponiamo che $P(n)$ sia vero per $n > 0$. Allora P(n) è vero per $n < 0$.

- Caso $p = 2$: $f(n) = n^2 - n \implies f(-n) = n^2 + n = f(n) + 2n$. Allora, $2 \mid f(n) \implies 2 \mid f(-n)$.
- Caso $p > 2$: In questo caso, p è dispari. Allora
$$f(n) = n^p - n \implies f(-n) = -n^p + n = -f(n).$$

L'affermazione $P(0)$ è vera. Supponiamo che $P(n)$ è vera. Allora,

$$\begin{aligned}(n+1)^p - (n+1) &= \sum_{k=0}^{p} \binom{p}{k} n^k - (n+1) \\ &= (n^p + 1) + \sum_{k=1}^{p-1} \binom{p}{k} - (n+1) \\ &= (n^p - n) + \sum_{k=1}^{p-1} \binom{p}{k}\end{aligned}$$

Per ipotesi di induzione, p è un divisore di $n^p - n$. Per il lemma precedente, p è un divisore di ogni termine $\mathrm{binomial}(p, k)$. Allora, p è un divisore di $(n+1)^p - (n+1)$ e quindi $P(n+1)$ è vera.

C.V.D.

Esercizio

☡ **Esercizio 4.** Sia p un numero primo e k un intero talr che $0 < k < p$. Allora, p è un divisore di $\mathrm{binomial}(p, k)$.

☡ **Esercizio 5.** Dimostra che, come conseguenza della regola di Pascal, $\mathrm{binomial}(n, k)$ è sempre un intero.

☡ **Esercizio 6.** Dimostra che un intero $n > 1$ è primo se e solo se n lo è non divisibile per nessun primo $1 < p \leq \sqrt{n}$.

4. Divide et impera

Informatica: Una classe di algoritmi che divide ricorsivamente un problema in due o più sottoproblemi di uguale dimensione fino a quando questi ultimi diventano facili da risolvere; quindi le soluzioni vengono combinate per ottenere la soluzione del problema dato.

Un famoso esempio di questo tipo di algoritmo è il calcolo di x^n.

Esempio 4.1. Calcolo x^{28}.

- $x^{28} = (x^{14})^2$
- $x^{14} = (x^7)^2$;
- $x^7 = x * (x^3)^2$;
- $x^3 = x * (x)^2$;

Come puoi vedere, ad ogni passaggio, dividiamo l'esponente a metà (sottraendo 1 se l'esponente è dispari).

```
int esponenziale(int x, int n)
{ int y;
  if(n==0) return 1;
  else
  {y = esponenziale(x, n/2);
   if ( (n % 2 ==0)) return y*y    // n is even
   else return y*y*x;              // n is odd.
}
```

ESERCIZI

Esercizio 7. Quanti passaggi utilizza l'algoritmo divide et impera per valutare x^n?

Esercizio 8. La regola di Horner è l'osservazione che il polinomio:

$$p(x) = p_0 x^n + p_1 x^{n-1} + \cdots + p_{n-1} x + p_n$$

può essere scritto come:

$$p(x) = p_n + x(p_{n-1} + x(p_{n-2} + \cdots + x(p_1 + p_0 x)))$$

Verficare questa regola utilizzando l'induzione. Quante moltiplicazioni e addizioni richiede la regola di Horner per valutare un polinomio di grado n? Quante addizioni e moltiplicazioni richiede l'algoritmo "ovvio"?

Esercizio 9. Descrivere un algoritmo per ridurre il calcolo di un polinomio di grado $n = k\ell$ che utilizza la valutazione indipendente di k polinomi di grado ℓ. (L'obiettivo qui è di fare i calcoli in parallelo)

ESERCIZIO 2

Sia p_n l'ennesimo numero primo.
Qual'é il raggio di convergenza della serie di potenze:

$$\sum_{j=0}^{\infty} p_j x^j$$

Per il criterio del rapporto:

$$\lim_{n\to\infty} \frac{p_{n+1} x^{n+1}}{p_n x^n} = \lim_{n\to\infty} \frac{p_{n+1} \cancel{x^n} x}{p_n \cancel{x^n}} = \lim_{n\to\infty} \frac{p_{n+1}}{p_n} \cdot x = \frac{p_{n+1}}{p_n} \cdot x \Rightarrow R = \frac{p_n}{p_{n+1} \cdot x}$$

ESERCIZIO 4

Sia p un numero primo e k un intero t.c. $0 < k < p$.
Allora p é un divisore di binomiale (p, k).

DIM

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \Rightarrow k!(p-k)!\binom{p}{k} = p!$$

$p \mid p!$ perché $p! = p(p-1)!$
Per il lemma di Euclide $p \mid k!$ o $p \mid (p-k)!$ o $p \mid \binom{p}{k}$
Ma poiché $0 < k < p$, $p \nmid k!$, $p \nmid (p-k)!$
$\Rightarrow p \mid \binom{p}{k}$

ESERCIZIO 5

Dimostrare che, come conseguenza della regola di Pascal, binomiale(n,k) é sempre un intero.

$P(n)$: binomiale(n,k) é un intero

$$P(n) \Rightarrow \binom{n}{k} = \underbrace{\binom{n-1}{k}}_{\in \mathbb{Z}} + \underbrace{\binom{n-1}{k-1}}_{\in \mathbb{Z}} \quad \checkmark$$

PER COSTRUZIONE DEL TRIANGOLO DI PASCAL

$$P(n+1) \Rightarrow \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \quad \checkmark$$

ESERCIZIO 6

Dimostrare che un intero $n > 1$ è primo $\iff$ n non è divisibile per nessun primo $1 < p \leq \sqrt{n}$

$\Rightarrow$) Se $n > 1$ è primo, allora $n > 1$ non è divisibile per nessun primo $1 < p \leq \sqrt{n}$

Supponiamo per assurdo n primo e n divisibile per $1 < p \leq \sqrt{n}$

$\Rightarrow p \mid n \Rightarrow p > n$ ↯

$\Rightarrow n$ è primo

$\Leftarrow$) Se $n > 1$ non è divisibile per nessun primo $1 < p \leq \sqrt{n}$ allora $n > 1$ è primo

Supponiamo per assurdo n non divisibile per nessun primo $1 < p \leq \sqrt{n}$ e n composto ($n = ab$, $a, b > 1$).

$ab \leq n \Rightarrow a \leq \sqrt{n}$ o $b \leq \sqrt{n}$

WLOG $a \leq \sqrt{n}$

a non è primo (per ipotesi), quindi è composto e ha (per il th fondam. dell'aritm.) un fattore primo $p < a$.

$\Rightarrow p < a \leq \sqrt{n}$ è un fattore primo di n ↯

$\Rightarrow n$ è primo

Lezione 4

1. Polinomi

Sia $\mathbb{Q}[x]$ l'insieme dei polinomi nella variabile x con coefficienti razionali. Sia $P_m[x]$ il $\mathbb{Q}$-sottospazio vettoriale di $\mathbb{Q}[x]$ che consiste di tutti gli elementi che può essere scritto come

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \qquad a_n, \ldots, a_0 \in \mathbb{Q}$$

Diciamo che $f \in P_n[x]$ ha grado n se $a_n \neq 0$. In questo caso, chiamiamo $a_n x^n$ il termine di ordine più alto di f e a_n il coefficiente di ordine più alto di f. Un polinomio monico è un polinomio diverso da zero con coefficiente di ordine massimo uguale a 1

Nota 1.1. Per enfasi: Il grado del polinomio zero è indefinito. Ma dobbiamo includere il polinomio zero in $P_n[x]$ per ottenere uno spazio vettoriale.

Definizione 1.2. Sia f e $g \in \mathbb{Q}[x]$. Allora diciamo che f divide g, scritto $f|g$, se esiste un polinomio $h \in \mathbb{Q}[x]$ tale che $fh = g$.

Per definire il minimo comune multiplo $\mathrm{mcm}(f, g)$ di una coppia di elementi non nulli f, $g \in Q[x]$, sia

$$S = \{\, h \in \mathbb{Q}[x] - \{0\} \mid f|h, \quad g|h \,\} \tag{1.3}$$

Allora S è non vuoto (perché?), e quindi esiste il più piccolo intero positivo d tale che $S \cap P_d[x]$ è non vuoto. Dopo aver riscalato, segue che $S \cap P_d[x]$ contiene un polinomio monico h. Per vedere che h è unico, sia $\tilde{h}$ un altro polinomio monico in $S \cap P_d[x]$. Allora, poiché h e $\tilde{h}$ sono polinomi monici di grado d, $h - \tilde{h}$ è zero o un polinomio di grado $< d$. Se $h - \tilde{h} = 0$ allora $h = \tilde{h}$. Supponiamo il contrario, cioè che $h - \tilde{h} \neq 0$. Allora,

$$f|h, \quad f|\tilde{h}, \quad g|h, \quad g|\tilde{h} \implies f|(h - \tilde{h}), \quad g|(\tilde{h} - h)$$

Quindi, $h - \tilde{h}$ è un elemento di S di grado strettamente inferiore rispetto a h e $\tilde{h}$, il che è una contraddizione.

Definizione 1.4. Il polinomio monico di grado minimo nell'insieme (1.3) è detto minimo comune multiplo di f e g.

Il prossimo risultato é l'analogo del teorema di divisione.

Teorema 1.5. *Siano f e $g \in \mathbb{Q}[x]$ e si supponga che $deg(g) > 0$. Allora, esistono elementi unici q, $r \in \mathbb{Q}[x]$ tali che*

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

dove (i) $r(x) = 0$ oppure (ii) $r(x) \neq 0$ e $\deg(r) < \deg(g)$.

Proof. Fissiamo il polinomio g e facciamo induzione su $\deg(f)$: Sia $d = \deg(g)$. Se $f = 0$ oppure $deg(f) < d$ poniamo $q = 0$ e $r = f$. Per $n \geq d$ sia $P(n)$ l'affermazione che se $\deg(f) = n$ allora esistono q, $r \in \mathbb{Q}[x]$ tale che $f = qg + r$ dove (i) $r = 0$ oppure (ii) $\deg(r) < \deg(g)$.

Per verificare $P(d)$, siano $f = f_d x^d + \cdots + f_0$ e $g = g_d x^d + \cdots + g_0$. Siano $q = f_d/g_d$ e $r = f - qg$. Allora, $f = qg + r$ e $r = 0$ oppure $\deg(r) < d$ perché abbiamo eliminato il termine di ordine più alto di f.

Supponiamo che $P(d)$,...,$P(n)$ siano vere. Sia

$$f(x) = f_{n+1}x^{n+1} + \cdots + f_0$$

un polinomio di grado $n+1$. Poniamo $q_{n+1-d} = (f_{n+1}/g_d)x^{n+1-d}$ e $\tilde{f} = f - q_{n+1-d}g$. Allora, $\deg(\tilde{f}) < n+1$ perché abbiamo eliminato il termine di ordine più alto di f. Per l'ipotesi di induzione, esistono polinomi q e r tale che $\tilde{f} = qg + r$ dove (i) $r = 0$ oppure (ii) $\deg(r) < d$. Quindi,

$$\tilde{f} = f - q_{n+1-d}g = qg + r \implies f = (q_{n+1-d} + q)g + r$$

Questo dimostra che anche $P(n+1)$ è vero. C.V.D.

Siano $f, g \in \mathbb{Q}[x]$ due polinomi tale che $(f, g) \neq (0, 0)$. Sia

$$T = \{\, af + bg \in \mathbb{Q}[x] - \{0\} \mid a, b \in \mathbb{Q}[x] \,\} \tag{1.6}$$

Lemma 1.7. *T contiene un unico polinomio monico di grado minimo.*

Proof. Il primo passo è di dimostrare che T contiene un polinomio h di minimo grado, ed e' lasciato come esercizio allo studente. Per vedere che h è unico, supponiamo che $\tilde{h}$ sia un altro polinomio monico di grado minimo in T. Perché h e $\tilde{h}$ sono polinomi monico dello stesso (=minimo) grado, $h - \tilde{h} = 0$ oppure $h - \tilde{h}$ ha un grado strettamente inferiore. Se $h - \tilde{h} = 0$ allora $h = \tilde{h}$. Supponiamo che $h - \tilde{h} \neq 0$. Per definizione,

$$h = af + bg, \qquad \tilde{h} = \tilde{a}f + \tilde{b}g \implies h - \tilde{h} = (a - \tilde{a})f + (b - \tilde{b})g \in T$$

che contraddice la minimalitá dei gradi di h e $\tilde{h}$. C.V.D.

Lemma 1.8. *Siano f, $g \in \mathbb{Q}[x]$ due polinomi tali che $(f, g) \neq (0, 0)$. Sia h l'unico polinomio monico di T di grado minimo. Allora, $h|f$ e $h|g$.*

Proof. Se $f = 0$ allora h è l'unico polinomio monico che è un multiplo scalare di g. Allo stesso modo, se $g = 0$ allora h è l'unico polinomio monico che è un multiplo scalare di f. Rimane quindi da considerare il caso in cui sia f che g siano diversi da zero. Chiaramente,

$$f,\, g \in T \implies \deg(h) \leq \min(\deg(f), \deg(g))$$

Siano $h = af + bg$ e $f = qh + r$ dove $r = 0$ oppure $\deg(r) < \deg(h)$. Se $r = 0$ allora $h|f$. Altrimenti,

$$f = q(af + bg) + r \implies r = (1 - qa)f - qbg \in T$$

Per la minimalità del grado di h, dobbiamo avere $r = 0$ ($\implies h|f$). Allo stesso modo, $h|g$ scambiando i ruoli di f e g. C.V.D.

Definizione 1.9. L'unico polinomio h di grado minimo in (1.6) si chiama massimo comun divisore $\mathrm{mcd}(f, g)$ di f e g.

Per calcolare $\mathrm{mcd}(f, g)$, usiamo l'algoritmo euclideo: Per analogia con i numeri interi:

$$f = qg + r \implies \mathrm{mcd}(f, g) = \mathrm{mcd}(r, g) = \mathrm{mcd}(g, r)$$

Esempio 1.10. Se $f \in \mathbb{Q}[x]$ and $c \in \mathbb{Q} - \{0\}$ allora $\mathrm{mcd}(f, c) = 1$ perché c ha grado 0.

Esempio 1.11. $f = x^2 - 3x + 2$, $g = x^2 - 2x + 1$

$$x^2 - 3x + 2 = (1)(x^2 - 2x + 1) + (-x + 1), \qquad q = 1, \quad r = -x + 1$$

Quindi,

$$\mathrm{mcd}(x^2 - 3x + 2, x^2 - 2x + 1) = \mathrm{mcd}(-x + 1, x^2 - 2x + 1) = \mathrm{mcd}(x^2 - 2x + 1, -x + 1)$$

Adesso, $x^2 - 2x + 1 = (x - 1)^2 = (-x + 1)^2$, e poi

$$\mathrm{mcd}(x^2 - 2x + 1, -x + 1) = \mathrm{mcd}(0, -x + 1) = x - 1$$

Esempio 1.12. $f = 6x^4 + 2x^3 + 5x^2 + 3x + 2$, $g = 2x^2 + 1$

$$6x^4 + 2x^3 + 5x^2 + 3x + 2 = (3x^2 + x + 1)(2x^2 + 1) + (2x + 1)$$

Quindi,

$$\begin{aligned}\mathrm{mcd}(6x^4 + 2x^3 + 5x^2 + 3x + 2, 2x^2 + 1)\\ &= \mathrm{mcd}((3x^2 + x + 1)(2x^2 + 1) + (2x + 1), 2x^2 + 1)\\ &= \mathrm{mcd}(2x + 1, 2x^2 + 1) = \mathrm{mcd}(2x^2 + 1, 2x + 1)\end{aligned}$$

Tuttavia, $2x^2 + 1 = (1/2)(2x + 1)(2x - 1) + 3/2$, quindi

$$\begin{aligned}\mathrm{mcd}(2x^2 + 1, 2x + 1) &= \mathrm{mcd}((1/2)(2x + 1)(2x - 1) + 3/2, 2x + 1)\\ &= \mathrm{mcd}(3/2, 2x + 1) = \mathrm{mcd}(2x + 1, 3/2) = 1\end{aligned}$$

Esercizi

Esercizio 1. Calcolare $\mathrm{mcd}(x^4 - 1, x^4 + 2x^2 - 3)$.

Esercizio 2. Mostra che se $f \in \mathbb{Q}[x] - \{0\}$ e $f(0) = 0$ allora $x|f(x)$. Più in generale, dimostra che se r è un numero razionale tale che $f(r) = 0$, allora $(x - r)|f(x)$.

Esercizio 3. Mostra che l'insieme T che appare in (1.6) contiene un elemento monico di grado minimo.

Esercizio 4. Ricordiamo che la prova per il contropositivo è semplicemente la dichiarazione che

$$[P \implies Q] \iff [(\neg Q) \implies (\neg P)]$$

dove $\neg R$ è la negazione di R. Verifica questo fatto usando le seguenti tavole di verità:

P	Q	$P \implies Q$
F	F	V
F	V	V
V	F	F
V	V	V

P	Q	$P \iff Q$
F	F	V
F	V	F
V	F	F
V	V	V

2. Fattorizzazione

Un polinomio costante è un polinomio della forma $f(x) = f_0$ per qualche $f_0 \in \mathbb{Q}$. In particolare, un polinomio non-costante ha grado maggiore di zero.

Definizione 2.1. Un polinomio $f \in \mathbb{Q}[x]$ non costante è irriducibile se non esistono polinomi non-costante g, $h \in \mathbb{Q}[x]$ tale che $f = gh$. Altrimenti, f è riducibile.

Esempio 2.2. Un polinomio di grado 1 è irriducibile: Se $f = gh$ dove g e h sono non-costante allora $deg(g) \geq 1$ e $\deg(h) \geq 1$. Quindi $\deg(f) = \deg(g) + \deg(h) > 1$, contaddizione.

Esempio 2.3. Se $f \in \mathbb{Q}[x]$ è irriducibile e $c \in \mathbb{Q} - \{0\}$ allora anche cf è irreducibile.

Esempio 2.4. Se $f \in Q[x] - \{0\}$ ha un radice rationale $x = r$ allora f è riducibile perché $(x - r)|f$.

Esempio 2.5. Sia $f \in \mathbb{Q}[x]$ un polinomio di grado 2. Allora, f è irriducibile se e sole se f non ha una radice razionale. Per vedere questo, sia P la proposizione che f è irriducibile e sia Q la proposizione che f non ha una radice razionali. Così il contropositiva di $P \implies Q$ è $(\neg Q) \implies (\neg P)$, i.e. se f ha una radice razionale allora f è riducibile (vedi esempio precedente). Il contropositivo di $Q \implies P$ è $(\neg P) \implies (\neg Q)$, cioè se f è riducibile di grado 2 allora f ha una radice razionale. Perché f ha grado 2, f riducibile implica che $f = gh$ dove g e h ha grado 1, e quindi f ha una radice razionale.

Lemma 2.6. *Sia f, $g \in \mathbb{Q}[x]$. Se f è irriducibile allora $\mathrm{mcd}(f, g) = 1$ oppure $f|g$.*

Proof. Sia $m = \mathrm{mcd}(f, g)$. Allora, $m|f$ e quindi $f = mq$ per qualche $\mathbb{Q}[x]$. Per definizione, poiché f è irriducibile, segue che o m o q ha grado 0, cioè o (i) $m = 1$ o (ii) $m = uf$ per qualche $u \in \mathbb{Q} - \{0\}$. Nel caso (i), $m = \mathrm{mcd}(f, g) = 1$. Nel caso (ii), $m = \mathrm{mcd}(f, g) = uf|g \implies f|g$. C.V.D.

Il risultato seguente è l'analogo del lemma di Euclide per i polinomi:

Lemma 2.7. *Sia $f \in \mathbb{Q}[x]$ irriducibile. Se $f|gh$ allora $f|g$ o $f|h$.*

Proof. In base al lemma precedente, se f non divide g allora $\mathrm{mcd}(f, g) = 1$. Pertanto, esistono a, $b \in \mathbb{Q}[x]$ tali che $1 = af + bg$ e quindi $h = afh + \cancel{bg}$. Per ipotesi $f|\cancel{gh}$ e $f|afh$ segue che $f|h$. bgh bgh C.V.D.

Combinando i risultati precedenti, otteniamo ora l'analogo della fattorizzazione unica dei numeri interi per i polinomi:

Teorema di Fattorizzazione Unica. *Ogni polinomio non costante $f \in \mathbb{Q}[x]$ può essere scritto come prodotto di polinomi irriducibili. Inoltre, questa fattorizzazione è unica: Se*

$$f(x) = p_1(x) \cdots p_r(x), \qquad f(x) = q_1(x) \cdots q_s(x) \tag{2.8}$$

sono due fattorizzazioni in un prodotto di irriducibili allora (i) $r = s$ e (ii) Esiste una permutazione $sigma$ di $\{1, \ldots, r\}$ e una collezione di costanti non nulle $\{c_j\}$ tali che

$$q_j(x) = c_j p_{\sigma(j)}(x)$$

per $j = 1 \ldots, r$.

Proof. Il primo passo consiste nel dimostrare che ogni polinomio non-costante $f \in \mathbb{Q}[x]$ è un prodotto di polinomi irriducibili. A tal fine, utilizziamo l'induzione sul grado di f. Sia $P(n)$ la proposizione che ogni polinomio di grado n può essere scritto come prodotto di fattori irriducibili. Allora $P(1)$ è vera in base all'esempio precedente. Supponiamo che $P(1), P(n)$ siano vere, e che f sia un polinomio di grado $n + 1$. Allora, o f è irriducibile oppure $f = gh$ dove $deg(g)$ e $deg(h) < n+1$. Per l'ipotesi di induzione, sia g che h possono essere scritti come prodotto di polinomi irriducibili. polinomi irriducibili.

Supponiamo ora di avere due fattorizzazioni di f come nell'equazione (2.8). Allora, dal momento che $p_1|f$ e $f = q_1 \cdots q_r$ segue che $p_1|q_j$ per qualche j (esercizio). Dal momento che p_1 e q_j sono irriducibili, ne consegue che $q_j = c_1 p_1$ per qualche $c \in \mathbb{Q} - \{0\}$. Dopo aver reordinato i fattori, possiamo assumere che $j = 1$.

Per completare la dimostrazione, ora induciamo sul numero totale di fattori $r + s$ che compaiono nell'equazione (2.8). Sia $P(n)$ l'affermazione che se un polinomio non costante f ha una coppia di fattorizzazioni irriducibili (2.8) tali che $r + s \leq n$ allora $r = s$ e la fattorizzazione è unica fino al riordino dei fattori e alla loro moltiplicazione per elementi non nulli di $\mathbb{Q}$. L'affermazione $P(1)$ è vera perché non esistono polinomi di questo tipo, dato che ogni lato di (2.8) contiene almeno un fattore. L'affermazione

$P(2)$ è vera perché in questo caso $r = s = 1$ e la fattorizzazione è $f = p_1 = q_1$ dove $q_1 = c_1 p_1$. Supponiamo che $P(1), \dots, P(n)$ siano veri. In base al paragrafo precedente, la fattorizzazione assume la forma

$$p_1 p_2 \cdots p_r = (c_1 p_1) q_2 \cdots q_s$$

Dividendo entrambi i lati per p_1 e assorbendo la costante c_1 in q_2, otteniamo

$$g = p_2 \cdots p_r = q_2 \cdots q_s$$

dove il numero totale di fattori è $(r-1) + (s-1) = r + s - 2 = n + 1 - 2 = n - 1$. In particolare, poiché $P(n-1)$ è vero, ne consegue che (i) $r - 1 = s - 1$ e (ii) la fattorizzazione di g in fattori irriducibili è unica fino a riordino e moltiplicazione per elementi non nulli di $\mathbb{Q}$. Pertanto, $r = s$ e la fattorizzazione (2.8) è unica fino a riordino e moltiplicazione per elementi non nulli di $\mathbb{Q}$. C.V.D.

Nota 2.9. Se f è un polinomio monico non-costante allora f è un prodotto di fattori irriducibili ognuno dei quali è un polinomio monico.

Corollary 2.10. *Siano f, $g \in \mathbb{Q}[x]$ polinomi monici non-costanti. Allora,*

$$fg = \operatorname{mcm}(f, g) \operatorname{mcd}(f, g)$$

Proof. Sia $\{p_1, \dots, p_n\}$ l'insieme dei fattori irriducibili di f e g. Allora, possiamo scrivere

$$f = p_1^{a_1} \dots p_n^{a_n}, \qquad g = p_1^{b_1} \dots p_n^{b_n}$$

dove si ammette la possibilità che $a_j = 0$ se p_j non è un fattore di f e $b_j = 0$ se p_j non è un fattore di g. Allora,

$$\operatorname{mcm}(f, g) = p_1^{\max(a_1, b_1)} \cdots p_n^{\max(a_n, b_n)}$$
$$\operatorname{mcd}(f, g) = p_1^{\min(a_1, b_1)} \cdots p_n^{\max(a_n, b_n)}$$

Quindi

$$\begin{aligned} \operatorname{mcm}(f, g) \operatorname{mcd}(f, g) &= p_1^{\max(a_1, b_1) + \min(a_1, b_1)} \cdots p_n^{\max(a_n, b_n) + \min(a_1, b_1)} \\ &= p_1^{a_1 + b_1} \cdots p_n^{a_n + b_n} = fg \end{aligned}$$

C.V.D.

Esempio 2.11. $f = x^2 - 3x + 2$, $g = x^2 - 2x + 1 \implies \operatorname{mcd}(f, g) = (x - 1)$. Allora,

$$\operatorname{mcm}(f, g) = fg / \operatorname{mcd}(f, g) = \frac{(x^2 - 3x + 2)(x^2 - 2x + 1)}{(x - 1)} = x^3 - 4x^2 + 5x - 2$$

Esercizi

♉ **Esercizio 5.** Trovare il mcm e il mcd dei seguenti polinomi:

$$f = x^4 + 10x^3 + 35x^2 + 50x + 24, \qquad g = x^4 - 2x^3 - 13x^2 + 14x + 24$$

♉ **Esercizio 6.** Dimostrare che se $f \in \mathbb{Q}[x]$ è irriducibile e $f | g_1 g_2 \cdots g_r$ allora $f | g_j$ per qualche g_j.

♉ **Esercizio 7.** Sia $f \in \mathbb{Q}[x]$ di grado 3. Mostrare che f è irriducibile se e solo se f non ha radici razionali.

♉ **Esercizio 8.** Costruire un polinomio riducibile $f \in \mathbb{Q}[x]$ di grado 4 senza radici razionali.

♉ **Esercizio 9.** Dimostrare che se f è un polinomio monico non-costante allora f è un prodotto di fattori irriducibili ognuno dei quali è un polinomio monico.

3. Teorema delle radici razionali

Sia $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ l'insieme dei polinomi con coefficienti interi. Le radici razionali di un polinomio non-costante $f \in \mathbb{Q}[x]$ tali che $f(0)$ sia diverso da zero possono essere trovate come segue: Sia m il più piccolo intero positivo tale che $g = mf \in \mathbb{Z}[x]$. Allora, r è una radice di f se e solo se r è una radice di g. Sia

$$g(x) = g_n x^n + \cdots + g_0$$

dove g_n, $g_0 \neq 0$. Allora, ogni radice razionale di f è della forma $r = p/q$ dove $p|g_0$, $q|g_n$ e $\mathrm{mcd}(p, q) = 1$.

Proof. Si supponga che Si supponga che p/q sia una radice di g con $\mathrm{mcd}(p, q) = 1$. Allora,

$$g_n \left(\frac{p}{q}\right)^n + g_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + g_0 = 0$$

Dopo aver moltiplicato entrambi i lati per q^n, otteniamo:

$$g_n p^n + g_{n-1} p^{n-1} q + \cdots + g_0 q^n = 0 \tag{3.1}$$

Equivalente,

$$p(g_n p^{n-1} + \cdots + g_1 q^{n-1}) = -g_0 q^n$$

che implica $p|g_0 q^n$. Per ipotesi, $\mathrm{mcd}(p, q) = 1$. Quindi, $p|g_0$. D'altra parte, l'equazione (3.1) può anche essere riscritta come

$$q(g_{n-1} p^{n-1} + \cdots + g_0 q^{n-1}) = -g_n p^n$$

quindi $q|g_n p^n$. Poiché $\mathrm{mcd}(p, q) = 1$ ne consegue che $q|g_n$. C.V.D.

Nota 3.2. Se $f(0) = 0$ allora $r = 0$ è una radice $x|f$. Scrive $f = x^n h$ con $h(0)$ diversa da zero e applicare il metodo descritto nel paragrafo precedente a $h(x)$.

Esempio 3.3. Sia $r = p/q$ una radice razionale di $f = x^3 - 7x - 6$ with $\mathrm{mcd}(p, q) = 1$. Allora $p|(-6)$ e $q|1$. Quindi, le possibili radici razionali di f sono ± 1, ± 2, ± 3, ± 6. Si calcola che:

$$x^3 - 7x - 6 = (x + 1)(x + 2)(x - 3)$$

Per continuare, notiamo il seguente corollario del test della radice razionale:

Proposizione 3.4. *Sia $f \in \mathbb{Z}[x]$ un polinomio non-constante monico. Allora, ogni radice razionale di f é un numero intero.*

Proof. Scrive $f = x^n + f_{n-1} x^{n-1} + \cdots + f_0$. Sia $r = p/q$ una radice razionale di f con $\mathrm{mcd}(p, q) = 1$. Allora, $p|f_0$ e $q|1$. Quindi, $r \in \mathbb{Z}$. C.V.D.

Sia r una radice di un polinomio monico non-costante $f \in \mathbb{Z}[x]$ e $a \in \mathbb{Z}$. Allora $g(x) = f(x + a)$ è un polinomio monico con radice $r - a$. Pertanto, $r - a$ è un divisore del termine costante $g(0)$ di $g(x)$. Questo trucco a volte può essere utilizzato per accelerare il processo di trovare le radici intere:

Esempio 3.5. Sia $f = x^5 + 7x^2 - 60$. Allora, ogni radice intera di f è contenuta nell'insieme

$$R_0 = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60\}$$

$r=1 \Rightarrow r-1=0 \notin \{\pm 1, \pm 2, \pm 4, \pm 13\}$

$r=-1 \Rightarrow r-1=-2 \in$ " $\Rightarrow -1 \in R_1$

$r=2 \Rightarrow r-1=1 \in$ " ma $f(1) \neq 0$

$r=-2 \Rightarrow r-1=-3 \notin$ "

$r=3 \Rightarrow r-1=2 \in$ " $\Rightarrow 3 \in R_1$

$r=-3 \Rightarrow r-1=-4 \in$ " $\Rightarrow -3 \in R_1$ ....

di divisori interi di 60. Per essere sistematici, consideriamo le possibili radici in ordine crescente di valore assoluto.

$f(1) = -52$: Quindi $(r-1)|52 = (4)(13)$, e di conseguenza:

$$[(r-1) \in \{\pm 1, \pm 2, \pm 4, \pm 13\}] \wedge [r \in R_0] \implies r \in R_1 = \{2, -1, 3, -3, 5, -12\}$$

$f(-1) = -54$: Quindi $(r+1)|54 = (2)(3^3)$, e di consequenza:

$$[(r+1) \in \{\pm 1, \pm 2, \overset{\pm 3}{\cancel{\pm 4}}, \pm 9, \pm 27\}] \wedge [r \in R_1] \implies r \in R_2 = \{-3, 2, \cancel{3}\}$$

Si calcola che $f(2) = 0$, ~~$f(3) = 246$~~ and $f(-3) = -240$. Cosí, 2 è la sola radice razionale di f.

Esercizi

Esercizio 10. Scrivere $x^3 - 8x^2 + 3x - 24$ come prodotto di polinomi irriducibili in $\mathbb{Q}[x]$.

Esercizio 11. Scrivere $x^4 + 3x^2 - 4$ come prodotto di polinomi irriducibili in $\mathbb{Q}[x]$.

Esercizio 12. Verificare che $x^3 - 41x + 60 \in \mathbb{Q}[x]$ è irriducibile.

ESERCIZIO 1

Calcolare $MCD(x^4-1, x^4+2x^2-3)$

$$
\begin{array}{cccc|c}
x^4 & +2x^2 & -3 & & x^4-1 \\ \cline{5-5}
x^4 & & -1 & & 1 \\ \cline{1-3}
 & 2x^2 & -2 & & \\
\end{array}
$$

$$x^4+2x^2-3 = (1)(x^4-1) + 2x^2-2$$

$$MCD(x^4-1, x^4+2x^2-3) = MCD(x^4-1, 2x^2-2) =$$

$$
\begin{array}{cccc|c}
x^4 & & & -1 & 2x^2-2 \\ \cline{5-5}
x^4 & -x^2 & & & \frac{x^2}{2}+\frac{1}{2} \\ \cline{1-4}
 & -x^2 & & -1 & \\
 & -x^2 & & -1 & \\ \cline{2-4}
 & & & 0 & \\
\end{array}
$$

$$x^4-1 = \left(\frac{x^2}{2}+\frac{1}{2}\right)(2x^2-2) + 0$$

$$= MCD(0, 2x^2-2) = MCD(0, 2(x^2-1)) = x^2-1$$

ESERCIZIO 2

Mostrare che se $f \in \mathbb{Q}[x] - \{0\}$ e $f(0) = 0$ allora $x \mid f(x)$. Più in generale dimostrare che se r è un numero razionale t.c. $f(r) = 0 \Rightarrow (x-r) \mid f(x)$

i) $f(x) \in \mathbb{Q}[x] - \{0\}$, $f(0) = 0 \Rightarrow x \mid f$

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$
$$\Rightarrow f(0) = a_0$$
$$f(0) = 0 \Rightarrow a_0 = 0$$
$$\Rightarrow f(x) = a_n x^n + \dots + a_1 x = x(a_n x^{n-1} + \dots + a_1)$$
$$\Rightarrow x \mid f$$

ii) $f(x) \in \mathbb{Q}[x] - \{0\}$, $f(\overset{\in \mathbb{Q}}{r}) = 0 \Rightarrow (x-r) \mid f(x)$

$$f(x) = a_n x^n + \dots + a x + a_0$$
$$f(x) = q(x)(x-r) + r(x)$$
$$\Rightarrow f(r) = q(x) \cdot 0 + r(x)$$
$$\Rightarrow f(r) = 0 \Leftrightarrow r(x) = 0 \Rightarrow (x-r) \mid f(x)$$

ESERCIZIO 3

Mostrare che l'insieme $T = \{af + bg \in \mathbb{Q}[x] - \{0\} : a, b \in \mathbb{Q}[x]\}$ contiene un elemento monico di grado minimo.

$T \neq \emptyset$ perché $fg \in T$

$\Rightarrow \exists$ il più piccolo intero positivo d t.c. $T \cap P_d[x] \neq \emptyset$

$h \in T \cap P_d[x] \Rightarrow$ dopo avere riscalato h, h è monico

ESERCIZIO 4

Verificare che $[P \Rightarrow Q] \Leftrightarrow [\neg Q \Rightarrow \neg P]$

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$[P \Rightarrow Q] \Leftrightarrow [\neg Q \Rightarrow \neg P]$
F	F	V	V	V	V	V
F	V	V	F	V	F	F
V	F	F	V	F	V	F
V	V	F	F	V	V	V

ESERCIZIO 5

Trovare mcm e MCD di:

$(f, g) = (x^4 + 10x^3 + 35x^2 + 50x + 24,\ x^4 - 2x^3 - 13x^2 + 14x + 24)$

$$
\begin{array}{l|l}
x^4 + 10x^3 + 35x^2 + 50x + 24 & x^4 - 2x^3 - 13x^2 + 14x + 24 \\
\cline{2-2}
x^4 - 2x^3 - 13x^2 + 14x + 24 & 1 \\
\cline{1-1}
\quad 12x^3 + 48x^2 + 36x &
\end{array}
$$

$MCD(f, g) = MCD(x^4 - 2x^3 - 13x^2 + 14x + 24,\ 12x^3 + 48x^2 + 36x) =$

$$
\begin{array}{l|l}
x^4 - 2x^3 - 13x^2 + 14x + 24 & 12x^3 + 48x^2 + 36x \\
\cline{2-2}
x^4 + 4x^3 + 3x^2 & \frac{x}{12} - \frac{1}{2} \\
\cline{1-1}
\quad -6x^3 - 16x^2 + 14x + 24 & \\
\quad -6x^3 - 24x^2 - 18x & \\
\cline{1-1}
\qquad\qquad 8x^2 + 32x + 24 &
\end{array}
$$

$= MCD(12x^3 + 48x^2 + 36x,\ 8x^2 + 32x + 24) =$

$$
\begin{array}{l|l}
12x^3 + 48x^2 + 36x & 8x^2 + 32x + 24 \\
\cline{2-2}
12x^3 + 48x^2 + 36x & \frac{3}{2}x \\
\cline{1-1}
\qquad\qquad 0 &
\end{array}
$$

$= MCD(8x^2 + 32x + 24, 0) = MCD(x^2 + 4x + 3, 0) =$
$= x^2 + 4x + 3$

$$mcm(f,g) = \frac{f \cdot g}{MCD(f,g)} = x^6 + 4x^5 - 17x^4 - 80x^3 + 4x^2 + 256x + 192$$

ESERCIZIO 6

Dimostrare che se $f \in \mathbb{Q}[x]$ è irriducibile e $f | g_1 g_2 \dots g_r$ allora $f | g_j$ per qualche j.

$f | g \Rightarrow MCD(g, f) = m \neq 1$
$\exists u, v$ t.c. $fu + (g_1 \dots g_r)v = m$
WLOG
$\Rightarrow g_1 (g_2 \dots g_r) v = m g_1 - f u g_1 \Rightarrow f | g_1$

ESERCIZIO 7

Sia $f \in \mathbb{Q}[x]$ di grado 3. Mostrare che f è irriducibile $\Leftrightarrow$ f non ha radici razionali.

$P = \{ f \text{ irriducibile} \}$
$Q = \{ f \text{ non ha radici razionali} \}$
Il contronominale di $P \Rightarrow Q$ è $\neg Q \Rightarrow \neg P$
cioè se f ha una radice razionale allora è riducibile.
Il contronominale di $Q \Rightarrow P$ è $\neg P \Rightarrow \neg Q$
cioè se f è riducibile allora f ha una radice razionale.
$\deg(f) = 3$, f riducibile $\Rightarrow f = gh$, $\deg(g) = 1$ o $\deg(h) = 1$
$\Rightarrow f$ ha una radice razionale

ESERCIZIO 8

Costruire un polinomio riducibile $f \in \mathbb{Q}[x]$ di grado 4 senza radici razionali.

$$f = (x^2+1)(x^2+2)$$

ESERCIZIO 9

Dimostrare che se f é un polinomio monico non costante allora f é un prodotto di fattori irriducibili ognuno dei quali é un pol. monico.

$$f \text{ monico} \Rightarrow f = x^n + \dots + f_0$$

$$f = \underbrace{(\cancel{a_{n_1}} x^{n_1} + \dots + a_0)(\cancel{b_{n_2}} x^{n_2} + \dots + b_0)(\dots) \dots}_{a_{n_1} b_{n_2} \dots}$$

dove $a_{n_1} b_{n_2} \dots = 1$

ESERCIZIO 10

Scrivere $x^3 - 8x^2 + 3x - 24$ come prodotto di polinomi irriducibili in $\mathbb{Q}[x]$

$$(p/q)^3 - 8(p/q)^2 + 3(p/q) - 24 = 0$$

$$p^3 - 8p^2q + 3pq^2 - 24q^3 = 0$$
$$p(p^2 - 8pq + 3q^2) = 24q^3$$

$$p \mid 24q^3 \Rightarrow p \mid 24$$

$$-8p^2q + 3pq^2 - 24q^3 = -p^3$$
$$q(-8p^2 + 3pq - 24q^2) = -p^3$$

$$q \mid p^3 \Rightarrow q \mid 1$$

$$q = \pm 1$$
$$p = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8\} \quad (*)$$

Ogni radice razionale di f è della forma p/q ed è quindi contenuta nell'insieme $(*)$

$$f(8) = 0 \Rightarrow f = (x-8)\cdot h = (x-8)(x^2+3)$$

$$\begin{array}{r|l}
x^3 - 8x^2 + 3x - 24 & x - 8 \\ \cline{2-2}
x^3 - 8x^2 \qquad\qquad & x^2 + 3 \\ \cline{1-1}
3x - 24 & \\
3x - 24 & \\ \cline{1-1}
0 &
\end{array}$$

ESERCIZIO 11

Scrivere $x^4 + 3x^2 - 4$ come prodotto di polinomi irriducibili in $\mathbb{Q}[x]$

$$(p/q)^4 + 3(p/q)^2 - 4 = 0$$

$$p^4 + 3p^2q^2 - 4q^4 = 0$$

$$p(p^3 + 3pq^2) = 4q^4 \Rightarrow p \mid 4$$

$$q(3p^2q - 4q^3) = -p^4 \Rightarrow q \mid 1$$

$$q = \pm 1$$

$$p = \{\pm 1, \pm 2, \pm 4\}$$

$$\left.\begin{array}{l} f(1) = 0 \\ f(-1) = 0 \end{array}\right\} \Rightarrow f = (x-1)(x+1)(x^2+4)$$

$$\begin{array}{r|l} x^4 + 3x^2 - 4 & x^2 - 1 \\ \cline{2-2} \underline{x^4 - x^2} & x^2 + 4 \\ 4x^2 - 4 & \\ \underline{4x^2 - 4} & \\ 0 & \end{array}$$

ESERCIZIO 12

Verificare che $x^3 - 41x + 60 \in \mathbb{Q}[x]$ è irriducibile

$\deg(f) = 3 \Rightarrow f$ irriducibile $\Leftrightarrow f$ non ha radici razionali

$(p/q)^3 - 41(p/q) + 60 = 0$

$p^3 - 41pq^2 + 60q^3 = 0$

$p(p^2 - 41q^2) = -60q^3 \Rightarrow p \mid 60$

$q(-41pq + 60q^2) = -p^3 \Rightarrow q \mid 1$

$q = \pm 1$

$p = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60\}$ R_0

$f(1) = 20 = 2^2 \cdot 5$

$\Rightarrow (r-1) \in \{\pm 1, \pm 2, \pm 4, \pm 5\} \wedge r \in R_0 \Rightarrow R_1 = \{-1, \pm 3, -4, 6\}$

$f(-1) = 100$

$f(3) = -36 \qquad f(-3) \neq 0$

$f(-4) = 160 \qquad f(6) \neq 0$

$f(p/q) \neq 0 \ \forall p, q \Rightarrow f$ irriducibile

Lezione 5

1. NP-DIFFICILE

Un problema decisionale è un problema il cui risultato è un singolo valore booleano: SI o NO.

Consideriamo tre classi di problemi, l'ultimo dei quali non deve necessariamente essere un problema decisionale:

- P è l'insieme dei problemi decisionali che possono essere risolti in tempo polinomiale. Intuitivamente, P è l'insieme dei problemi che possono essere risolti rapidamente.

  Esempio 1.1. Una data matrice quadrata con elementi interi è invertibile? (Calcola il determinante usando le mosse di Gauss).

  Esempio 1.2. Data una coppia di numeri interi positivi A e B, è $\overset{\text{MCD}}{\cancel{\text{mcm}}}(A, B) = 1$? (Utilizzate l'algoritmo euclideo).

- NP è l'insieme dei problemi decisionali con la seguente proprietà: Se la risposta è SI, allora esiste una dimostrazione di questo fatto che può essere verificata in tempo polinomiale. Intuitivamente, NP è l'insieme di problemi decisionali in cui è possibile verificare rapidamente una risposta SI se si dispone della soluzione.

  Esempio 1.3. Decidere se un dato grafo ammette una colorazione con un insieme di k colori per un dato $k > 2$. (Ciò significa che due vertici adiacenti non hanno lo stesso colore).

- Un problema H è NP-difficile se ogni problema di classe NP può essere risolto in tempo polinomiale, dato un "oracolo" che risolve H in tempo unitario.

  Esempio 1.4. (Problema di somma dei sottoinsiemi). Dato un insieme di numeri interi S, esiste un sottoinsieme finito e non vuoto di S la cui somma degli elementi è zero (o un altro valore fisso)?

Nota 1.5. Il test di primalità di Agrawal-Kayal-Saxena determina se un dato intero positivo è primo in tempo polinomiale. (PROBLEMA DI CLASSE P)

ESERCIZI

Esercizio 1. A quale classe appartiene il problema di determinare se un dato polinomio con coefficienti razionali ha una radice razionale? P

Esercizio 2. Fornisci un esempio di un problema NP derivante dall'informatica (giustifica la tua risposta). CLIQUE, SAT (SODDISF. DI FORMULE BOOLEANE), ZAINO, CAMMINO HAMILTONIANO

Esercizio 3. Fornisci un esempio di un problema informatico per il quale si può dimostrare che non esiste una soluzione in tempo polinomiale.

- IL PROBLEMA DELL'ARRESTO: SI PUÒ DIM. CHE NON ESISTE UN ALGORITMO CHE DECIDA IN TEMPO POLINOMIALE SE UN CERTO ALGORITMO ARBITRARIO TERMINA LA SUA COMPUTAZIONE SU DATI ARBITRARI
- EQUIVALENZA TRA DUE PROGRAMMI: È INDECIDIBILE STABILIRE SE DUE PROGR. A PARITÀ DI INPUT PRODUCONO LO STESSO OUTPUT

2. Teoria dei reticoli

Sia $B = \{b_1, \dots, b_m\}$ un insieme di vettori linearmente indipendenti in $\mathbb{R}^n$. Sia L lo spazio costituito dalle combinazioni lineari integrali di questi vettori:

$$L = \{\lambda_1 b_1 + \cdots + \lambda_m b_m \mid \lambda_1, \dots, \lambda_m \in \mathbb{Z}\}$$

Chiamiamo L un reticolo e B una base per L. Per semplicità, se non diversamente specificato, assumiamo che $m = n$.

Nota 2.1. A volte scriviamo $L(B)$ invece di L per chiarire il ruolo della base B.

Esempio 2.2. $L = \mathbb{Z}^n$, $B = \{e_1, \dots, e_n\}$.

Esempio 2.3. Sia $n \geq 2$.

$$L = \{\, (x_1, \dots, x_n) \in \mathbb{Z}^n \mid 2|(x_1 + \cdots + x_n) \,\} \tag{2.4}$$

è un reticolo con base

$$b_j = e_j - e_{j+1}, \quad j = 1, \dots, n-1, \qquad b_n = e_n + e_{n-1} \tag{2.5}$$

Per continuare, ricordiamo che dall'algebra lineare, se dobbiamo misurare sia lunghezze che angoli, abbiamo bisogno di un prodotto scalare. Se abbiamo bisogno solo di lunghezze, possiamo invece utilizzare una norma.

Definizione 2.6. Per un numero reale $p \geq 1$, la p-norma di $x \in \mathbb{R}^n$ è definita da

$$|(x_1, \dots, x_n)|_p = (|x_1|^p + \cdots + |x_n|^p)^{\frac{1}{p}}$$

Definiamo anche:

$$|(x_1, \dots, x_n)|_\infty = \max(|x_1|, \dots, |x_n|)$$

Proposizione 2.7. *Per ogni $p \geq 1$, la p-norma e una norma nel senso di algebra lineare:*

- *Solo il vettore zero ha lunghezza zero, i.e. $|x|_p = 0 \iff x = 0$;*
- *La lunghezza del vettore è omogenea positiva rispetto alla moltiplicazione per uno scalare, i.e. $|\lambda x|_p = |\lambda||x|_p$;*
- *$|x + y|_p \leq |x|_p + |y|_p$ (triangolare disuguaglianza).*

Esempio 2.8. $p = 2$ è la distanza euclidea standard. Spesso scriviamo $|x|$ invece di $|x|_2$.

Esempio 2.9. Per $p = 1$, abbiamo $|(x_1, \dots, x_n)| = |x_1| + \cdots |x_n|$.

Il seguente teorema implica che, in molti casi, possiamo scegliere la norma più adatta al problema.

Teorema 2.10. *Le norme $|*|_p$ e $|*|_q$ sono equivalenti nel senso che esistono costanti C e D tali che*

$$C|x|_p \leq |x|_q \leq D|x|_p$$

per ogni $x \in \mathbb{R}^n$.

Definizione 2.11. Il problema del vettore più breve (SVP$_p$) nella norma p è il seguente:

- **INPUT**: Un reticolo L specificato da una base B.
- **OUTPUT**: Si ottiene il vettore (diverso da zero) più breve in quella base utilizzando la norma $|*|_p$.

Teorema 2.12. *(P. van Emde Boas, 1979) SVP$_\infty$ è* NP*-difficile.*

Nota 2.13. Purtroppo, per il problema del vettore più breve, non possiamo usare l'equivalenza tra $|*|_p$ e $|*|_\infty$ per concludere che SVP_p è NP-difficile.

Con un abuso di notazione, identifichiamo la base di un reticolo L con una matrice B $n \times n$ tale che $B(\mathbb{Z}^n) = L$. [1] Sia T una matrice di rango pieno con valori interi. Allora BT è la base di un nuovo reticolo.

Esempio 2.14.

$$B = (\vec{b}_1 \;\; \vec{b}_2), \quad T = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \implies BT = (\vec{b}_1 + 2\vec{b}_2 \;\; 3\vec{b}_2)$$

Per eliminare la dipendenza dalla scelta della base B di L, ricordiamo il seguente fatto di algebra lineare:

QUADRATA

Teorema 2.15. *Sia T una matrice con solo valori (voci) interi. Allora T^{-1} esiste e ha solo valori (voci) interi se e solo se $\det(T) = \pm 1$. In questo caso, si dice che T è una matrice unimodulare.*

Osserviamo poi quanto segue:

Lemma 2.16. *Sia T una matrice invertibile con voci interi e B una base di un reticolo $L = L(B)$. Allora, $L(BT) \subseteq L(B)$.*

Dimostrazione. $L(BT) = BT(\mathbb{Z}^n) \subseteq B(\mathbb{Z}^n) = L(B)$.

C.V.D.

Teorema 2.17. *$L(B) = L(C)$ se e sole se esiste una matrice U unimodulare tale che $C = BU$.*

Dimostrazione. Per il lemma, $C = BU \implies L(C) \subseteq L(B)$. Nello stesso modo, $C = BU$ e U è unimodulare implica che $B = CU^{-1}$. Quindi, $L(B) = L(CU^{-1}) \subseteq L(C)$. Dunque, $L(B) = L(C)$. Viceversa, se $L(B) = L(C)$ allora $B = CT$ per qualche matrice T con valori intere (ogni $b \in B$ deve essere una combinazione lineare intera di elementi di C). Poiché B e C sono entrambi una base di $\mathbb{R}^n$, T è invertibile.

C.V.D.

Data una base $B = \{b_1, \ldots, b_n\}$ di L, il parallelepipedo fondamentale è

$$P(B) = \{b_1 x_1 + \cdots + b_n x_n \mid x_1, \ldots, x_n \in \cancel{[1,0)}\}$$ [0,1]

Il volume di $P(B)$ è $|\det(B)|$. Se C è un'altra base di L allora $C = BU$ dove U è unimodulare. Quindi,

$$\mathrm{vol}(P(C)) = |\det(C)| = |\det(BU)| = |\det(B)\det(U)| = |\det(B)| = \mathrm{vol}(P(B))$$

Definizione 2.18. $\mathrm{vol}(L) = |\det(B)|$ dove B è una qualsiasi base di L.

In particolare, due basi che danno i parallelepipedi fondamentali con volumi diversi definiscono reticoli diversi.

PERCHÉ $\det\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \neq \det\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$

Esempio 2.19. $B = \{(1,-1),(1,1)\}$ e $C = \{(2,3),(1,2)\}$ definiscono reticoli diversi.

$\mathbb{R}^n \to$ VETT. COLONNA

Esempio 2.20. $B = \{(1,-1),(1,1)\}$ e $C = \{(1,0),(1,2)\}$ definiscono reticoli diversi: La somma delle coordinate dei vettori base di B è sempre pari e quindi ogni vettore in $L(B)$ ha questa proprietà. Al contrario, la somma delle coordinate dei vettori base di C è dispari. Osserviamo che $|\det(B)| = |\det(C)|$.

$1-1=0$
$1+1=2$

[1] La base di L è costituita dalle colonne di B, non dalle righe!

Per continuare, ricordiamo che un insieme $S \subset \mathbb{R}^n$ si dice convesso se, dati due punti qualsiasi p e $q \in S$, il segmento di retta tra p e q è anch'esso contenuto in S.

Teorema 2.21. *(Blichfield) Sia $L \subset \mathbb{R}^n$ un reticolo e $S \subseteq \mathbb{R}^n$ un insieme convesso tale che $\mathrm{vol}(S) > \mathrm{vol}(L)$. Allora esistono punti distinti p_1 e $p_2 \in S$ tali che $p_1 - p_2 \in L$.*

Teorema 2.22. *(Minkowski) Se $L \subseteq \mathbb{R}^n$ è un reticolo e S è un insieme di volume maggiore di $2^n \det(L)$ che è convesso e simmetrico rispetto all'origine. Allora S contiene un punto non nullo di L.*

Dimostrazione. Sia $S' = (1/2)S$. Allora $\mathrm{vol}(S') = 2^{-n}\,\mathrm{vol}(S)$ e quindi $\mathrm{vol}(S') > \det(L)$. Per il teorema di Blichfield, esistono punti distinti $p_1, p_2 \in S'$ tali che $p_1 - p_2 \in L$. Perchè $S' = (1/2)S$ ne segue che $2p_1$, $2p_2 \in S$. Ma, $S' = (1/2)S$ è anche simmetrico rispetto all'origine, e quindi $-2p_1$, $-2p_2 \in S$. In quanto tale, S contiene il punto medio

$$p_1 - p_2 = \frac{1}{2}(2p_1 - 2p_2)$$

di $2p_1$ e $-2p_2$, poiché S è convesso.

C.V.D.

Il "volume" $V_n(r)$ della palla

$$B_n(r) = \{\, x = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid |x| \leq r \,\}$$

di raggio r in $\mathbb{R}^n$ è dato dalla formula

PER n DISPARI

$$\underbrace{V_{2n}}_{\text{IN DIMENSIONE } 2n}(r) = \frac{\pi^n}{n} r^{2n}, \qquad V_{2n+1}(r) = \frac{2(k)(4\pi)^n}{(2k+1)} r^{2n+1}$$

Per semplificare la formula successiva, scriviamo $V_n(r) = \underbrace{\gamma_n}_{\text{COSTANTE}} r^n$.

Corollario 2.23. *Dato un reticolo $L \subseteq \mathbb{R}^n$, sia $\lambda_1(L)$ la lunghezza del vettore non nullo più corto in L rispetto alla norma euclidea $|*|$. Allora,*

$$\lambda_1(L) \leq 2(\mathrm{vol}(L)/\gamma_n)^{\frac{1}{n}}$$

Dimostrazione. $r > 2(\mathrm{vol}(L)/\gamma_n)^{\frac{1}{n}} \implies V_n(r) = \gamma_n r^n > \gamma_n 2^n(\mathrm{vol}(L)/\gamma_n) = 2^n\,\mathrm{vol}(L)$ Pertanto, per il teorema di Minkowiski, ogni sfera di questo tipo conterrà un vettore reticolare non nullo, e quindi il vettore più breve di L diverso da zero.

C.V.D.

Nota 2.24. La sfera di raggio r contiene l'ipercubo $[-r/\sqrt{n}, r/\sqrt{n}]$, da cui segue che $\lambda_1(n) \leq \sqrt{n}\,\mathrm{vol}(L)^{\frac{1}{n}}$.

ESERCIZI

- **Esercizio 4.** Verificare che (2.5) è un base di (2.4).
- **Esercizio 5.** Verificare che $\mathbb{Z}^n$ e (2.4) sono diversi.
- **Esercizio 6.** Trova un vettore diverso da zero di lunghezza ($|*|_2$) minima in (2.4).
- **Esercizio 7.** Verificare il teorema (2.15).
- **Esercizio 8.** Verificare il lemma (2.16)

3. Algoritmo di Gauss

Sia $\lfloor x \rceil$ il numero intero più vicino a $x \in \mathbb{R}$ (scegliendo il numero intero pari più vicino se $2x \in \mathbb{Z}$). In dimensione 2, Gauss trovò il seguente algoritmo per trovare il vettore più corto nel reticolo generato da v_1 e v_2, con complessità temporale $O(\log(|v_1| + |v_2|))$.

Algoritmo di Gauss

Sia $L = L(B) \subseteq \mathbb{R}^2$, dove $B = \{v_1, v_2\}$.

- Se $|v_2| < |v_1|$ scambia v_1 e v_2;
- Sia $v_2^* = v_2 - mv_1$ dove $m = \lfloor (v_1, v_2)/|v_1|^2 \rceil$.
- Se $m = 0$ restituire la base $\{v_1, v_2\}$
- In caso contrario, sostituisci v_2 con v_2^* e ripeti i passaggi precedenti.

Il passaggio chiave qui è quello che coinvolge m e v_2^*, che è una forma approssimativa di proiezione ortogonale. Ad ogni passo si riduce la lunghezza dei vettori base.

Lemma 3.1. *Sia $\{v_1, v_2\}$ il risultato dell'algoritmo di Gauss. Allora $\cancel{v_2}$ v_1 è un vettore più breve di L.*

Dimostrazione. Poiché l'algortimo è terminato, sappiamo che:

PERCHÉ L'ALG. LI SCAMBIA SE $|v_2|<|v_1|$

$$|v_1| \leq |v_2|, \qquad \frac{|(v_1, v_2)|}{|v_1|^2} \leq \frac{1}{2} \tag{3.2}$$

PER L·7

Sia $v = c_1v_1 + c_2v_2 \in L$. Allora,

$|v|^2 = (c_1v_1 + c_2v_2, c_1v_1 + c_2v_2)$

$$\begin{aligned} |v|^2 &= c_1^2|v_1|^2 + 2c_1c_2(v_1, v_2) + c_2^2|v_2|^2 \\ &\geq c_1^2|v_1|^2 - 2|c_1c_2||(v_1, v_2)| + c_2^2|v_2|^2 \\ &\geq c_1^2|v_1|^2 - |c_1c_2||v_1|^2 + c_2^2|v_2|^2 \\ &\geq (c_1^2 - |c_1c_2| + c_2^2)|v_1|^2 \end{aligned}$$

METTO VAL. ASS. c_1c_2 E (v_1, v_2) PERCHÉ NON NE CONOSCO I SEGNI POI "−" COSÌ VALE LA DISUG.

dove gli ultimi due passi sono giustificati dall'equazione (3.2). La quantità

$$c_1^2 - |c_1c_2| + c_2^2 = \underbrace{(|c_1| - |c_2|)^2}_{\geq 0} + |c_1c_2| \geq 0 \tag{3.3}$$

è un intero. Pertanto, è sufficiente dimostrare che

$$(c_1, c_2) \neq (0, 0) \implies c_1^2 - |c_1c_2| + c_2^2 > 0$$

Poiché (3.3) è invariante al variare dei segni di c_1 e c_2, possiamo assumere che c_1 e c_2 siano non negativi e verificare invece che

$$c_1^2 - c_1c_2 + c_2^2 \geq 0 \tag{3.4}$$

(esercizio, algebra per le scuole superiori).

C.V.D.

Esempio 3.5.

- $u = (2, 3), v = (5, 8), m = 3$;
- $u = (-1, -1), v = (2, 3), m = \cancel{2}$; -2
- $u = (0, 1), v = (-1, -1), m = -1$;
- $\underbrace{u = (0, 1)}$, $v = (-1, 0)$. VETTORE PIÙ CORTO IN L

Esempio 3.6.

- $u = (5, -3), v = (-3, 5), m = -1$;
- $u = (2, 2), v = (5, -3), m = 0$;

Nelle lezioni successive vedremo come utilizzare il reticolo per costruire crittosistemi. Gli ingredienti essenziali sono:

- Una base di vettori brevi per il reticolo. Questa è la chiave segreta.

- Una base di vettori lunghi per il reticolo, questa è la chiave pubblica.

Per questo motivo, vorremmo essere in grado di costruire matrici unimodulari con valori grandi. Consideriamo la matrice,

$$M = \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \implies \det(M) = x^2 - ny^2 \tag{3.7}$$

dove n è un intero. Allora, M è unimodulare se e sole se $x, y \in \mathbb{Z}$ e $\det(M) = 1$. Questa è l'equazione di Pell,

$$x^2 - ny^2 = 1 \tag{3.8}$$

che è stata considerata in varie forme fin dall'antichità.

Esempio 3.9. Per $n = 313$, $(x_1, y_1) = (32188120829134849, 1819380158564160)$.

Una bella caratteristica dell'equazione (3.8) è che ha un numero infinito di soluzioni $(1, 0), (x_1, y_1), (x_2, y_2), \ldots$ che possono essere trovate utilizzando la relazione di ricorrenza (Brahmaguta):

$$x_{k+1} = x_1 x_k + n y_1 y_k, \qquad y_{k+1} = x_1 y_k + y_1 x_k \tag{3.10}$$

Il problema della prima soluzione fu risolto da Bhāskara intorno al 1150.

Esempio 3.11. Per $n = 13$, $(x_1, y_1) = (649, 180)$. Quindi,

$$M = \begin{pmatrix} x_1 & y_1 \\ ny_1 & x_1 \end{pmatrix} = \begin{pmatrix} 649 & 180 \\ 2340 & 649 \end{pmatrix}$$

Sia L il reticolo generato da $B = \{(5, -3), (-3, 5)\}$. Moltiplicando B per la matrice M si ottiene una nuova base $\{(2705, 9753), (-1047, -3775)\}$ di L. Applicando l'algoritmo di Gauss si trova il vettore più corto di L:

- $u = (-1047, -3775), v = (2705, 9753), m = -3$;
- $u = (-436, -1572), v = (-1047, -3775), m = 2$;
- $u = (-175, -631), v = (-436, -1572), m = 2$;
- $u = (-86, -310), v = (-175, -631), m = 2$;
- $u = (-3, -11), v = (-86, -310), m = 28$;
- $u = (-2, -2), v = (-3, -11), m = 4$;
- $u = (-2, -2), v = (5, -3), m = 0$;

Il seguente lemma è all'origine della relazione di ricorrenza (3.10):

Lemma 3.12. *Se A e B sono matrici $n \times n$ unimodulari, anche AB è unimodulare. Se A è unimodulare lo è anche A^t.*

Dimostrazione. AB è una matrice con valori interi e $\det(AB) = \det(A)\det(B) = \pm 1$. Allo stesso modo, A^t è unimodulare e $\det(A^t) = \det(A) = \pm 1$.

C.V.D.

In particolare, siano

$$A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix}, \qquad B = \begin{pmatrix} u & v \\ nv & u \end{pmatrix}$$

dove $\det(A) = x^2 - ny^2 = 1$ e $\det(B) = u^2 - nv^2 = 1$ allora,

$$AB = \begin{pmatrix} ux + nvy & vx + uy \\ nvx + nuy & ux + nvy \end{pmatrix} = \begin{pmatrix} r & s \\ ns & r \end{pmatrix}$$

Ma, $\det(AB) = \det(A)\det(B) = 1$ e $\det(AB) = r^2 - ns^2$.

In una prossima lezione, dimostreremo il seguente risultato sulla struttura delle matrici intere 2×2 con determinante 1:

Teorema 3.13. *Ogni matrice intera 2×2 di determinante 1 può essere scritta come prodotto finito delle matrici*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

il prodotto vuoto è la matrice identità.

Nota 3.14. La moltiplicazione di matrici non ̀commutativo! La rappresentazione di una matrice come prodotto di S e T non è unica!

L'utilizzo dell'equazione di Pell in questo modo presenta almeno tre problemi:

1. Come abbiamo visto, le soluzioni dell'equazione di Pell hanno una struttura molto articolata che potrebbe facilitare la violazione del nostro schema di crittografia.
2. Non esiste un algoritmo noto in tempo polinomiale per costruire le soluzioni dell'equazione di Pell.
3. Funziona solo per matrici 2×2.

Possiamo superare i problemi 1 e 2 con il seguente algoritmo probabilistico: Genera casualmente due numeri interi grandi A e B. Le tecniche per la dimostrazione del teorema dei numeri primi dimostrano che la probabilità che $\mathrm{mcd}(A, B) = 1$ è $6/\pi^2$. Usando l'algoritmo euclideo, possiamo verificare rapidamente se $\mathrm{mcd}(A, B) = 1$. Per il lemma di Bézout, se $\mathrm{mcd}(A, B) = 1$ allora esistono interi C e D tali che $AD + BC = 1$. Quindi,

$$\begin{pmatrix} A & -B \\ C & D \end{pmatrix}$$

è unimodulare.

Per costruire matrici unimodulari più grandi, utilizziamo la teoria delle forme normali di Hermite:

$$\begin{pmatrix} 1 & 3 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_1 = R_1 - R_2} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

TIPO GAUSS-JORDAN MA PER INTERI

Definizione 3.15. Sia H una matrice $n \times m$ con valori intere. Allora H è in forma normale di Hermite se e sole se

1. H è in forma echelon a righe. (A SCALINI)
2. Ogni pivot di H è un numero intero positivo. (SE CI SONO PIVOT NEG. SI MOLTIPLICA PER -1)
3. Se una colonna contiene un pivot, le voci sopra il pivot sono numeri interi non negativi strettamente inferiori al pivot.

ES.
$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Teorema 3.16. *Sia A una matrice $n \times m$ con valori interi. Allora esiste un'unica matrice H in forma normale di Hermite tale che $H = UA$ per qualche matrice unimodulare U.*

Pertanto, possiamo costruire matrici unimodulari casuali partendo da una matrice intera casuale A e calcolando la forma normale di Hermite $H = UA$. Ciò può essere fatto in tempo polinomiale utilizzando l'algoritmo di riduzione LLL discusso nella prossima sezione.

Possiamo anche usare la forma normale di Hermite per determinare quando $L(B) = L(C)$. A tal fine, supponiamo che le matrici corrispondenti B^t e C^t abbiano la stessa forma normale H:

$$UB^t = H = VC^t$$

$$\det(H) = \underbrace{\det(U)}_{\pm 1}\underbrace{\det(A)}_{\neq 0} \Rightarrow \det(H) \neq 0$$

$$\Rightarrow U = HA^{-1} \text{ SE } \det(A) \neq 0$$

dove U e V sono unimodulari. Allora, $BU^t = CV^t \implies B = CV^t(U^t)^{-1}$. Ma $V^t(U^t)^{-1}$ è unimodulare. Così $L(B) = L(C)$.

SAGEMATH

Esempio 3.17. Costruire a caso una matrice unimodulare:

```
sage: import sage.matrix.matrix_integer_dense_hnf as matrix_integer_dense_hnf
sage: A = random_matrix(ZZ,5,5); A
[ -1   1  -2  -1   4]
[  1   1  -3   0  -8]
[ -3   0  -1  -1  -3]
[  0   4 -14  -3   0]
[  1   3  -2   0  -1]
sage: A.det()
-103
sage: H, U = matrix_integer_dense_hnf.hnf_with_transformation(A)
sage: H
[  1   0   0   0  99]
[  0   1   0   0  76]
[  0   0   1   0  61]
[  0   0   0   1  57]
[  0   0   0   0 103]
sage: U
[-33 -31   3  10   8]
[-27 -25   3   8   7]
[-20 -19   2   6   5]
[-29 -24   4   8   7]
[-37 -34   4  11   9]
sage: U.det()
-1
```

Esempio 3.18. Continuando l'ultima sessione di SAGE, verifichiamo che i due reticoli generati dalle colonne delle matrici B e $D = BU$ sono uguali:

```
sage: B = random_matrix(ZZ,5,5); B
[     0      1    -12      2     -1]
[     1      0      2      0     -2]
[     1     -1     -1     10     -1]
[     0      2      0     17      0]
[    -1  -2905      3     -1     -2]
sage: B.det()
-742797
sage: C = B.transpose()
sage: H, V = matrix_integer_dense_hnf.hnf_with_transformation(C)
sage: H
[      1       0       2       0   99033]
[      0       1       1       0  247598]
[      0       0       3       0   99029]
```

```
[      0       0       0       1  122345]
[      0       0       0       0  247599]
sage: D = B*U
sage: E = transpose(D)
sage: H, V = matrix_integer_dense_hnf.hnf_with_transformation(E)
sage: H
[      1       0       2       0   99033]
[      0       1       1       0  247598]
[      0       0       3       0   99029]
[      0       0       0       1  122345]
[      0       0       0       0  247599]
```

Esempio 3.19. Sostituendo $D = BU$ con una matrice D generata casualmente, vediamo che otteniamo un nuovo reticolo:

```
sage: D = random_matrix(ZZ,5,5); D
[-100   -54   -10     0     3]
[   -1     5     4    -2     2]
[    0    -1    65     4     0]
[   -1     6     1   -19     1]
[    3    -5     0   -35     2]
sage: D.det()
4475460
sage: E = D.transpose()
sage: H, V = matrix_integer_dense_hnf.hnf_with_transformation(E)
sage: H
[        1        0        0        0  1387803]
[        0        1        0        0   353096]
[        0        0        1        0   542109]
[        0        0        0        1  4081321]
[        0        0        0        0  4475460]
```

Esercizi

Esercizio 9. Verificare che (3.4) è uguale zero se e sole se $(c_1, c_2) = (0, 0)$.

Esercizio 10. Verificare che (3.10) genera soluzioni all'equazione (3.8).

Esercizio 11. Scrivere un programma per computer per implementare l'algoritmo di Gauss.

Esercizio 12. Trova il vettore più corto del reticolo con base $B = \{u, v\}$ dove $u = (3, 4)$, $v = (5, 12)$.

Esercizio 13. Trova le soluzioni $(1, 0), (5, 2), (x_2, y_2), (x_3, y_3), (x_4, y_4)$ dell'equazione di Pell per $n = 6$.

4. Algoritmi di Gram-Schmid e Lenstra–Lenstra–Lovász

Se V è uno spazio vettoriale reale (risp. complesso) con un prodotto scalare (risp. prodotto hermitiano) e u è un elemento non nullo di V, allora

$$\text{Proj}_u : V \to V, \qquad \text{Proj}_u(v) = \frac{(v,u)}{(u,u)}u \tag{4.1}$$

è una mappa lineare (rispetto a v, non a u!).

Lemma 4.2. *(Gram-Schmidt) Se $S = \{b_1, \dots, b_n\} \subset V$ è un insieme finito di vettori linearmente indipendenti allora*

$$b_1^* = b_1, \quad b_2^* = b_2 - \text{Proj}_{b_1^*}(b_2), \dots, \quad b_n^* = b_n - \sum_{k=1}^{n-1} \text{Proj}_{b_k^*}(b_n)$$

è un insieme di vettori ortogonali tale che

$$span(b_1, \dots, b_\ell) = span(b_1^*, \dots, b_\ell^*), \quad \ell = 1, \dots, n$$

Proof. Questa è un'induzione sul numero di elementi di S. C.V.D.

Nota 4.3. I vettori $\{b_1^*, \dots, b_n^*\}$ sono solo ortogonali: $(b_i^*, b_j^*) = 0$ a meno che $i = j$. Per ottenere i vettori unitari bisogna dividere ogni b_i^* per la sua norma.

Esempio 4.4. Applicare il processo di Gram-Schmidt alla base $\{1, x, x^2, x^3\}$ di $P_3[x]$ relativa al prodotto scalare

$$(f,g) = \int_{-1}^{1} f(x)g(x)\,dx$$

Per iniziare, si calcola:

$$(x^a, x^b) = \int_{-1}^{1} x^{a+b}\,dx = \frac{x^{a+b+1}}{a+b+1}\bigg|_{-1}^{1} = \begin{cases} \dfrac{2}{a+b+1}, & a+b \text{ pari} \\ 0, & a+b \text{ dispari} \end{cases}$$

Quindi:

$$b_1^* = b_1, \qquad b_2^* = b_2 - \text{Proj}_{b_1^*}(b_2) = x - \frac{(x,1)}{(1,1)}x = x$$

$$b_3^* = b_3 - \text{Proj}_{b_1^*}(b_3) - \text{Proj}_{b_2^*}(b_3) = x^2 - \frac{(x^2,1)}{(1,1)}1 - \frac{(x^2,x)}{(x,x)}x = x^2 - \frac{1}{3}$$

$$b_4^* = b_4 - \text{Proj}_{b_1^*}(b_4) - \text{Proj}_{b_2^*}(b_4) - \text{Proj}_{b_3^*}(b_4) = x^3 - \frac{3}{5}x$$

A causa dei denominatori che compaiono nell'equazione (4.1), non è possibile applicare questo metodo direttamente a un reticolo L. L'algoritmo di Lenstra-Lenstra-Lovasz (solitamente abbreviato LLL)è un analogo dell'algoritmo di Gauss che modifica il processo Gram-Schmid per produrre una base ridotta del reticolo, che consiste di vettori relativamente brevi, quasi ortogonali. (MA NON TROVA UN VETTORE PIÙ CORTO)

Definizione 4.5. Una base $(b_1, \dots, b_d)$ è (δ, η)-LLL-ridotta se:

- Per ogni $i > j$ che abbiamo $|\mu_{ij}| \le \eta$.
- Per ogni $i < d$ abbiamo $\delta |b_i^*|^2 \le |b_{i+1}^* + \mu_{i+1,i} b_i *|^2$

dove $\mu_{ij} = (b_i, b_j^*)/(b_j^*, b_j^*)$ e b_i^* è l'i-esimo vettore di l'ortogonalizzazione di Gram-Schmidt di $(b_1, \dots, b_d)$. I parametri δ e η devono soddisfare $0.25 \le \delta \le 1$ e $0.5 \le \eta < \sqrt{\delta}$.

I parametri predefiniti per SAGE sono $(\delta, \eta) = (0.99, 0.501)$. Molti autori presentano l'algoritmo per $(\delta, \eta) = (3/4, 1/2)$. Lo pseudo-codice per l'algoritmo LLL può essere trovato sulla sua pagina wikipedia.

Esempio 4.6. Le colonne della matrice A sottostante sono una base per il reticolo (2.4) per $n = 3$. Ma l'output di LLL non è un elemento di questo reticolo, poiché la somma delle coordinate della prima colonna è dispari.

```
sage: A = Matrix([[1,0,0],[-1,1,1],[0,-1,1]]); A
[ 1  0  0]
[-1  1  1]
[ 0 -1  1]
sage: A.LLL(delta=0.75, eta=0.5)
[ 1  0  0]
[ 0  1  1]
[ 0 -1  1]
```

Leggi la documentazione. L'algoritmo sta probabilmente usando le righe di A come base invece delle colonne:

```
sage: B = A.transpose(); B
[ 1 -1  0]
[ 0  1 -1]
[ 0  1  1]
sage: B.LLL(delta=0.75, eta=0.5)
[ 1 -1  0]
[ 0  1 -1]
[ 0  1  1]
```

In generale, la trasposizione di matrici fornisce un dizionario tra vettori riga e vettori colonna. In particolare, le matrici trasformano gli spazi riga per la moltiplicazione a destra $A \mapsto MA$ invece che per la moltiplicazione a sinistra $A \mapsto AM$ per gli spazi colonna:

Esempio 4.7.
```
sage: B = Matrix([[1,-1,0],[0,1,-1],[0,1,1]]); B
[ 1 -1  0]
[ 0  1 -1]
[ 0  1  1]
sage: M = random_matrix(ZZ,3,3); M
[ 1 -2 16]
[ 1  2 15]
[ 0  1  3]
sage: M.det()
13
sage: D = B*M; D
[ 0 -4  1]
[ 1  1 12]
[ 1  3 18]
```

```
sage: C = M*B; C
[ 1 13 18]
[ 1 16 13]
[ 0  4  2]
```

In particolare la somma degli elementi della prima riga di D è -3, mentre la somma delle righe di B è sempre pari. Pertanto, il reticolo generato dalle righe di B non può contenere la prima riga di D.

Oltre a trovare la forma normale di Hermite di una matrice, un'altra applicazione dell'algoritmo LLL è la fattorizzazione dei polinomi. In particolare, il problema di determinare se un polinomio con coefficienti razionali ha una radice razionale ha una complessità temporale polinomiale.

ESERCIZI

♉ **Esercizio 14.** Ripeti l'esempio (4.4) usando il prodotto scalare $(f, g) = \int_0^1 f(x)g(x)\,dx$.

ESERCIZIO 4

Verificare che $b_j = e_j - e_{j+1}$ $j=1,\dots,n-1$, $b_n = e_n + e_{n-1}$ è una base di $L = \{(x_1,\dots,x_n) \in \mathbb{Z}^n : 2 \mid (x_1 + \dots + x_n)\}$

$2 \mid (x_1 + \dots + x_n) \Rightarrow x_1 + \dots + x_n = 2k$

$\Rightarrow \underbrace{(x_1 + \dots + x_n)}_{2k} - k\underbrace{(e_n + e_{n-1})}_{2} \in \{\underbrace{y_1 + \dots + y_n = 0}_{\Rightarrow \text{ I VETTORI DI } B \text{ SONO LIN. INDIPENDENTI}}\} \subseteq \mathbb{R}^n\}$

ESERCIZIO 5

Verificare che $\mathbb{Z}^n$ e $L = \{(x_1,\dots,x_n) \in \mathbb{Z}^n : 2 \mid (x_1 + \dots + x_n)\}$ sono diversi

Una base per $\mathbb{Z}^n$ è $B_1 = \{e_1, \dots, e_n\}$

Una base per L è $B_2 = \begin{cases} b_j = e_j - e_{j+1} & j=1,\dots,n-1 \\ b_n = e_n + e_{n-1} \end{cases}$

La somma delle coordinate dei vettori di B_1 è sempre 1, quindi tutti i vettori in $\mathbb{Z}^n(B_1)$ hanno questa proprietà.

Invece, la somma delle coord. dei vett. in B_2 è 0 fino al vettore n-1-esimo, mentre è 2 per il vettore n-esimo.

$\Rightarrow L \neq \mathbb{Z}^n$

[equivalentem. $\overbrace{(1,0,\dots,0)}^{e_1} \in \mathbb{Z}^n$, ma $\notin L$ perché $2 \nmid e_1$]

$\Rightarrow \mathbb{Z}^n \neq L$

<u>ESEMPIO</u> (PER $n=3$)

$B_1 = \{(1,0,0),(0,1,0),(0,0,1)\}$

$B_2 = \{(e_1 - e_2),(e_2 - e_3),(e_3 + e_2)\} = \{(1,-1,0),(0,1,-1),(0,1,1)\}$

Inoltre $|\det(B_1)| \neq |\det(B_2)|$

ESERCIZIO 6

Trova un vettore diverso da zero di lunghezza ($|*|_2$) minima in $L = \{(x_1, \dots, x_n) \in \mathbb{Z}^n : 2 \mid (x_1 + \dots + x_n)\}$

Una base per L è $B = \begin{cases} b_j = e_j - e_{j+1} & j = 1, \dots, n-1 \\ b_n = e_n + e_{n-1} \end{cases}$

Un vettore non nullo di lungh. min. è:

$b_1 = (e_1 - e_2) = (1, -1, 0, \dots, 0)$

ESERCIZIO 7

Dimostrare il seguente teorema:

Sia T una mat. con sole voci intere. Allora T^{-1} esiste ed ha solo voci intere $\iff \det(T) = \pm 1$.

In questo caso si dice che T è una mat. unimodulare.

DIM

MAT $n \times n$
$\downarrow$ CON VOCI INTERE

$$T^{-1} = \frac{1}{\det(T)} \cdot (\quad) \quad , \det(T) = \pm 1$$

$$\det(T^{-1}) = \frac{1}{\det(T)} \quad , T \in \mathbb{Z} \Rightarrow T^{-1} \in \mathbb{Z}$$

ESERCIZIO 8

Dimostrare il lemma:

Sia T una matrice $n \times n$ invertibile con valori interi e B una base di un reticolo $L = L(B)$.

Allora $L(BT) \subseteq L(B)$

DIM

$$L(BT) = B \cdot \overbrace{(T(\mathbb{Z}^n))}^{\subseteq \mathbb{Z}^n} \subseteq \overbrace{B(\mathbb{Z}^n)}^{= \lambda_1 \vec{b}_1 + \dots + \lambda_n \vec{b}_n} = L(B)$$

dove $B = (\vec{b}_1, \dots, \vec{b}_n)$ sono vett. colonna

ESERCIZIO 9

Verificare che $c_1^2 - c_1c_2 + c_2^2 = 0$ se e solo se $(c_1, c_2) = (0,0)$

$$c_1^2 - c_1c_2 + c_2^2 = 0$$

$$\Rightarrow \frac{\overbrace{(c_1-c_2)^2}^{\geq 0} + \overbrace{c_1^2}^{\geq 0} + \overbrace{c_2^2}^{\geq 0}}{2} = 0 \Leftrightarrow (c_1, c_2) = (0,0)$$

ESERCIZIO 10

Verificare che la relazione di ricorrenza

$x_{k+1} = x_1x_k + ny_1y_k$, $y_{k+1} = x_1y_k + y_1x_k$

genera soluzioni per l'eq. di Pell $x^2 - ny^2 = 1$

$(x_1, y_1) = (3, 2)$, $n = 2$

$$\begin{cases} x_2 = x_1x_1 + ny_1y_1 = 9 + 2\cdot 4 = 17 \\ y_2 = x_1y_1 + y_1x_1 = 3\cdot 2 + 2\cdot 3 = 12 \end{cases}$$

$17^2 - 2\cdot 12^2 = 1$ ✓

ESERCIZIO 12

Trova il vettore più corto del reticolo con base $B = \{u, v\}$

dove $u = (3,4)$, $v = (5,12)$

$u = v_1$; $v = v_2$

$|v_2| > |v_1|$

$$v_2^* = v_2 - \left\lfloor \frac{(v_1, v_2)}{|v_1|^2} \right\rceil v_1 = (5,12) - 3(3,4) = (5,12) - (9,12) = (-4,0)$$

$v_2 = v_2^*$

$|v_2| < |v_1| \Rightarrow v_1 = (-4,0)$; $v_2 = (3,4)$

$v_2^* = (3,4) + (-4,0) = (-1,4)$

$v_2 = v_2^*$

$|v_2| > |v_1|$

$v_2^* = (-1,4) - 0$

$\Rightarrow \{v_1, v_2\} = \{(-4,0), (-1,4)\}$

Un vettore più corto per il reticolo con base $\{v_1, v_2\}$ é $(-4,0)$

ESERCIZIO 13

Trova le soluzioni $(1,0), (5,2), (x_2, y_2), (x_3, y_3), (x_4, y_4)$ dell' equazione di Pell per $n=6$

$$\begin{cases} x_{k+1} = x_1 x_k + n y_1 y_k \\ y_{k+1} = x_1 y_k + y_1 x_k \end{cases}$$

$$\begin{cases} x_2 = 25 + 6 \cdot 2 \cdot 2 = 49 \\ y_2 = 10 + 10 = 20 \end{cases}$$

$$\begin{cases} x_3 = 5 \cdot 49 + 6 \cdot 2 \cdot 20 = 485 \\ y_3 = 5 \cdot 20 + 2 \cdot 49 = 198 \end{cases}$$

$$\begin{cases} x_4 = 5 \cdot 485 + 6 \cdot 2 \cdot 198 = 4801 \\ y_4 = 5 \cdot 198 + 2 \cdot 485 = 1960 \end{cases}$$

ESERCIZIO 14

Applicare il processo di Gram-Schmidt alla base $\{1, x, x^2, x^3\}$ di $P_3[x]$ relativa al prodotto scalare

$u_1 \quad u_2 \quad u_3 \quad u_4$

$$(f,g) = \int_0^1 f(x)g(x)\,dx$$

$$v_1 = u_1 = 1$$

$$v_2 = u_2 - \frac{(u_2, v_1)}{(v_1, v_1)} v_1 = x - \frac{1}{2}$$

$$v_3 = x^2 - \frac{(u_3, v_1)}{(v_1, v_1)} v_1 - \frac{(u_3, v_2)}{(v_2, v_2)} v_2 = x^2 - \frac{1}{3} - \frac{1}{\cancel{12}} \cdot \cancel{12} \cdot \left(x - \frac{1}{2}\right) = x^2 - x + \frac{1}{6}$$

$$v_4 = x^3 - \frac{(u_4, v_1)}{(v_1, v_1)} v_1 - \frac{(u_4, v_2)}{(v_2, v_2)} v_2 - \frac{(u_4, v_3)}{(v_3, v_3)} v_3 =$$

$$= x^3 - \frac{1}{4} - \frac{3}{40} \cdot 12 \left(x - \frac{1}{2}\right) - \frac{1}{120} \cdot 180 \left(x^2 - x + \frac{1}{6}\right) =$$

$$= x^3 - \frac{3}{2}x^2 + \frac{3}{5}x - \frac{17}{40}$$

BASE ORTOGONALE: $\{v_1, v_2, v_3, v_4\}$

Lezione 6

1. Relazioni di equivalenza

Una delle nozioni di base in matematica è quella di due oggetti che sono relati. Per esempio, in geometria euclidea, di solito si pensa a due oggetti come equivalenti se sono in una relazione di isometria, cioè una combinazione di:

- Traslazioni
- Rotazioni
- Riflessioni

$T_1 \cong T_2$

Esempio 1.1. Due triangoli T_1 e T_2 sono congruenti se c'è una isometria che muove T_1 su T_2.

A volte si considera un sottoinsieme ristretto di isometrie:

Esempio 1.2. Le linee L_1 e L_2 sono parallele se si può muovere L_1 su L_2 con una traslazione.

A volte si ammettono addizionali trasformazioni:

Esempio 1.3. Due triangoli T_1 e T_2 sono simili se T_1 diventa congruente a T_2 dopo aver scalato le distanze.

La definizione formale è la seguente:

Definizione 1.4. Sia S un insieme. Allora, una relazione R su S è un sottoinsieme del prodotto cartesiano $S \times S$. Dati due elementi $a, b \in S$ diciamo che a è in relazione con b, scritto aRb se $(a, b) \in R$.

Esempio 1.5. $S = \mathbb{Z}$ e aRb se e solo se $a \leq b$.

Esempio 1.6. Sia S un insieme e $\mathcal{P}(S)$ l'insieme di tutti i sottoinsiemi di S. Allora $(A, B) \in R$ se e solo se $A \subseteq B$ è una relazione su $\mathcal{P}(S)$.

Una relazione R su un insieme finito $S = \{s_1, \ldots, s_n\}$ può essere rappresentata dalla matrice Booleana $n \times n$

$$M = (m_{ij}), \qquad m_{ij} = \begin{cases} 1 & (s_1, s_2) \in R \\ 0 & (s_1, s_2) \notin R \end{cases}$$

Equivalentemente, una relazione R può essere rappresentata da un grafo diretto il cui insieme di vertici è l'insieme S con una freccia da s_i a s_j se e solo se $m_{ij} = 1$, ovvero $(s_i, s_j) \in R$. Se M è simmetrica allora

$$(s_i, s_j) \in R \iff (s_j, s_i) \in R$$

In questo caso, possiamo rappresentare R con un grafo non diretto.

Definizione 1.7. Una relazione R su S è simmetrica se $(a, b) \in R \implies (b, a) \in R$ per ogni $(a, b) \in S \times S$.

Esempio 1.8. Esempi (1.1), (1.2) e (1.3) sono relazioni simmetriche. Esempi (1.5) e (1.6) non sono simmetriche: (e.g. $A \subseteq B$ non implica $B \subseteq A$).

A seconda della definizione, un grafo può avere o meno un "self loop" da un vertice allo stesso vertice. Nelle corrispondenza di sopra, un self loop da s_i a s_i corrisponde a $m_{ii} = 1$, che è permesso.

Definizione 1.9. Una relazione R su S è riflessiva se aRa per ogni $a \in S$.

Esempio 1.10. Tutti gli esempi di sopra sono riflessive. $(a \leq a,\ A \subseteq A)$

Esempio 1.11. Il caso più semplice di una relazione che non è riflessiva è di prendere un insieme S arbitrario e definire $R = \emptyset \subset S \times S$. Se R è una relazione riflessiva su un insieme finito allora le entrate sulla diagonale della matrice corrispondente sono tutte uguali a 1.

Esempio 1.12. $S = \{2, 3, ...\}$ e aRb se e solo se a e b sono relativamente primi. Questo esempio è simmetrico perché $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a)$ ma non è riflessivo perché $\mathrm{mcd}(a, a) = a > 1$.

Un'altra proprietà che una relazione può avere è la transitività, che significa:

$$aRb, \quad bRc \implies aRc$$

Se una matrice booleana M rappresenta una relazione transitiva R allora $(M^2)_{ac} \neq 0 \implies M_{ac} \neq 0$.

Esempio 1.13. Tutti gli esempi di sopra tranne (1.12) sono transitivi: $\mathrm{mcd}(2, 3) = 1$ e $\mathrm{mcd}(3, 4) = 1$ ma $\mathrm{mcd}(2, 4) = 2$.

Ciò ci conduce a due classi di relazioni di fondamentale importanza:

Definizione 1.14. Una relazione R su un insieme S è una relazione di equivalenza se e solo se è riflessiva, simmetrica e transitiva.

Definizione 1.15. Una relazione R su un insieme S è un ordine parziale se e solo se è riflessiva, antisimmetrica e transitiva.

Esempio 1.16. Congruenza, parallelismo e similarità (esempi (1.1), (1.2) e (1.6)) sono relazioni di equivalenza. Le relazioni $\leq$ e $\subseteq$ date negli esempi (1.5) e(1.6) sono ordini parziali.

Nota 1.17. Relazioni di equivalenza sono di solito scritte $a \sim b$. Ordini parziali sono di solito scritti $a \leq b$.

Nota 1.18. Sia M una matrice quadrata booleana generata casualmente. In generale, la relazione R associata non è:

- Riflessiva perchè qualche voce diagonale $\cancel{M_{ii} \neq 0}$. $M_{ii} = 0$
- Simmetrica perchè M non è simmetrica.
- Transitiva perchè $(M^2)_{ac} \neq 0 \not\Rightarrow M_{ac} \neq 0$.

Per il resto di questa classe, consideriamo relazioni di equivalenza.

Esempio 1.19. Sia S l'insieme di tutte le matrici $n \times m$. Allora $A \sim B$ se e solo se A è righe-equivalente a B è una relazione di equivalenza.

Esempio 1.20. Sia S l'insieme di tutte le matrici $n \times n$. Allora, $A \sim B$ se e solo se A è simile a B è una relazione di equivalenza (ciò significa che $A = PBP^{-1}$ per qualche matrice $n \times n$ invertibile P).

~~PERCHÉ~~

$A \sim A \quad P = I$

$A \sim B \quad A = PBP^{-1} \Rightarrow P^{-1}AP = B$

$A \sim B,\ B \sim C \Rightarrow A = PBP^{-1},\ B = QCQ^{-1} \Rightarrow A = PQCQ^{-1}P^{-1} =$
$= (PQ)C(PQ)^{-1}$

Definizione 1.21. Sia $\sim$ una relazione di equivalenza su S e $a \in S$. Allora l'insieme

$$[a] = \{b \in S \mid a \sim b\}$$

è chiamato la classe di equivalenza di a. Un elemento $s \in S$ tale che $s \sim a$ si chiama un rappresentante di $[a]$.

Lemma 1.22. *Sia $\sim$ una relazione di equivalenza sull' insieme S. Siano $[a]$ e $[b]$ due classi di equivalenza. Allora o $[a] = [b]$ oppure $[a] \cap [b] = \emptyset$.*

Dimostrazione. Esercizio per lo studente.

C.V.D.

Definizione 1.23. Sia $\sim$ una relazione di equivalenza su S. Allora, $S/\sim$ è l'insieme di tutte le classi di equivalenza di elementi di S. L'insieme $S/\sim$ è chiamato lo spazio quoziente di S rispetto a $\sim$.

Può essere difficile a volte capire lo spazio quoziente. Un metodo per riuscire a capirlo è di provare a costruire una mappa $f : S \to T$ tale che

- $f(S) = T$ (f SURIETTIVA)
- $f(a) = f(b) \iff a \sim b$

Data una tale mappa f, possiamo definire una mappa $g : (S/\sim) \to T$ con la regola

$$g([s]) = f(s) \tag{1.24}$$

Per vedere che (1.24) è ben definita, supponiamo che $s' \sim s$. Allora, $f(s) = f(s')$. In altre parole, la funzione (1.24) dipende solo dalla classe di equivalenza $[s]$ che appare a sinistra e non dal particolare rappresentante s che appare nel lato destro. Poiché f è suriettiva, lo è anche g. Infine, g è iniettiva perchè $g([s]) = g([s'])$ significa che $f(s) = f(s')$ e quindi $s \sim s'$, ovvero $[s] = [s']$.

Esempio 1.25. Tornando all'esempio (1.19), sia S l'insieme di matrici $n \times m$ e T l'insieme di matrici $n \times m$ in forma canonica di riga. Allora, l'eliminazione di Gauss-Jordan da una mappa $f : S \to T$ che è suriettiva. Inoltre, due matrici A e B forma di riga canonica se e solo se sono equivalenti per righe, ovvero $f(A) = f(B)$ se e solo se $A \sim B$. Quindi, la mappa indotta $g : (S/\sim) \to T$ è biettiva.

Esempio 1.26. Sia P l'insieme di tutte le permutazioni di $\{1, \ldots, n\}$. Allora, la relazione $\sim$ on $S = \mathbb{C}^n$ definita da $(z_1, \ldots, z_n) \sim (w_1, \ldots, w_n)$ se e solo se esiste una permutazione $\sigma \in P$ tale che $z_j = w_{\sigma(j)}$ per $j = 1, \ldots, n$ è una relazione di equivalenza su $\mathbb{C}^n$. Sia $T \subseteq \mathbb{C}[\lambda]$ l'insieme dei polinomi monici di grado n nella variabile λ. Allora,

$$f : S \to T, \qquad f(z_1, \ldots, z_n) = (\lambda - z_1)(\lambda - z_2) \cdots (\lambda - z_n)$$

è suriettiva perché un polinomio monico di grado n si fattorizza in un prodotto di questa forma per il teorema fondamentale dell'algebra. Similmente, il valore di $f(z_1, \ldots, z_n)$ è chiaramente invariante sotto permutazioni di $(z_1, \ldots, z_n)$. Infine, poichè la fattorizzazione di un polinomio monico $p(\lambda)$ in fattori lineari della forma $(\lambda - a)$ è unica fino al riordino, ne segue che $f(z) = f(w) \iff z \sim w$.

Esempio 1.27. Sia S l'insieme dei triangoli nel piano e sia $\sim$ la relazione di equivalenza data dalla congruenza. Si fissa una linea L nel piano e sia $\Delta \in S$ un triangolo con lunghezze dei lati $\lambda_1 \leq \lambda_2 \leq \lambda_3$. Se Δ è un triangolo equilatero con lati di lunghezza λ, attraverso un movimento rigido, si ponga un lato di Δ lungo L. Altrimenti:

- Se $\lambda_2 < \lambda_3$, attraverso un movimento rigido, si ponga il lato più lungo di Δ su L e si ponga $\lambda = \lambda_3$.
- Se $\lambda_2 = \lambda_3$, attraverso un movimento rigido, si ponga il lato più corto di Δ su L e si ponga $\lambda = \lambda_1$.

Siano θ_1 e θ_2 gli angoli di Δ corrispondenti ai vertici di Δ su L. Poiché la riflessione rispetto a una linea perpendicolare a L è una congruenza, possiamo assumere che $\theta_1 \leq \theta_2$. Inoltre, $\theta_1 + \theta_2 < \pi$ radianti.

Sia $T = \{(\theta_1, \theta_2, \lambda) \in (0, \pi) \times (0, \pi) \times (0, \infty) \mid \theta_1 \leq \theta_2, \quad \theta_1 + \theta_2 < \pi\}$. Allora, il processo descritto nel paragrafo precedente definisce una mappa $f : S \to T$. Se Δ_1 e Δ_2 sono congruenti, allora $f(\Delta_1) = f(\Delta_2)$. Viceversa, per il criterio di congruenza angolo-lato-angolo, se $f(\Delta_1) = f(\Delta_2)$ allora Δ_1 è congruente a Δ_2. Infine, poiché $\theta_1 + \theta_2 < \pi$, dato un punto in T possiamo costruire un triangolo con queste proprietà: Scegliamo un semipiano H su un lato di L, e disegniamo i raggi in H che cominciano ai dati vertici, formano il dato angolo con L e si muovono nella direzione dell'altro vertice. Poichè $\theta_1 + \theta_2 < \pi$, questi due raggi si intersecano.

Esempio 1.28. Sia S l'insieme delle linee in $\mathbb{R}^2$ e sia $\sim$ la relazione di equivalenza data da traslazioni. Allora, ogni linea $\ell \in S$ è equivalente a un'unica linea L che passa per l'origine $(0, 0)$. Sia C il cerchio unitario dato dall'equazione $x^2 + y^2 = 1$. Allora, una linea L che passa per l'origine interseca C in due punti antipodali (x, y) e $(-x, -y)$. Sia C' il sottoinsieme di C costituito dai punti per cui $y \geq 0$. Allora, a meno che L sia l'asse x, $L \cap C'$ è un singolo punto (x, y) con $y > 0$. Se L è l'asse x allora $L \cap C' = \{(1, 0), (-1, 0)\}$. Sia $T = C' - \{(-1, 0)\}$. Allora, $L \cap T$ è sempre un singolo punto p, da cui si può recuperare L come la linea attraverso l'origine e p. In questo modo, otteniamo una mappa suriettiva $f : S \to T$. Inoltre, per costruzione $f(\ell) = f(\ell')$ se e solo se ℓ è parallela a ℓ', ovvero $\ell \sim \ell'$.

Un modo alternativo di descrivere relazioni di equivalenza è il seguente:

Definizione 1.29. Sia S un insieme. Allora, una partizione di S è una collezione di sottoinsiemi $\mathcal{P}$ di S tale che

- $s \in S \implies \exists A \in \mathcal{P}$ tale che $s \in A$;
- $A, B \in \mathcal{P} \implies A = B$ oppure $A \cap B = \emptyset$.

In altre parole, una partizione di S è una decomposizione di S in una collezione di sottoinsiemi mutualmente disgiunti.

Esempio 1.30. Sia $\mathcal{P}$ una partizione dell'insieme S. Allora,

$$a \sim b \iff \exists P \in \mathcal{P} \text{ tale che } a, b \in P \tag{1.31}$$

è una relazione di equivalenza su S. (Esercizio)

Esempio 1.32. Sia $\sim$ una relazione di equivalenza su S. Allora,

$$\mathcal{P} = \{\, [a] \mid a \in S\} \tag{1.33}$$

è una partizione di $\mathcal{P}$. (Esercizio)

Teorema 1.34. *Si fissi un insieme S. Sia Π l'insieme di tutte le possibili partizioni di S e si denoti con $\mathcal{E}$ l'insieme di tutte le possibili relazioni di equivalenza su S. Si denoti con $f : \Pi \to \mathcal{E}$ la mappa definita dall'equazione* (1.31). *Si denoti con $g : \mathcal{E} \to \Pi$ la mappa definita dall'equazione* (1.33). *Allora, $f \circ g$ e $g \circ f$ sono le mappe identità su $\mathcal{E}$ e Π rispettivamente. In altre parole, f e g sono biezioni inverse.*

$\forall x \in \mathcal{E} \quad id_{\mathcal{E}}(x) = x$

$\forall x \in \Pi \quad id_{\Pi}(x) = x$

dove $id_{\Pi} : \Pi \to \Pi$

Dimostrazione.

FUNZIONE IDENTITÀ:
funzione che associa ad ogni elem. l'elem. stesso

- $f \circ g = \mathrm{Id}_{\mathcal{E}}$: Sia $\mathcal{P} = g(\sim)$ e $R = f(\mathcal{P})$. Dobbiamo dimostrare che $aRb \iff a \sim b$.
  1. Supponiamo che $a \sim b$. Allora, per l'equazione (1.33) esiste $P \in \mathcal{P}$ tale che $a, b \in P$. Allora, per l'equazione (1.31), aRb. In altra parole $a \sim b \implies aRb$.
  2. Viceversa, supponiamo che aRb. Allora per l'equazione (1.31), esiste $P \in \mathcal{P}$ tale che $a, b \in P$. Allora, per l'equazione (1.33), $a \sim b$.
- $g \circ f = \mathrm{Id}_{\mathcal{P}}$: Sia $R = f(\mathcal{P})$ e $\mathcal{P}' = g(R)$. Allora, poiché $\mathcal{P}$ e $\mathcal{P}'$ sono partizioni di S, dato $s \in S$ esiste $A \in \mathcal{P}$ e $B \in \mathcal{P}'$ che contengono s. Dobbiamo dimostrare che $A = B$.
  1. $A \subseteq B$: Supponiamo che $s' \in A$. Allora, per l'equazione (1.31), sRs'. Allora, per l'equazione (1.33), $s' \in B$.
  2. $B \subseteq A$: Supponiamo che $s' \in B$. Then, by equation (1.33), $s'Rs$. Allora, per l'equazione (1.31), $s' \in A$.

C.V.D.

Esercizi

Esercizio 1. Sia $f : X \to Y$ una funzione. Dimostrare che $a \sim b$ se e solo se $f(a) = f(b)$ è una relazione di equivalenza.

Esercizio 2. Ricordiamo che una matrice M di tipo $n \times n$ è ortogonale se $M^t = M^{-1}$. Sia S l'insieme di tutte le matrici reali simmetriche di tipo $n \times n$. Dimostrare che $A \sim B$ se e solo se $A = MBM^{-1}$ per qualche matrice ortogonale M definisce una relazione di equivalenza su S. Dare una descrizione di $S/\sim$ simile all'esempio (1.25).

Esercizio 3. Dimostrare il lemma (1.22).

Esercizio 4. Dare una descrizione geometrica dell'insieme S di linee in $\mathbb{R}^3$ mediante traslazione (vedere l'esempio (1.28)).

Esercizio 5. Dimostrare che (1.31) definisce una relazione di equivalenza.

Esercizio 6. Dimostrare che (1.33) definisce una partizione.

Esercizio 7. Per $n \geq 1$, sia B_n il numero delle possibili partizioni di un insieme con n elementi. Dimostrare per induzione che

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

dove $B_0 = 1$. Suggerimento: Se P è una partizione di $S = \{1, \ldots, n+1\}$ sia $S = A \cup B$ dove $A \in P$ contiene 1.

2. Spazi vettoriali quozienti

La costruzione dello spazio vettoriale quoziente è l'archetipo di molte costruzioni che seguiranno (per esempio gruppi quozienti e anelli quozienti).

La forma più semplice della costruzione è la seguente: Sia $\sim$ la relazione su $\mathbb{R}^n$ definita dalla condizione che $x \sim y$ se e solo se le ultime k coordinate di x e y sono le stesse. Per dimostrare che $\sim$ è una relazione di equivalenza, si possono verificare direttamente gli assiomi oppure sia $\pi : \mathbb{R}^n \to \mathbb{R}^k$ la mappa lineare data dalla proiezione sulle ultime k coordinate. Allora, $\sim$ è semplicemente la relazione di equivalenza associata a π come nell'esercizio (1).

Come primo passo per rendere questa costruzione non dipendente dalle coordinate, sia U il sottospazio di $\mathbb{R}^n$ costituito dai vettori x per cui le ultime k coordinate sono zero, ovvero $U = \ker(\pi)$. Allora,

$$x \sim y \iff x - y \in U$$

Certamente: Se $x \sim y$ allora le ultime k coordinate di x e y sono le stesse, e quindi $x - y \in U$. Viceversa, se $u = x - y \in U$ allora $x = u + y$, dove le ultime k coordinate di u sono zero. Allora, le ultime k coordinate di x e y sono identiche, e quindi $x \sim y$.

Avendo fatto questa osservazione, possiamo ora estendere questa costruzione a spazi vettoriali arbitrari come segue:

Lemma 2.1. *Sia U un sottospazio di V. Allora,*

$$x \sim y \iff x - y \in U$$

è una relazione di equivalenza su V.

Dimostrazione.

- Riflessività: $x \in V \implies x - x = 0 \in U \implies x \sim x$.
- Simmetria: $x, y \in V$ e $x \sim y \implies x - y = u \in U \implies y - x = -u \in U \implies y \sim x$.
- Transitività: $x, y, z \in V$ implica

$$x - z = (x - y) + (y - z) \in U$$

poiché $x \sim y \implies x - y \in U$ e $y \sim z \implies y - z \in U$. Allora, $x \sim z$.

C.V.D.

Lo spazio quoziente di V tramite la relazione di equivalenza (2.1) è di solito scritto V/U. Si può tediosamenta verificare il seguente lemma semplicemente verificando tutti gli assiomi:

Lemma 2.2. *Sia U un sottospazio di V. Allora, V/U è uno spazio vettoriale rispetto alle operazioni:*

- $c[u] \cancel{=} [cu]$; • $c[v] = [cv]$
- $[u] + [u'] \cancel{=} [u + u']$ • $[v] + [v'] = [v + v']$

Dimostrazione. Esercizio per lo studente. Parte dell'esercizio è assicurarsi che queste operazioni sono ben definite: dalla definizione, sembrano dipendenti dalla scelta di un rappresentante della classe di equivalenza.

C.V.D.

Siano U e W sottospazi di uno spazio vettoriale V. Per enunciare il prossimo risultato, ricordiamo che:

- $U + W$ è il più piccolo sottospazio di V che contiene $U \cup W$. Alternativamente, esso consiste di tutti gli elementi in v della forma $v = u + w$ dove $u \in U$ e $w \in W$.
- $V = U \oplus W$ se $U + W = V$ e $U \cap W = \{0\}$. In questo caso, ogni elemento v ha un unica rappresentazione come $v = u + w$ dove $u \in U$ e $w \in W$.

Proposizione 2.3. *Se $V = U \oplus W$ allora V/U è isomorfo a W attraverso la mappa*

$$f([v]) = w, \qquad v = u + w, \quad u \in U, \quad w \in W$$

Dimostrazione. La prima cosa da dimostrare è che f è ben definita. Prima, osserviamo che $V = U + W$ implica che ogni vettore $v \in V$ può essere scritto come una somma

$v = u + w$ dove $u \in U$ e $w \in W$. Supponiamo che $v = u' + w'$ è un'altra rappresentazione di v. Allora,

$$v = u + w = u' + w' \implies u - u' = w - w' \in U \cap W = \{0\} \implies u = u', \quad w = w'$$

Quindi, $f([v]) = w$ è ben definita. La dimostrazione che f è una mappa lineare è lasciata alla lettrice. Chiaramente, $w \in W \implies f([w]) = w$, e quindi $f : V/U \to W$ è suriettiva. Rimane da dimostrare che f è iniettiva. Supponiamo che $f([v]) = 0$ e scriviamo $v = u+w$ con $U \in u$ e $w \in W$. Allora, $f([v]) = w = 0$, e quindi $v \in U$. Quindi, $[v] = 0$.

C.V.D.

Un metodo standard per trovare una decomposizione come somma diretta $V = U \oplus W$ è attraverso operatori di proiezione:

Definizione 2.4. Un endomorfismo $\pi : V \to V$ è chiamato un operatore proiezione se $\pi^2 = \pi$. Se U è un sottospazio di V allora un operatore proiezione su U è un un operatore proiezione tale che $\pi(V) = U$.

Lemma 2.5. *Sia $\pi : V \to V$ un operatore proiezione. Sia $U = \pi(V)$ e $W = \ker(I - \pi)$ dove $I : V \to V$ è la mappa identità . Allora, $V = U \oplus W$.*

Dimostrazione. Sia $v \in V$. Allora, $v = \pi(v) + (I - \pi)(v)$ dove $\pi(v) \in U$ e $(I - \pi(v)) \in W$. Allora, $v \in U + W$ e quindi $V = U + W$. Supponiamo che $t \in U \cap W$. Allora, $t \in U \implies t = \pi(v)$ per qualche $v \in V$. Similmente $t \in W \implies t = (I - \pi)(v')$ per qualche $v' \in V$. Allora,

$$\pi^2 = \pi, \qquad t = \pi(v) \implies \pi(t) = \pi(\pi(v)) = \pi(v) = t$$

D'altra parte,

$$\pi^2 = \pi, \qquad t = (I - \pi(v')) \implies \pi(t) = \pi(v') - \pi^2(v') = 0$$

Allora, $t = 0$.

C.V.D.

Sia $(*, *)$ un prodotto scalare (risp. prodotto hermitiano) su uno spazio vettoriale reale (risp. complesso) V e sia U un sottospazio di V. Allora,

$$U^\perp = \{\, v \in V \mid (v, u) = 0 \, \forall u \in U \,\}$$

è chiamato il complemento ortogonale di U. Continuando, ricordiamo che per il processo di Gram-Schmidt, se U ha dimensione finita, possiamo costruire una base ortonormale (risp. unitaria) $B = \{u_1, \ldots, u_n\}$ tale che $(u_i, u_j) = \delta_{ij}$.

Proposizione 2.6. *Sia $(*, *)$ un prodotto scalare (risp. prodotto hermitiano) su uno spazio vettoriale reale (risp. complesso) V. Sia U un sottospazio di dimensione finita di V con base ortogonale (risp. unitaria) base $B = \{u_1, \ldots, u_n\}$. Allora,*

$$\pi(v) = \sum_{j=1}^{n} (v, u_j) u_j$$

è un operatore proiezione con immagine U.

Dimostrazione.

- $\pi(V) = U$: Per definizione, $v \in V \implies \pi(v)$ è una combinazione lineare dei vettori della base B, e quindi $\pi(V) \subseteq U$. Viceversa, poiché B è una base ortonormale (risp. unitaria) di U,

$$\pi(u_k) = \sum_{j=1}^{n} (u_k, u_j) u_j = u_k \tag{2.7}$$

  e quindi $u = \sum_{j=1}^{n} c_j u_j \in U \implies \pi(u) = u$. Ciò implica che $U \subseteq \pi(V)$, e quindi $\pi(V) = U$.
- Si scriva $\pi(v) = \sum_{j=1}^{n} c_j u_j$. Allora, (2.7) implica che

$$\begin{aligned}\pi^2(v) - \pi(v) &= \pi\left(\sum_{j=1}^{n} c_j u_j\right) - \sum_{j=1}^{n} c_j u_j \\ &= \sum_{j=1}^{n} c_j \pi(u_j) - \sum_{j=1}^{n} c_j u_j = \sum_{j=1}^{n} c_j u_j - \sum_{j=1}^{n} c_j u_j = 0\end{aligned}$$

C.V.D.

ESERCIZIO 1

Sia $f: X \to Y$ una funzione.
Dimostrare che $a \sim b \iff f(a) = f(b)$ è una rel. di equiv.

- $f(a) = f(a)$ ✓
- $f(a) = f(b) \Rightarrow f(b) = f(a)$ ✓
- $f(a) = f(b),\ f(b) = f(c) \Rightarrow f(a) = f(c)$ ✓

ESERCIZIO 2

Ricordiamo che una matrice M $n \times n$ è ortogonale se $M^T = M^{-1}$.
Sia S l'insieme di tutte le mat. reali simmetriche $n \times n$. Dimostrare che $A \sim B \iff A = MBM^{-1}$ per una qualche mat. ortogonale M definisce una relazione di equiv. su S.
Dare una descrizione di $S/\sim$.

- $A \sim A \Rightarrow P = I$ rel. riflessiva ✓
- $A \sim B \Rightarrow A = PBP^{-1} \Rightarrow P^{-1}AP = B$ rel. simmetrica ✓
- $A \sim B,\ B \sim C \Rightarrow A = PBP^{-1},\ B = QCQ^{-1} \Rightarrow A = PQCQ^{-1}P^{-1} =$
$= (PQ)C(PQ)^{-1}$
rel. transitiva ✓

$A \sim B \iff A$ è simile a B (cioè $A = MBM^{-1}$)
$S = \{$mat. reali simmetriche $n \times n\}$
Per il th spettrale, poiché A è simmetrica, A è simile a una matrice diagonale $D = MAM^{-1}$ unica.
Dunque:
$S/\sim = \{$mat. della forma di $D\}$

ESERCIZIO 3

Dimostrare il seguente lemma:

Sia $\sim$ una relazione di equiv. sull' insieme S.

Siano $[a]$ e $[b]$ due classi di equiv.

Allora $[a]=[b]$ oppure $[a]\cap[b]=\emptyset$

- $a,b \in S$, $aRb \Rightarrow [a]=[b]$

  Sia $x \in [a]$, allora per la def. di classe di equiv. aRx

  R rel. di equiv. $\Rightarrow R$ simmetrica $\Rightarrow aRb = bRa$

  " " " " $\Rightarrow R$ transitiva $\Rightarrow bRa, aRx \Rightarrow bRx$

  $\Rightarrow x \in [b]$

  Sia $x \in [b]$, allora bRx.

  $\Rightarrow bRa = aRb$

  $\Rightarrow aRb, bRx \Rightarrow aRx$

  $\Rightarrow x \in [a]$

  $x \in [a] \Leftrightarrow x \in [b] \Rightarrow [a]=[b]$

- Supponiamo $[a]\cap[b] \neq \emptyset$.

  Allora $\exists x \in [a]\cap[b]$, quindi aRx, bRx

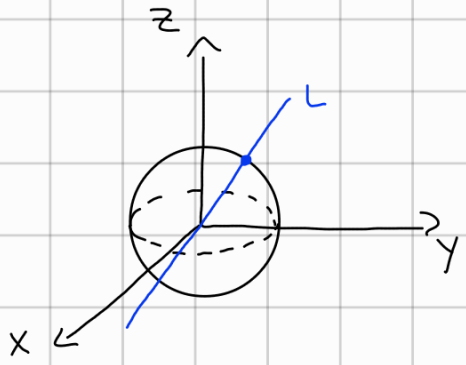
  $\Rightarrow bRx = xRb$

  $\Rightarrow aRx, xRb \Rightarrow aRb$

  $\Rightarrow [a]=[b]$ e $[a]\cap[b]$ sono equivalenti

ESERCIZIO 4

Fornire una descrizione geometrica dell'insieme S di linee in $\mathbb{R}^3$ mediante traslazione.



Sia $x^2+y^2+z^2=1$ la sfera di raggio unitario
Per $z \geq 0$ la retta L interseca la sfera in un solo pto.
Per $z=0$ siamo in $\mathbb{R}^2$ e ci possiamo ricondurre al caso dell'esempio 1.28.

ESERCIZIO 5

Dimostrare che $a \sim b \iff \exists P \in \mathcal{P}$ t.c. $a,b \in P$ definisce una relazione di equivalenza.

- $S = \bigcup_{A \in \mathcal{P}} A \Rightarrow a \sim a$ perché $\exists A$ t.c. $a \in A$

- $a \sim b \Rightarrow a,b \in A \Rightarrow b,a \in A \Rightarrow b \sim a$
- $a \sim b,\ b \sim c$

  $a,b \in P_1,\ b,c \in P_2$

  $\Rightarrow b \in P_1 \cap P_2$

  $P_1 \cap P_2 \neq \emptyset \Rightarrow P_1 = P_2 \Rightarrow a,c \in P_1 = P_2 \Rightarrow a \sim c$

ESERCIZIO 6

Dimostrare che $P = \{[a] : a \in S\}$ definisce una partizione.

- $S = \cup [a]$ (cioè S è l'unione di tutte le classi di equiv.)
  $s \in S \Rightarrow s \sim s \Rightarrow s \in [s]$

- $[a] \cap [b] = \begin{cases} [a] = [b] \\ \emptyset \end{cases}$

  $c \in [a] \cap [b] \Rightarrow a \sim c,\ b \sim c$
  $\Downarrow$ PER SIMMETRIA
  $c \sim b$

  $a \sim c,\ c \sim b \Rightarrow a \sim b \Rightarrow [a] = [b]$

ESERCIZIO 7

Per $n \geq 1$, sia B_n il numero delle possibili partizioni di un insieme con n elementi.
Dim. per induzione che $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$, dove $B_0 = 1$.

(Se P è una partizione di $S = \{1, \dots, n+1\}$, sia $S = A \cup B$ dove $A \in P$ contiene 1)

P = partizione di $\{1, \dots, n+1\}$
$\Rightarrow \exists A \in P$ t.c. $1 \in A$,
$\Rightarrow P = \{A\} \cup P'$, P' = partizione di $\{1, \dots, n+1\} - A$

$|A| = 1 \Rightarrow A = \{1\}$, P' = partiz. di $\{2, \dots, n+1\}$
$\Rightarrow$ # possibili partizioni per $P' = B_n$

$|A| = 2 \Rightarrow A = \{1, k_1\}$, $k_1 \in \{2, \dots, n+1\}$
$\Rightarrow$ # possibili partiz. per $A = \binom{n}{1} = n$
$\Rightarrow$ # " " " $P' = B_{n-1}$

$|A| = 3 \Rightarrow A = \{1, k_1, k_2\}$, $k_1, k_2 \in \{2, \dots, n+1\}$

$\Rightarrow$ # possibili partiz. per $A = \binom{n}{2}$

$\Rightarrow$ # " " " $P' = B_{n-2}$

$\vdots$

$$|P| = \overbrace{\binom{n}{0}}^{1} B_n + \binom{n}{1} B_{n-1} + \binom{n}{2} B_{n-2} + \dots + \binom{n}{n} B_0 = \sum_{k=0}^{n} \binom{n}{k} B_k$$

$A = \{1, \dots, n+1\}$

$P' =$ partiz. di $\{\emptyset\}$

$|A| = 1, \dots, n+1$

<u>ESEMPIO:</u>

$S = \{1, 2, 3\}$, $k = 3$

$A = \{1\}$, rimangono $\{2, 3\}$, $B_2 = 2$

$A = \{1, 2\}$, rimane $\{3\}$, $B_1 = 1$

$A = \{1, 3\}$, " $\{2\}$, $B_1 = 1$

$A = \{1, 2, 3\}$ " $\{\emptyset\}$, $B_0 = 1$

$$B_3 = \sum_{k=0}^{2} \binom{2}{k} B_k = \binom{2}{0} B_0 + \binom{2}{1} B_1 + \binom{2}{2} B_2 =$$

$$= 1 \cdot 1 + 2 \cdot 1 + 1 \cdot 2 = 5 =$$

= # di partizioni che posso ottenere da un insieme di 3 elementi

Infatti, le 5 possibili partizioni sono:

$\{\{1\}, \{2\}, \{3\}\}$

$\{\{1\}, \{2, 3\}\}$

$\{\{1, 2\}, \{3, 4\}\}$

$\{\{1, 3\}, \{2\}\}$

$\{1, 2, 3\}$

Lezione 7

1. Aritmetica modulare

Questo è un trattamento rapido del materiale nelle sezioni 5 e 6 di "A concrete introduction to higher algebra" by L. Childs.

Si fissi un intero $n > 1$. Siano a e b interi. Allora, diciamo che $a \equiv b \mod n$ se e solo se n divide $a - b$.

Lemma 1.1. *$\equiv \mod n$ è una relazione di equivalenza su $\mathbb{Z}$.*

Dimostrazione. Per dimostrare che $\equiv \mod n$ è una relazione di equivalenza dobbiamo verificare:

- Riflessività: $a \equiv a \mod n$ perché $a - a = 0$ e $n|0$.
- Simmetria: $a \equiv b \mod n \implies b \equiv a \mod n$ perché $n|(a-b) \implies n|(b-a)$.
- Transitività: $a \equiv b \implies n|(a-b)$. Allo stesso modo $b \equiv c \implies n|(b-c)$. Allora, $n|(a-c)$ perché $a - c = (a-b) + (b-c)$. Quindi $a \equiv c \mod n$.

C.V.D.

Supponiamo adesso che $a, b \in \{0, 1 \ldots, n-1\}$ e $a \equiv b \mod n$. Scambiando a e b se necessario, assumiamo che $a \geq b$. Allora,

$$a \equiv b \mod n \implies n|(a-b) \in \{0, 1, \ldots, n-1\}$$

e quindi $a - b = 0$, ovvero $a = b$. Sia

$$T = \{\, [0], \ldots, [n-1] \,\} \tag{1.2}$$

Per il teorema della divisione, dato $a \in \mathbb{Z}$ esiste un'unica coppia di interi q e r tali che

$$a = qn + r, \qquad 0 \leq r < n$$

Definiamo $f : \mathbb{Z} \to T$ tramite $f(a) = [a]$. Allora,

- $f(\mathbb{Z}) = T$;
- $f(a) = f(b) \iff a \equiv b \mod n$.

La proposizione $f(\mathbb{Z}) = T$ è vera perché $j \in \{0, \ldots, n-1\} \implies f(j) = [j]$. Supponiamo adesso che $f(a) = f(b) = [r]$. Allora, $a = nq + r$ e $b = nq' + r$ per interi q e q' e quindi

$$a - b = n(q - q') \implies a \equiv b \mod n$$

Viceversa, $a \equiv b \mod n \implies n|(a-b)$ e quindi c'è un intero c tale che $a - b = nc$. Sia $b = nq + r$ con $0 \leq r < n$. Allora,

$$a = a - b + b = nc + nq + r = n(c+q) + r$$

e quindi $f(a) = f(b)$. Insomma, abbiamo dimostrato che:

Lemma 1.3. *Sia $\mathbb{Z}_n$ lo spazio quoziente di $\mathbb{Z}$ rispetto a ($\equiv \mod n$). Sia T l'insieme* (1.2)*. Allora, $f : \mathbb{Z} \to T$ definita da $f(a) = [a]$ definisce una bigezione da $\mathbb{Z}_n$ a T.*

Adesso, definiamo addizione e moltiplicazione su $\mathbb{Z}_n$ usando T.

Definizione 1.4. Sia $[a], [b] \in T$. Allora,

- $[a] + [b] = [a + b]$.
- $[a][b] = [ab]$.

Nota 1.5. Dati $a, b \in \{0, 1, \ldots, n-1\}$, $a+b$ (risp. ab) potrebbe essere maggiore di n. In questo caso, dobbiamo scrivere $a+b = qn+r$ (risp. $ab = qn+r$) dove $0 \leq r < n$ e definiamo $[a+b] = [r]$ (risp. $[ab] = [r]$).

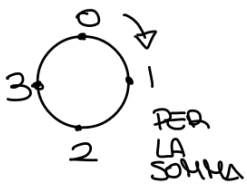
Esempio 1.6. Addizione e moltiplicazione modulo 2:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

,

$*$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Esempio 1.7. Addizione e moltiplicazione modulo 4:



$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

,

$*$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Esempio 1.8. Addizione e moltiplicazione modulo 5:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

,

$*$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

$x^2 \not\equiv 2 \mod 5$ PERCHÉ 2 NON È UN QUADRATO (VEDI DIAGONALE PRINC.) QUINDI $x^2 \equiv 2 \mod 5$ NON HA SOL

PERCHÉ $16 \mod 5 = 1$

La cosa buona di questa definizione è che è definita senza ambiguità. Il lato negativo è che ci forza a usare sempre elementi di T per i nostri calcoli. Il lemma successivo dimostra che infatti possiamo usare ogni scelta di rappresentativi performare addizione e moltiplicazione modulo n.

Lemma 1.9. *Supponiamo che* $a \equiv a' \mod n$ *e* $b \equiv b' \mod n$. *Allora,* $a+b \equiv a'+b' \mod n$ *e* $ab \equiv a'b' \mod n$.

Dimostrazione. Esercizio per lo studente.

C.V.D.

In particolare, ne segue che tutte le proprietà standard di addizione e moltiplicazione per interi elencate nella Table1 valgono per addizione e moltiplicazione modulo n:

TABLE 1. Proprietà di Addizione e Moltiplicazione, a, b, $c \in \mathbb{Z}$

	Addizione	Moltiplicazione
Chiusura	$a+b \in \mathbb{Z}$	$a*b \in \mathbb{Z}$
Associatività	$a+(b+c) = (a+b)+c$	$(ab)c = a(bc)$
Commutatività	$a+b = b+a$	$a*b = b*a$
Elementi Identità 1, 0	$a+0 = a$	$a*1 = a$
Esistenza di Inversi	$a+(-a) = 0$	? (DI SOLITO NO)
Proprietà distributiva	$a*(b+c) = a*b+a*c$	

Esempio 1.10. Sia n un intero. Allora, n è divisibile per 4 se e solo se le ultime due cifre (base 10) del n sono divisibili per 4. Per vedere questo, notiamo che $4|100$. Quindi,

$$n = (a_m 10^m + \cdots + a_2 10^2) + a_1 10 + a_0$$

da cui lo si vede $n \equiv a_1 10 + a_0 \mod 4$.

Teorema 1.11. *(Reciprocità Quadratica, Gauss). Siano p e q distinti numeri primi.* DISPARI

- *Se $q \equiv 1 \mod 4$ allora $x^2 \equiv p \mod q$ è solvibile se e solo se $x^2 \equiv q \mod p$ è solvibile.*
- *Se $q \equiv 3 \mod 4$ e $p \equiv 3 \mod 4$ allora la congruenza $x^2 \equiv p \mod q$ è solvibile se e solo se $x^2 \equiv -q \mod p$ è solvibile.*

Dimostrazione. La dimostrazione è omessa.

C.V.D.

Esempio 1.12. $x^2 \equiv p \mod q$, $y^2 \equiv q \mod p$

- $(p, q) = (3, 13)$: $4^2 = 16 \equiv 3 \mod 13$, $1^2 = 1 \equiv 13 \mod 3$.
- $(p, q) = (2, 17)$: $6^2 = 36 \equiv 2 \mod 17$, $1^2 = 1 \equiv 17 \mod 2$.
- $(p, q) = (5, 29)$: $11^2 \overset{121}{=} 1 \equiv 5 \mod 29$, $2^2 = 4 \equiv 29 \mod 5$.
- $(p, q) = (7, 29)$: $6^2 = 36 \equiv 7 \mod 29$, $1^2 = 1 \equiv 28 \mod 7$.

Esempio 1.13. $x^2 \equiv p \mod q$, $y^2 \equiv -q \mod p$

- $(p, q) = (3, 11)$: $5^2 = 25 \equiv 3 \mod 11$, $1^2 = 1 \equiv -11 \mod 3$.
- $(p, q) = (7, 19)$: $8^2 = 64 \equiv 7 \mod 19$, $3^2 = 9 \equiv -19 \mod 7$.
- $(p, q) = (11, 19)$: $7^2 = 49 \equiv 11 \mod 19$, $5^2 = 25 \equiv -19 \mod 11$.
- $(p, q) = (3, 23)$: $7^2 = 49 \equiv 3 \mod 23$, $1^2 = 1 \equiv -23 \mod 3$.

Proposizione 1.14. *(Primo supplemento alla reciprocità quadratica) La congruenza $x^2 \equiv -1 \mod p$ ha soluzione se e solo se p è congruente a 1 mod 4.*

Possiamo anche considerare sistemi lineari $(A|b)$ usando aritmetica modulare modulo n. Per la regola di Cramer, ci aspetteremmo che se A è una matrice quadrata, allora

$$Ax \equiv b \mod n$$

ha una soluzione purché possiamo risolvere l'equazione $[\delta][\det(A)] \equiv 1 \mod n$.

Esempio 1.15. Sia

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix}$$

allora, $\det(A) = 2$ e

$$A^{-1} = \frac{1}{2} \begin{pmatrix} 6 & -6 & 2 \\ -5 & 8 & -3 \\ 1 & -2 & 1 \end{pmatrix}$$

Poiché $[2][3] \equiv [1] \mod 5$ ne segue che

$$A^{-1} \mod 5 = [3] \begin{pmatrix} [1] & [4] & [2] \\ [0] & [3] & [2] \\ [1] & [3] & [1] \end{pmatrix} = \begin{pmatrix} [3] & [2] & [1] \\ [0] & [4] & [1] \\ [3] & [4] & [3] \end{pmatrix}$$

D'altra parte, non c'è una soluzione di $[2][c] \equiv [1] \mod 4$, quindi proviamo riduzione di righe:

$$(A|b) \equiv \left(\begin{array}{ccc|c} \overbrace{\begin{matrix}[1] & [1] & [1]\\ [1] & [2] & [0]\\ [1] & [3] & [1]\end{matrix}}^{A \text{ mod } 4} & \begin{matrix}[b_1]\\ [b_2]\\ [b_3]\end{matrix}\end{array}\right) \equiv \left(\begin{array}{ccc|c} [1] & [1] & [1] & [b_1]\\ [0] & [1] & [3] & [b_2-b_1]\\ [0] & [2] & [0] & [b_3-b_1]\end{array}\right) \equiv \left(\begin{array}{ccc|c} [1] & [1] & [1] & [b_1]\\ [0] & [1] & [3] & [b_2-b_1]\\ [0] & [0] & [2] & [b_1-2b_2+b_3]\end{array}\right)$$

Allora, se x è il vettore colonna corrispondente a (x_1, x_2, x_3) dobbiamo poter risolvere $[2x_3] \equiv [b_1 - 2b_2 + b_3] \mod 4$ per essere in grado di risolvere $Ax = b \mod 4$. Per esempio, se $(b_1, b_2, b_3) = (1, 0, 0)$ allora $Ax = b$ non ha una soluzione $\mod 4$.

Esercizi

Esercizio 1. Costruire le tavole di addizione e moltiplicazione modulo 3.

Esercizio 2. Verificare i seguenti esempi di reciprocità quadratica:

- $(p, q) = (13, 29)$: $10^2 \equiv 13 \mod 29$, $4^2 \equiv 29 \mod 13$.
- $(p, q) = (23, 29)$: $9^2 \equiv 23 \mod 29$, $11^2 \equiv 29 \mod 23$.
- $(p, q) = (3, 15)$: $15^2 \equiv 3 \mod 37$, $1^2 \equiv 37 \mod 3$.

Esercizio 3. Verificare i seguenti esempi di reciprocità quadratica:

- $(p, q) = (7, 31)$: $10^2 \equiv 7 \mod 31$, $2^2 \equiv -31 \mod 7$.
- $(p, q) = (19, 31)$: $9^2 \equiv 19 \mod 31$, $8^2 \equiv -31 \mod 19$.
- $(p, q) = (11, 43)$: $21^2 \equiv 11 \mod 43$, $1^2 \equiv -43 \mod 11$.

Esercizio 4. Sia

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

allora, $\det(A) = 360$. Qual'è il minimo numero primo p per cui ti aspetti che A^{-1} esiste $\mod p$? Calcolare $A^{-1} \mod p$.

Esercizio 5. Modificare l'esempio (1.10) per dimostrare che l'intero n è divisibile per 9 se e solo se la somma delle cifre di n è divisibile per 9.

Esercizio 6. Dimostrare il lemma (1.9).

2. Anelli Commutativi Con Identità

Definizione 2.1. Un anello commutativo con identità è un insieme R con due mappe $+ : R \times R \to R$ e $* : R \times R \to R$ che soddisfano le proprietà elencate nella Tavola (1) purché $\underbrace{1 \neq 0}$. CIOÉ L'ELEM. IDENTITÁ DELLA MOLT. DEVE ESSERE ≠ DALL' ELEM. IDENTITÁ DELL' ADDIZ.

ALTRIMENTI, SE $1 = 0$ AVREMMO UN ANELLO CON UN SOLO ELEM.: ZERO

INFATTI $x \cdot 1 = x \cdot 0 \Rightarrow x = 0$

Esempio 2.2. Sia R un anello commutativo con identità. Allora, possiamo definire l'anello polinomiale $R[x]$ come l'insieme di elementi della forma

$$f(x) = a_n x^n + \cdots + a_0, \qquad a_n, \ldots, a_0 \in R$$

rispetto alle regole usuali di addizione e moltiplicazione di polinomi. Un polinomio $f \in R[x]$ definisce una funzione $\mathrm{ev}(f) : R \to R$ data dalla valutazione. Si noti comunque che se R è un insieme finito allora l'insieme di tutte le funzioni da R a R è finito. In contrasto, R ha almeno due elementi, ovvero 0 e 1, quindi $R[x]$ è un insieme infinito. Per esempio, se p è un numero primo allora $f(x) = x^p - x$ è un elemento non nullo di $\mathbb{Z}_p[x]$. Per il piccolo teorema di Fermat, $a \in \mathbb{Z}_p \implies f(a) = 0$.

Esempio 2.3. Se $(R, +, *)$ e $(S, +, *)$ sono anelli commutativi con identità allora $R \times S$ è un anello commutativo con identità rispetto all'addizione e moltiplicazione sulle componenti:

$$(r_1, s_1) + (r_2, s) = (r_1 + r_2, s_1 + s_2), \qquad (r_1, s_1) * (r_2, s_2) = (r_1 r_2, s_1 s_2)$$

L'elemento identità per l'addizione è $(0_R, 0_S)$. L'elemento identità per la moltiplicazione è $(1_R, 1_S)$. La verifica degli assiomi di un anello è lasciata alla lettrice.

Esempio 2.4. Siano m e n interi maggiori di 1. Dato $x \in \mathbb{Z}$, sia $[x]_m$, $[x]_n$ e $[x]_{mn}$ le classi di equivalenza di x in $\mathbb{Z}_m$, $\mathbb{Z}_n$ e $\mathbb{Z}_{mn}$ rispettivamente. Allora,

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \qquad f([x]_{mn}) = ([x]_m, [x]_n) \tag{2.5}$$

è una mappa ben definita tale che (SIMILE A MOLT. SCALARE PER MATRICI LINEARI)

$$f([x+y]_{mn}) = f([x]_{mn}) + f([y]_{mn}) \qquad f([x]_{mn}[y]_{mn}) = f([x]_{mn}) * f([y_{mn}]) \tag{2.6}$$

Per dimostrare che è ben definita, supponiamo che $x \equiv x' \mod mn$. Allora, $x' = x + \alpha mn$ per qualche intero α, e quindi $x' \equiv x \mod m$ e $x' \equiv x \mod n$. Similmente, se $y \equiv y' \mod mn$ allora esiste un intero β tale che $y' = y + \beta mn$. L'equazione (2.6) ora segue da calcoli diretti.

Una grande differenza fra $\mathbb{Z}$ e $\mathbb{Z}_n$ è la possibile esistenza di divisori di zero: Se a e b sono interi e $ab = 0$ allora $a = 0$ o $b = 0$. In contrasto se n non è un primo e $n = ab$ allora $[a][b] = [0]$ in $\mathbb{Z}_n$.

DOMINIO DI INTEGRITÀ

Definizione 2.7. Un ~~dominio integrale~~ è un anello commutativo con identità tale che $a * b = 0 \implies a = 0$ o $b = 0$.

Esempio 2.8. $\mathbb{Q}[x]$ è un dominio integrale rispetto alle operazioni usuali di addizione e moltiplicazione polinomiali. Se R e S sono anelli commutativi con identità, allora $R \times S$ non è mai un dominio integrale perché $(1_R, 0_s) * (0_R, 1_S) = (0_R, 0_S)$.

Strettamente correlata con la proprietà di essere un dominio integrale è l'esistenza di inversi moltiplicativi:

Definizione 2.9. Sia $(R, +, *)$ un anello commutativo con identità. Allora, un elemento non nullo $u \in R$ è una unità se esiste $v \in R$ tale che $uv = 1$.

Le uniche unità in $\mathbb{Z}$ sono ± 1. Invece in $\mathbb{Z}_n$ abbiamo:

Lemma 2.10. *$[a] \in \mathbb{Z}_n$ ha un inverso moltiplicativo se solo se* $\mathrm{mcd}(a, n) = 1$.

Dimostrazione. Supponiamo che $[a][b] = 1$. Allora, esiste un numero intero c tale che $ab = 1 + cn$, il che implica $ab + (-c)n = 1$ e quindi $\mathrm{mcd}(a, n) = 1$. Viceversa, se $\mathrm{mcd}(a, n) = 1$, allora esistono interi b e c tali che $ab + cn = 1$ e quindi $[a][b] = [1]$.

C.V.D.

Corollary 2.11. *Sia p un numero primo. Allora, ogni elemento non nullo in $\mathbb{Z}_p$ ha un inverso moltiplicativo.*

Dimostrazione. Se $a \in \{1, \ldots, p-1\}$ e p è primo allora $\mathrm{mcd}(a, p) = 1$.

C.V.D.

Definizione 2.12. La funzione ϕ sugli interi positivi definita dalla regola che $\phi(1) = 1$ e $\phi(n)$ è il numero di unità in $\mathbb{Z}_n$ altrimenti è chiamata la funzione ϕ di Eulero.

Esempio 2.13. Se p è un numero primo allora $\phi(p) = p - 1$ per il Corollario (2.11). Più generalmente, se r è un intero positivo allora

$$\phi(p^r) = p^{r-1}(p-1) = p^r\left(1 - \frac{1}{p}\right)$$

Per dimostrare questo, notiamo che $\mathrm{mcd}(a, p^r) = 1$ a meno che a sia un multiplo di p. Il numero di tali multipli in $\{0, \ldots, p^r - 1\}$ è p^{r-1}.

Lemma 2.14. *Siano A e B insiemi finiti della stessa cardinalità. Allora, le seguenti sono equivalenti:*

- *$f : A \to B$ è iniettiva.*
- *$f : A \to B$ è suriettiva.*

Dimostrazione. Intuitivamente, questo lemma è ovvio: Se $f : A \to B$ è una iniezione, allora $|f(A)| = |A|$. Allora, $|f(A)| = |A| = |B|$ e quindi f è suriettiva. Similmente, per mostrare che se $f : A \to B$ è suriettiva allora $f : A \to B$ è iniettiva, consideriamo il contrapposto: Se $f : A \to B$ non è iniettiva, allora $f : A \to B$ non è suriettiva. Chiaramente, se $f : A \to B$ non è iniettiva, allora $|f(A)| < |A| = |B|$, e quindi f non è suriettiva. Il problema con questo approccio è che si devono definire attentamente le nozioni di insieme finito e cardinalità per renderli rigorosi.

C.V.D.

Supponiamo adesso che $\mathrm{mcd}(m, n) = 1$ dove m, $n > 1$. Allora, dati interi a e b esiste un intero c tale che

$$c \equiv a \mod m, \qquad c \equiv b \mod n \tag{2.15}$$

Per mostrare ciò, ricordiamo che per il teorema di Bézout, esistono interi u e v tali che

$$mu + nv = \mathrm{mcd}(m, n) = 1 \tag{2.16}$$

Sia $c = anv + bmu$. Allora,

$$\begin{aligned} c &= a(1 - mu) + bmu = a + mu(b - a) \equiv a \mod m \\ c &= anv + b(1 - nv) = nv(a - b) + b \equiv b \mod n \end{aligned} \tag{2.17}$$

Corollary 2.18. *Supponiamo che m, n siano interi > 1 tali che $\mathrm{mcd}(m, n) = 1$. Allora, la mappa (funzione) $f([x]_{mn}) = ([x]_m, [x]_n)$ da $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ considerata sopra [vedi (2.5)] è una bigezione.*

Dimostrazione. La suriettività di f segue dall'equazione (2.15). Poiché $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ hanno mn elementi, ne segue che f è iniettiva, e quindi f è una bigezione.

C.V.D.

Proposizione 2.19. *Supponiamo che m, n sono interi maggiori di uno tali che $\mathrm{mcd}(m, n) = 1$. Sia A l'insieme di unità in $\mathbb{Z}_m$, B l'insieme di unità in $\mathbb{Z}_n$ e sia C l'insieme di unità in $\mathbb{Z}_{mn}$. Allora, la mappa (funzione) $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ data da (2.5) si restringe a una bigezione da C a $A \times B$. Particolarmente $\phi(mn) = |C| = |A||B| = \phi(m)\phi(n)$.*

Dimostrazione. Per definizione, $f^{-1}(A \times B) = \{[x] \in \mathbb{Z}_{mn} \mid f(x) \in A \times B\}$. Inoltre, poiché $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ è una bigezione, ne segue che f si restringe a una bigezione $f^{-1}(A \times B) \to A \times B$.

Per mostrare che $f^{-1}(A \times B) \subseteq C$, dato $([a]_m, [b]_n) \in A \times B$, sia

$$[c]_{mn} = f^{-1}([a]_m, [b]_n), \qquad [c']_{mn} = f^{-1}([a]_m^{-1}, [b]_n^{-1})$$

allora,

$$f([c]_{mn} * [c']_{mn}) = f(c) * f(c') = ([a]_m, [b]_n) * ([a]_m^{-1}, [b]_n^{-1}) = ([1]_m, [1]_n)$$

In particolare, poiché $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ è una bigezione, ne segue che $[c]_{mn} * [c']_{mn} = [1]_{mn}$.

Viceversa, supponiamo che $[c]_{mn} \in \mathbb{Z}_{mn}$ è una unità. Allora, $\mathrm{mcd}(c, mn) = 1$ e quindi per il teorema di Bézout, esistono interi μ e ν tali che $c\mu + (mn)\nu = 1$. Allora,

$$c\mu + m(n\nu) = 1 \implies \mathrm{mcd}(c, m) = 1, \qquad c\mu + n(m\nu) = 1 \implies \mathrm{mcd}(c, n) = 1$$

e quindi $[c]_m$ è una unità di $\mathbb{Z}_m$ e $[c]_n$ è una unità di $\mathbb{Z}_n$. Come tali, $[c]_{mn} \in f^{-1}(A \times B)$.

C.V.D.

Proposizione 2.20. *(Prodotto di Eulero) Se n è un intero positivo allora,*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

dove il prodotto è preso su tutti i divisori primi p di n (ed è il prodotto vuoto $= 1$ quando $n = 1$).

Dimostrazione. Sia $n = p_1^{r_1} \cdots p_k^{r_k}$ la fattorizzazione in primi di n. allora,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{r_1}) \cdots \phi(p_k^{r_k}) \\
&= p_1^{r_1} \left(1 - \frac{1}{p_1}\right) p_2^{r_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{r_k} \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

C.V.D.

Il prossimo risultato è una generalizzazione del piccolo teorema di Fermat:

Teorema 2.21. *(Euler) Siano a e n interi positivi con $n > 1$. Se $\mathrm{mcd}(a, n) = 1$ allora $a^{\phi(n)} \equiv 1 \mod n$.*

Dimostrazione. Prima, notiamo che se R è un anello commutativo con identità, allora il prodotto di due unità di R è ancora una unità di R. Sia $R = \mathbb{Z}_n$ e S l'insieme di unità in R. allora, S è un insieme finito di cardinalità $\phi(n)$ e quindi anche

$$u = \prod_{s \in S} s$$

è una unità di R.

Sia $v \in S$. Allora, la mappa $f : S \to R$ definita da $f(s) = vs$ ha immagine contenuta in S perché $(vs)^{-1} = v^{-1}s^{-1}$. Inoltre, poiché v è una unità, f è iniettiva:

$$f(s) = f(s') \implies vs = vs' \implies v^{-1}vs = v^{-1}vs' \implies s = s'$$

Poiché S è finito, ne segue che f induce una bigezione da S a S. Perciò,

$$u = \prod_{s \in S} s = \prod_{s \in S} f(s) = \prod_{s \in S} vs = v^{\phi(n)} \prod_{s \in S} s = v^{\phi(n)} u$$

e quindi $v^{\phi(n)} = 1$ perché u è una unità. Per finire la dimostrazione, notiamo che $\mathrm{mcd}(a, n) = 1$ implica che $[a] \in R$ è una unità. Ponendo $v = [a]$ ne segue che $[a]^{\varphi(n)} = [1]$, ovvero $a^{\varphi(n)} \equiv 1 \mod n$.

C.V.D.

Teorema 2.22. *(Gauss) Sia n un intero positivo. Allora,*

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

Dimostrazione. Esercizio per lo studente.

C.V.D.

ESERCIZI

Esercizio 7. Trova le soluzioni di $x \equiv 5 \mod 7$ e $x \equiv 3 \mod 13$.

Esercizio 8. Usare il teorema di Eulero per dimostrare che $3^{102} \equiv 9 \mod 10$.

Esercizio 9. Verificare il Teorema (2.22) nei casi $n = 12$ e $n = 60$.

Esercizio 10. Dimostrare che se R e S sono anelli commutativi con identitá, allora anche $R \times S$ é un anello commutativo con identitá rispetto ad addizione e moltiplicazione sulle componenti.

Esercizio 11. Dimostrare che se R é un dominio ~~integrale~~ DI INTEGRITÁ allora $R[x]$ é un dominio integrale.

Esercizio 12. Dimostrare che se R é un dominio integrale con un numero finito di elementi e $a \in R - \{0\}$, allora

$$f : R - \{0\} \to R - \{0\}, \qquad f(x) = ax$$

é suriettiva. Suggerimento: Questa é un'altra applicazione del Lemma (2.14).

Esercizio 13. Verifica il Teorema (2.22). Suggerimento: Si può dimostrare questo per induzione usando la proprietà moltiplicativa di ϕ selezionando un fattore primo p di n e scrivendo $n = p^r m$ con $\mathrm{mcd}(p^r, m) = 1$.

ESERCIZIO 1

Costruire le tavole di addizione e moltiplicazione mod 3

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

*	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

ESERCIZIO 2

Verificare i seguenti esempi di reciprocità quadratica:

- $(p,q) = (13,29)$:

  $29 = 4\cdot 7 + 1,\ 1 = 4\cdot 0 + 1 \Rightarrow 29 \equiv 1 \mod 4$ ✓

  $10^2 \equiv 13 \mod 29$ $\quad (100 = 29\cdot 3 + 13,\ 13 = 29\cdot 0 + 13$ ✓ $)$

  $4^2 \equiv 29 \mod 13$ $\quad (16 = 13\cdot 1 + 3,\ 29 = 13\cdot 2 + 3$ ✓ $)$

  $16 \mod 13 = 3,\ 29 \mod 13 = 3 \Rightarrow 16 \equiv 29 \mod 13$

- $(p,q) = (23,29)$:

  $29 = 4\cdot 7 + 1,\ 1 = 4\cdot 0 + 1 \Rightarrow 29 \equiv 1 \mod 4$ ✓

  $9^2 \equiv 23 \mod 29$ $\quad (81 = 29\cdot 2 + 23,\ 23 = 29\cdot 0 + 23$ ✓ $)$

  $11^2 \equiv 29 \mod 23$ $\quad (121 = 23\cdot 5 + 6,\ 29 = 23\cdot 1 + 6$ ✓ $)$

- $(p,q) = (3,15)$

  $\left.\begin{array}{l} 15 = 4\cdot 3 + 3,\ 3 = 4\cdot 0 + 3 \Rightarrow 15 \equiv 3 \mod 4 \\ 3 = 4\cdot 0 + 3 \Rightarrow 3 \equiv 3 \mod 4 \end{array}\right\}$ ✓

  $15^2 \equiv 3 \mod 37$ $\quad (225 = 37\cdot 6 + 3,\ 3 = 37\cdot 0 + 3$ ✓ $)$

  $1^2 \equiv 37 \mod 3$ $\quad (1 = 3\cdot 0 + 1,\ 37 = 3\cdot 12 + 1)$

ESERCIZIO 3

Verificare i seguenti esempi di reciprocità quadratica:

- $(p,q) = (7,31)$

$$\left.\begin{array}{l} 31 = 4\cdot 7 + 3,\ 3 = 4\cdot 0 + 3 \Rightarrow 31 \equiv 3 \bmod 4 \\ 7 = 4\cdot 0 + 3 \Rightarrow 7 \equiv 3 \bmod 4 \end{array}\right\} \checkmark$$

$10^2 \equiv 7 \bmod 31$ $(100 = 31\cdot 3 + 7,\ 7 = 31\cdot 0 + 7\ \checkmark)$

$2^2 \equiv -31 \bmod 7$ $(4 = 7\cdot 0 + 4,\ -31 + 7\cdot 5 = 4 = 7\cdot 0 + 4\ \checkmark)$

- $(p,q) = (19,31)$

$$\left.\begin{array}{l} 31 = 4\cdot 7 + 3,\ 3 = 4\cdot 0 + 3 \Rightarrow 31 \equiv 3 \bmod 4 \\ 19 = 4\cdot 4 + 3 \Rightarrow 19 \equiv 3 \bmod 4 \end{array}\right\} \checkmark$$

$9^2 \equiv 19 \bmod 31$ $(81 = 31\cdot 2 + 19,\ 19 = 31\cdot 0 + 19\ \checkmark)$

$8^2 \equiv -31 \bmod 19$ $(64 = 19\cdot 3 + 7,\ -31 + 19\cdot 2 = 7 = 19\cdot 0 + 7\ \checkmark)$

ESERCIZIO 4

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

Allora $\det(A) = -360$.

Qual'è il minimo numero primo p per cui ci si aspetta che A^{-1} esista mod p? Calcolare $A^{-1} \bmod p$.

$[x][\det(A)] \equiv [1] \bmod n$

(*) $[2][-360] \equiv [1] \bmod 7 \Rightarrow p = 7$

[OPPURE
i) CALCOLO $A \bmod n$
ii) CALCOLO $A^{-1} \bmod n$]

$$A^{-1} = \frac{1}{360}\begin{pmatrix} -37 & 38 & 23 \\ 68 & 8 & -52 \\ -7 & -22 & 53 \end{pmatrix}$$

$$A^{-1} \bmod 7 = \overset{[5]}{\overset{\shortparallel}{[-2]}} \begin{pmatrix} [5] & [3] & [2] \\ [5] & [1] & [4] \\ [0] & [6] & [4] \end{pmatrix} = \begin{pmatrix} [4] & [1] & [3] \\ [4] & [5] & [6] \\ [0] & [2] & [6] \end{pmatrix}$$

PERCHÉ

$1/360 = -2$ DA (*)

ESERCIZIO 5

Modificare l'esempio (1.10) per dim. che l'intero n è divisibile per 9 se e solo se la somma delle cifre di n è divisibile per 9.

$n \in \mathbb{Z}$

$9 \mid n \iff 9 \mid (a_m + a_{m-1} + \dots + a_0)$

$9 \mid (10-1) \Rightarrow 10 \equiv 1 \mod 9$

$\Rightarrow 10^k \equiv 1^k \equiv 1 \mod 9$

$$(a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0) \equiv (a_m \cdot 1 + a_{m-1} \cdot 1 + \dots + a_1 \cdot 1 + a_0) \mod 9$$

ESERCIZIO 6

Dim. il seguente lemma:

Supponiamo che $a \equiv a' \mod n$ e $b \equiv b' \mod n$.

Allora, $a+b \equiv a'+b' \mod n$ e $ab \equiv a'b' \mod n$.

- $\boxed{a \equiv a' \mod n,\ b \equiv b' \mod n \Rightarrow a+b \equiv a'+b' \mod n}$

  $a \equiv a' \mod n \Rightarrow a - a' = nq,\ q \in \mathbb{Z} \Rightarrow a = a' + nq$

  $b \equiv b' \mod n \Rightarrow b - b' = nr,\ r \in \mathbb{Z} \Rightarrow b = b' + nr$

  $(a+b) - (a'+b') = \cancel{a'} + nq + \cancel{b'} + nr - \cancel{a'} - \cancel{b'} = \underbrace{n(q+r)}_{\text{MULTIPLO DI } n}$

  $\Rightarrow a+b \equiv a'+b' \mod n$

- $\boxed{a \equiv a' \mod n,\ b \equiv b' \mod n \Rightarrow ab \equiv a'b' \mod n}$

  $a \equiv a' \mod n \Rightarrow a = a' + ns,\ s \in \mathbb{Z}$

  $b \equiv b' \mod n \Rightarrow b = b' + nt,\ t \in \mathbb{Z}$

  $\Rightarrow ab = (a'+ns)(b'+nt) = a'b' + \underbrace{a'nt + nsb' + n^2st}_{\text{MULTIPLO DI } n}$

  $\Rightarrow ab \equiv a'b' \mod n$

[OPPURE, PER TRANSITIVITÀ (≡ È UNA REL. DI EQUIV.)]

$a \equiv a' \mod n \Rightarrow ab \equiv a'b \mod n$ (MOLTIPLICO PER b ENTR. I MEMBRI)

$b \equiv b' \mod n \Rightarrow a'b \equiv a'b' \mod n$ (" " a' " " ")

$\Rightarrow ab \equiv a'b' \mod n$

ESERCIZIO 7

Trovare le soluzioni di $x \equiv 5 \mod 7$ e $x \equiv 3 \mod 13$

i) $x \equiv 5 \mod 7$

$x = 40$ perché $40 \mod 7 = 5 = 5 \mod 7$

ii) $x \equiv 3 \mod 13$

$x = 40$ perché $40 \mod 3 = 1 = 40 \mod 13$

ESERCIZIO 8

Usare il th di Eulero per dim. che $3^{102} \equiv 9 \mod 10$

$$\left.\begin{array}{l} a, n \in \mathbb{Z}, \ a, n > 1 \\ MCD(a,n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \mod n \end{array}\right\} \text{TH DI EULERO}$$

$\phi(10) = \phi(5 \cdot 2) = \phi(5)\phi(2) = 4$

$3^{100} \cdot 3^2 \mod 10 = (3^4)^{25} \cdot 3^2 \mod 10 = 1^{25} \cdot 3^2 \mod 10 = 9$

ESERCIZIO 9

Verificare il seguente th nei casi $n=12$ e $n=60$:

Sia n un intero positivo.

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

i) $n = 12 = \sum_{d|12} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12)$

$= 1 + 1 + 2 + 2 + 3\left(1-\frac{1}{3}\right)2\left(1-\frac{1}{2}\right) + 3\left(1-\frac{1}{3}\right)4\left(1-\frac{1}{2}\right)$

$= 6 + (3-1)(2-1) + (3-1)(4-2) =$

$= 6 + 2 + 4 = 12$ ✓

ii) $n = 60 = \sum_{d|60} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(5) + \phi(6) + \phi(10) +$

$+ \phi(12) + \phi(15) + \phi(20) + \phi(30) + \phi(60) =$

$= 1 + 1 + 2 + 2 + 4 + 4 + 4 + 2 + 3\left(1-\frac{1}{3}\right)5\left(1-\frac{1}{5}\right) +$

$+ 5\left(1-\frac{1}{5}\right)4\left(1-\frac{1}{2}\right) + 2\left(1-\frac{1}{2}\right)5\left(1-\frac{1}{5}\right)3\left(1-\frac{1}{3}\right) +$

$+ 4\left(1-\frac{1}{2}\right)5\left(1-\frac{1}{5}\right)3\left(1-\frac{1}{3}\right) =$

$= 20 + (3-1)(5-1) + (5-1)(4-2) + (2-1)(5-1)(3-1)$

$+ (4-2)(5-1)(3-1) =$

$= 20 + (3-1)(5-1) + (5-1)(4-2) + (2-1)(5-1)(3-1)$

$+ (4-2)(5-1)(3-1) =$

$= 20 + 8 + 8 + 8 + 16 = 60$ ✓

ESERCIZIO 10

Dim. che se R e S sono anelli comm. con id., allora $R \times S$ è un anello comm. con id. rispetto ad addizione e moltiplic. sulle componenti.

Siano $(r_1, s_1), (r_2, s_2), (r_3, s_3) \in R \times S$

ADDIZIONE: $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$

MOLTIPLICAZ.: $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$

ADDIZIONE

CHIUSURA: $(r_1 + r_2, s_1 + s_2) \in R \times S$

ASSOCIATIVITÀ: $(r_1, s_1) + ((r_2, s_2) + (r_3, s_3)) = (r_1, s_1) + (r_2 + r_3, s_2 + s_3)$

$= (r_1 + r_2 + r_3, s_1 + s_2 + s_3) =$

$= ((r_1, s_1) + (r_2, s_2)) + (r_3, s_3) = (r_1 + r_2, s_1 + s_2) + (r_3, s_3)$

$= (r_1 + r_2 + r_3, s_1 + s_2 + s_3)$

COMMUTATIVITÀ: $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) = (r_2, s_2) + (r_1, s_1)$

IDENTITÀ: $(r_1, s_1) + (0, 0) = (r_1, s_1)$

INVERSO: $(r_1, s_1) + (-r_1, -s_1) = (0, 0)$

MOLTIPLICAZIONE

CHIUSURA: $(r_1 r_2, s_1 s_2) \in R \times S$

ASSOCIATIVITÀ: $((r_1, s_1)(r_2, s_2))(r_3, s_3) = (r_1 r_2, s_1 s_2)(r_3 s_3) =$

$= (r_1 r_2 r_3, s_1 s_2 s_3) =$

$= (r_1, s_1)((r_2, s_2)(r_3, s_3)) = (r_1, s_1)(r_2 r_3, s_2 s_3) =$

$= (r_1 r_2 r_3, s_1 s_2 s_3)$

COMMUTATIVITÀ: $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2) = (r_2 s_2)(r_1 s_1)$

IDENTITÀ: $(r_1, s_1)(1, 1) = (r_1, s_1)$

PROPR. DISTRIBUTIVA:

$(r_1, s_1)((r_2, s_2) + (r_3, s_3)) = (r_1, s_1)(r_2 + r_3, s_2 + s_3) = (r_1(r_2 + r_3), s_1(s_2 + s_3))$

$= (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3)$

$= (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3) = (r_1 r_2, s_1 s_2) + (r_1 r_3, s_1 s_3)$
$= (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3)$

ESERCIZIO 11

Dim. che se R è un dominio di integrità, allora $R[x]$ è un dominio di integrità.

Siano $f(x) = a_n x^n + \dots + a_0$, $g(x) = b_n x^m + \dots + b_0$

$f(x) \neq 0, g(x) \neq 0 \Rightarrow a_n \neq 0, b_n \neq 0$ perché R è un dominio di integrità ($a \cdot b = 0 \Rightarrow a = 0$ o $b = 0$)

$$\Rightarrow f \cdot g = \underbrace{a_n b_n x^{n+m}}_{\neq 0 \Rightarrow f \cdot g \neq 0} + \dots + a_0 b_0$$

$\therefore f \neq 0, g \neq 0 \Rightarrow f \cdot g \neq 0 \Rightarrow R[x]$ è un dominio di integrità

ESERCIZIO 12

Dim. che se R è un dominio integrale con un num. finito di elementi $a \in R - \{0\}$, allora:
$f: R - \{0\} \to R - \{0\}$, $f(x) = ax$ è suriettiva

$|R| < \infty \Rightarrow |R - \{0\}| < \infty$
$f: A \to B$, $|A| = |B| = |R - \{0\}|$
$\therefore$ per il lemma 2.14 è sufficiente dim. che f è iniettiva
$f(x) = f(y) \Rightarrow ax = ay \Rightarrow a(x-y) = 0$, $a \neq 0$
Dichè R è un dominio integrale $uv = 0 \Leftrightarrow u = 0$ o $v = 0$
$\therefore a(x-y) = 0 \Leftrightarrow \cancel{a = 0}$ oppure $x - y = 0 \Rightarrow x = y$

PERCHÉ $a \in R - \{0\}$

$\therefore f(x) = f(y) \Rightarrow x = y \Rightarrow f$ è iniettiva (quindi suriettiva)

ES. DI GRUPPO:

$\mathbb{Z}_5 - \{0\} = \{[1], [2], [3], [4]\}$

- ASSOCIATIVITÀ ✓
- IDENTITÀ: 1
- INVERSI: $[1]^{-1} = [1]$
  $[2]^{-1} = [3]$ → PERCHÉ $2 \cdot 3 \bmod 5 = 1$
  $[4]^{-1} = [4]$

Lezione 8 e 9

CIOÈ L'INSIEME G DEVE ESSERE CHIUSO RISPETTO ALL'OPERAZIONE *

1. Gruppi

Definizione 1.1. Un gruppo $(G, *)$ consiste di un insieme G con una mappa $* : G \times G \to G$ con le seguenti proprietà:

- (Associatività): $(a * b) * c = a * (b * c)$ per ogni $a, b, c \in G$.
- (Identità): Esiste $e \in G$ tale che $e * a = a$ e $a * e = a$ per ogni $a \in G$.
- (Inverso): Per ogni $a \in G$ esiste $b \in G$ tale che $a * b = e$ e $b * a = e$.

Spesso scriviamo ab e 1 invece di $a * b$ e e quando la mappa $*$ e l' elemento identità e sono chiari dal contesto. Un gruppo abeliano è un gruppo $(G, *)$ tale che $a * b = b * a$ per ogni $a, b \in G$.

Esempio 1.2. $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$ sono gruppi abeliani con elemento identità 0. L' inverso di $a \in \mathbb{Z}$ è $-a$. L' inverso di $[a] \in \mathbb{Z}_n$ è $[-a]$.

Esempio 1.3. Sia V uno spazio vettoriale. Allora, $(V, +)$ è un gruppo abeliano con elemento identità $0 \in V$. L'inverso di $v \in V$ è $-v$. (COME GRUPPO NON VALE LA MOLT. SCALARE)

Nota 1.4. Visti i due esempi precedenti, se G è un gruppo abeliano, di solito scriviamo $+$ invece di $*$, 0 invece di e, e $-a$ invece di a^{-1}.

LO PERCHÉ 0 È L'ELEM. NEUTRO PER L'ADDIZIONE

ANCHE $\mathbb{Z}_p$, O UN CAMPO,

Esempio 1.5. L'insieme $GL_n(K)$ di tutte le matrici invertibili di tipo $n \times n$ per $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ è un gruppo rispetto alla moltiplicazione di matrici $A * B = AB$. L'elemento identità è la matrice identità $n \times n$. L'inverso di $A \in GL_n$ è A^{-1}.

Esempio 1.6. L'insieme U di matrici unimodulari di tipo $n \times n$ è a gruppo rispetto alla moltiplicazione di matrici. L'elemento identità è la matrice identità $n \times n$. l'inverso di A è A^{-1}.

Esempio 1.7. Ricordiamo che una matrice di tipo $n \times n$ $A = (a_{ij})$ è una matrice diagonale se $a_{ij} = 0$ quando $i \neq j$. L'insieme di matrici diagonali in $GL_n(K)$ per $K = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ è un gruppo rispetto alla moltiplicazione di matrici.

Esempio 1.8. sia S uno set. Allora, l'insieme G di tutte le mappe biunivoche $f : S \to S$ è UN GRUPPO rispetto alla composizione $(f * g)(s) = f(g(s))$. L'elemento identità è la funzione identità $f(s) = s$ per ogni $s \in S$. L'inverso di $f \in G$ è la funzione inversa f^{-1}.

Nota 1.9. Sia S un'insieme con n elementi. Allora, il gruppo di permutazioni di S è di solito denotato con S_n e chiamato il gruppo simmetrico (o di permutazioni) su n lettere.

Ora, dei controesempi:

IL MOTIVO PER CUI S NON È UN GRUPPO È CHE * NON È UNA MAPPA $S \times S \to S$

Esempio 1.10. Sia S l'insieme di matrici invertibili di tipo 2×2 che sono diagonalizzabili (su $\mathbb{C}$). Allora, S contiene la matrice identità e contiene elementi inversi. Ma S non è not chiuso rispetto alla moltiplicazione perché

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

CHE NON È DIAGONALIZZABILE PERCHÉ LA MOLTEPLICITÀ GEOM. (1) È DIVERSA DALLA MOLT. ALGEBRICA (2)

Comunque, $a * (b * c) = (a * b) * c$ quando tutti i termini sono elementi di S.

Nota 1.11. La differenza tra gli esempi (1.7) e (1.10) è che nel primo tutte le matrici sono diagonali rispetto alla base standard di $\mathbb{C}^n$, mentre nel secondo diventano diagonali solo dopo un cambio di basi.

(PERCHÉ SONO DIAGONALIZZ., NON DIAGONALI, DIVENTANO DIAGONALI SOLO PER UNA CERTA SCELTA DI BASI)

Esempio 1.12. Sia M l'insieme di tutte le matrici di tipo 2×2. Allora M è chiuso rispetto alla moltiplicazione di matrici e contiene la matrice identità. Inoltre, la moltiplicazione di matrici è associativa. Ma, M non è chiuso rispetto a inversi.

Esempio 1.13. Sia S l'insieme di funzioni lisce $f : \mathbb{R} \to \mathbb{R}$ tali che $\int_{-\infty}^{\infty} f^2(x)\,dx$ converge. Allora, il prodotto convoluzione

$$(f * g)(t) = \int_{-\infty}^{\infty} f(s)g(t-s)\,ds$$

definisce un'operazione binaria su S che è associativa per il teorema di Fubini. Tramite la sostituzione $r = t - s$ si vede che $(f * g)(t) = (g * f)(t)$. Supponiamo che δ sia l'elemento identità per questa operazione. Allora,

DELTA DI DIRAC

$$(f * \delta)(t) = \int_{-\infty}^{\infty} f(s)\delta(t-s)\,ds = f(t)$$

Ciò forza $\delta(v)$ ad essere zero per $v \neq 0$ (per evitare di incorporare il comportamento di f vicino a t) e ∞ a $v = 0$ per catturare il valore di f a t. Quindi, il prodotto convoluzione non ha un elemento identità.

La maggior parte delle relazioni binarie non sono associative.

Esempio 1.14. Sia $T = \{C, F, S\}$ dove C=Carta, F=Forbici e S=Sasso. Definiamo una mappa $* : T \times T \to T$ dichiarando che $A * B$ è il vincitore del gioco morra cinese con le regole usuali.

$*$	C	F	S
C	C	F	C
F	F	F	S
S	C	S	S

allora, $*$ è commutativo ma non associativo.

Esercizi

Esercizio 1. Dimostrare che le seguenti 6 matrici formano un gruppo:

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad R_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad R_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad T_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad T_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

rispetto alla moltiplicazione di matrici. Suggerimento: Poiché la moltiplicazione di matrici è associativa, puoi usare ciò per verificare l'associatività.

Esercizio 2. Dimostrare che l'insieme di elementi unità in $\mathbb{Z}_n$ rispetto alla moltiplicazione modulo n forma un gruppo.

Esercizio 3. Sia G uno gruppo e $g \in G$. Dimostrare che $(g^{-1})^{-1} = g$.

Esercizio 4. Sia G un gruppo con elemento identità e. Dimostrare che e è unico. In altre parole, se anche $f \in G$ soddisfa $a * f = a$ e $f * a = a$ per ogni $a \in G$ allora $e = f$. Suggerimento: Calcola $e * f$ in due modi diversi.

♉ **Esercizio 5.** sia G uno gruppo e $a \in G$. Mostrare che a^{-1} è unico. In altre parole, se $b \in G$ è un altro elemento tale che $a * b = e$ e $b * a = e$ allora $b = a^{-1}$. Suggerimento: Calcola $a^{-1} * a * b$ in due modi diversi.

♊ **Esercizio 6.** Dimostra che gli interi non-negativi non formano un gruppo rispetto all'addizione.

♋ **Esercizio 7.** Dimostra che la tavola di moltiplicazione per il gioco morra cinese non è associativa.

♌ **Esercizio 8.** Dimostra che gli interi non formano un gruppo rispetto alla sottrazione $a * b = a - b$.

2. SOTTOGRUPPI

Un sottogruppo è l'analogo di un sottospazio:

Definizione 2.1. Un sottoinsieme H di un gruppo G è un sottogruppo se e solo se

- H contiene l'elemento identità e di G.
- $a \in H \implies a^{-1} \in H$.
- $a, b \in H \implies a * b \in H$.

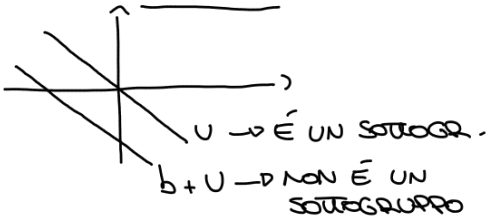
Esempio 2.2. Sia G un gruppo. allora, G e $\{e\}$ sono sottogruppi di G. Un sottogruppo H di G è chiamato proprio se $H \neq G$. Un sottogruppo H di G è non-triviale se $H \neq \{e\}$.

Esempio 2.3. Sia V uno spazio vettoriale e U un sottospazio di V. allora, U è un sottogruppo di $(V, +)$ poiché contiene l'elemento identità $0 \in V$, è chiuso rispetto a $+$ e contiene l'inverso $-u$ di ogni elemento $u \in U$. In contrasto, se $b \in V - U$ allora il traslato

$$b + U = \{b + u \in U \mid u \in U\}$$

non è una sottospazio perché non contiene 0:

$$u \in U, \quad b + u = 0 \implies b = -u \implies b \in U$$



Esempio 2.4. Sia n un intero positivo. Allora,

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

è un sottogruppo di $(\mathbb{Z}, +)$. DOVE $(\mathbb{Z}, +)$ É UN GRUPPO ABELIANO

Esempio 2.5. Le matrici unimodulari (esempio (1.6)) e le matrici diagonali (esempio (1.7)) sono sottogruppi del gruppo di matrici $GL_n(K)$ (esempio (1.5)). Il sottoinsieme $SL_n(K)$ di $GL_n(K)$ costituito dalle matrici con determinante 1 è un sottogruppo. L'insieme $SL_n(\mathbb{Z})$ di matrici $n \times n$ con determinante 1 con elementi interi è un sottogruppo del gruppo di matrici unimodulari.

Lemma 2.6. *Sia G un gruppo. Allora, un sottoinsieme non vuoto H di G è un sottogruppo se e solo se $a, b \in H \implies ab^{-1} \in H$.*

Dimostrazione. Poiché H non è vuoto, esiste un elemento $a \in H$. Allora, $aa^{-1} = e \in H$. Se $b \in H$ allora $eb^{-1} = b^{-1} \in H$. Quindi, $a, b \in H \implies a(b^{-1})^{-1} = ab \in H$. Viceversa, se H è un sottogruppo di G allora $e \in H$ e quindi H non è vuoto. Poiché H è chiuso rispetto al prodotto e inversi, $a, b \in H \implies ab^{-1} \in H$.

C.V.D.

Lemma 2.7. *Sia H un sottogruppo di $(G, *)$. allora, H è un gruppo rispetto alla restrizione di $*$ ad H.*

Dimostrazione. Esercizio per la studentessa.

C.V.D.

L'intersezione di due sottospazi vettoriali è un sottospazio. In contrasto, l'unione di due sottospazi vettoriali U_1 e U_2 non è un sottospazio a meno che o $U_1 \subseteq U_2$ o $U_2 \subseteq U_1$. Lo stesso vale per sottogruppi:

Lemma 2.8. *Siano H e K sottogruppi di G. Allora, $H \cap K$ è un sottogruppo di G.*

Lemma 2.9. *L'unione di due sottogruppi H e K di G è un sottogruppo se e solo se $H \subseteq K$ o $K \subseteq H$.*
(PERCHÉ L'UNIONE NON É CHIUSA RISPETTO ALLA SOMMA)

Dimostrazione. Sia P l'affermazione che $H \cup K$ è un sottogruppo di G e Q l'affermazione che $H \subseteq K$ o $K \subseteq H$. Allora,

- $Q \implies P$: In questo caso $H \cup K$ è H o K, che è un sottogruppo.
- $P \implies Q$: Consideriamo il contrapposto CONTRONOMINALE $(\neg Q) \implies (\neg P)$. Per definizione $\neg Q$ implica che esistono $h \in H$ e $k \in K$ tali che $h \notin K$ e $k \notin H$. Supponiamo che $H \cup K$ è un sottogruppo. Allora, $hk \in H \cup K$ e quindi $hk \in H$ o $hk \in K$. Se $hk \in H$ allora $k = h^{-1}hk \in H$ che è una contraddizione. Similmente, se $hk \in K$ allora $h = hk(k^{-1}) \in K$, che è di nuovo una contraddizione. Quindi, $\neg Q \implies \neg P$.

C.V.D.

Sia S un sottoinsieme di V. Allora, per definizione, span(S) è l'intersezione di tutti i sottospazi U di V tali che $S \subseteq U$. La stessa definizione funziona per sottoinsiemi di un gruppo G.

Definizione 2.10. Sia S un sottoinsieme di un gruppo G. allora, il sottogruppo $\langle S \rangle$ di G generato da S è l'intersezione di tutti i sottogruppi H di G che contengono S. (CIOÉ $\langle S \rangle = \bigcap_{S \subseteq H} H$)

Esempio 2.11. Sia $g \in G$. Allora

$$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$$

dove $g^0 = e$ e $g^{-n} = (g^{-1})^n$ per $n > 0$.

Alternativamente, in analogia con spazi vettoriali, possiamo definire $\langle S \rangle$ in termini di "combinazioni lineari finite":

Lemma 2.12. *$\langle S \rangle$ consiste di tutti i prodotti finiti di elementi $s_1 \dots s_r$ dove ogni s_j o $s_j^{-1} \in S$.*

Dimostrazione. Sia H l'insieme di tutti i prodotti finiti $s_1 \cdots s_r$ dove ogni s_j o $s_j^{-1} \in S$. Per definizione, il prodotto vuoto è e, perció $e \in H$. Se a, $b \in H$ allora anche ab è un prodotto finito di elementi di S e i loro inversi, quindi $ab \in H$. Similmente,

$$a = s_1 \dots s_r \in H \implies a^{-1} = s_r^{-1} \cdots s_1^{-1} \in H$$

quindi H è un sottogruppo di G che contiene S, e quindi per definizione $\langle S \rangle \subseteq H$.

Viceversa, $H \subseteq S$ perché ogni sottogruppo K di G che contiene S deve contenere tutti i prodotti finiti di elementi di S e inversi.

C.V.D.

Esempio 2.13. $\mathbb{Z} = \overbrace{\langle 2, 3 \rangle}^{H}$ poiché $1 = 3 - 2$.

$2, 3 \in H \implies 3 - 2 \in H \implies \underbrace{1 \in H}$

$\Downarrow$

$1 + 1 + 1 \dots \in H \implies H = \langle 2, 3 \rangle = \mathbb{Z}$

Esempio 2.14. Il gruppo $SL_2(\mathbb{Z}) = \langle A, B\rangle$ dove

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(Questo non è ovvio).

Definizione 2.15. Un gruppo G è ciclico se e solo se $G = \langle g\rangle$ per qualche $g \in G$.

Esempio 2.16. (i) $(\mathbb{Z}, +) = \langle 1\rangle$. (ii) $n\mathbb{Z} = \langle n\rangle$. (iii) $(\mathbb{Z}_n, +) = \langle [1]_n\rangle$. (iv) Il gruppo $\langle g\rangle$ è sempre abeliano. In particolare, se H è un gruppo non abeliano allora H non è della forma $\langle g\rangle$. ($G = \langle g \rangle \Rightarrow G$ ABELIANO, G NON ABELIANO $\Rightarrow G \neq \langle g \rangle$)

Definizione 2.17. Sia G un gruppo. Se G è finito allora $\mathrm{ord}(G) = |G|$. Altrimenti, $\mathrm{ord}(G) = \infty$. Se $g \in G$ allora $\mathrm{ord}(g) = \underbrace{\mathrm{ord}(\langle g\rangle)}$. # ELEM. NEL GRUPPO GENERATO DA g ↳ # ELEM. IN G

Esempio 2.18. Per l'esercizio (2), le unità in $\mathbb{Z}_n$ formano un gruppo. Quando $n = 5$, questo è semplicemente l'insieme di tutti gli elementi non nulli in $\mathbb{Z}_5$. Dalla lezione precedente, abbiamo la tavola moltiplicativa

$3^1 \bmod 5 = 3$
$3^2 \bmod 5 = 4$
$3^3 \bmod 5 = 2$
$3^4 \bmod 5 = 1$
$\Rightarrow \langle 3\rangle = \underbrace{\langle 1,2,4,3\rangle}$
$\Downarrow$
$\mathrm{ord}([3]) = 4$

$*$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

, $\quad [3]^2 = [4], [3]^3 = [2]$

$2^1 \bmod 5 = 2$
$2^2 \bmod 5 = 4$
$2^3 \bmod 5 = 3$
$2^4 \bmod 5 = 1$
$\Rightarrow \langle 2\rangle = \langle 1,3,4,2\rangle$
$\Rightarrow \mathrm{ord}([2]) = 4$

$1^k \bmod 5 = 1 \ \forall k$

allora, $\mathrm{ord}([1]) = 1$, $\mathrm{ord}([2]) = 4$, $\mathrm{ord}([3]) = 4$ e $\mathrm{ord}([4]) = 2$.

Ora facciamo un'osservazione fondamentale: sia G un gruppo e H un sottoinsieme finito non vuoto di G che chiuso rispetto al prodotto. Allora, anche l'insieme

$$\{h,\, h^2,\, h^3,\, \dots\} \subseteq H$$

è finito. In particolare, devono esistere due distinti interi positivi r e s tali che $h^r = h^s$. Scambiando r e s se necessario, assumiamo che $s > r$. Allora, $h^r = h^r h^{s-r}$, il che implica $h^{s-r} = e$. Se $s - r = 1$ ciò mostra che $h = e$. Altrimenti, $s - r > 1$. Allora, $h * h^{s-r-1} = e$ e quindi anche H contiene h^{-1}. Insomma, abbiamo dimostrato:

Lemma 2.19. *Sia H un sottoinsieme finito non vuoto di un gruppo G che è chiuso rispetto alla moltiplicazione. Allora, H è un sottogruppo di G.*

Ora facciamo attenzione a una costruzione che è interessante solo nel caso dove G è un gruppo non abeliano:

Esempio 2.20. Sia G un gruppo e $x \in G$. Allora,

$$C(x) = \{g \in G \mid gx = xg\} \tag{2.21}$$

è un sottogruppo di G chiamato il centralizzante di x:

- $ex = xe \implies e \in C(x)$.
- $ax = xa$ e $bx = xb \implies abx = axb = xab \implies ab \in C(x)$.
- $ax = xa \implies a^{-1}ax = a^{-1}xa \implies x = a^{-1}xa$
  $\implies xa^{-1} = a^{-1}xaa^{-1} \implies xa^{-1} = xa^{-1} \implies a^{-1} \in C(x)$.

Esempio 2.22. Sia $G = SL_2(\mathbb{R})$ e

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Allora, $C(X) = \{\, A \in GL_2(\mathbb{R}) \mid AX = XA \,\}$.

Esercizi

Esercizio 9. Verificare il Lemma (2.8).

Esercizio 10. Trovare un elemento di ordine 2 e un elemento di ordine 3 nel gruppo dell'esercizio (1).

Esercizio 11. Descrivere il centralizzante dell'esempio (2.22) in termini di condizioni algebriche sulle entrate della matrice A.

Esercizio 12. Verificare il Lemma (2.7).

Esercizio 13. Usa il teorema della divisione e il principio di buon ordinamento per mostrare che ogni sottogruppo di $(\mathbb{Z}, +)$ è della forma $n\mathbb{Z}$.

3. Gruppi prodotto

Un'altra costruzione di base dall'algebra lineare è che se U e V sono spazi vettoriali allora anche $U \times V$ è uno spazio vettoriale rispetto a addizione e moltiplicazione scalare di componenti. Lo stesso è vero per gruppi:

Proposizione 3.1. *Siano H e K gruppi. Allora, $H \times K$ è un gruppo rispetto all'operazione binaria*

$$(h_1, k_1) * (h_2, k_2) = (h_1 h_2, k_1 k_2)$$

con elemento identità $e = (e_H, e_K)$. Se H e K sono gruppi finiti, allora $ord(H \times K) = ord(H) \times ord(K)$. Altrimenti $H \times K$ ha ordine infinito.

Dimostrazione. Esercizio per lo studente.

C.V.D.

Per continuare, ricordiamo che un isomorfismo di spazi vettoriali è una mappa lineare biettiva $f : U \to V$.

Definizione 3.2. Siano G e H gruppi. Allora, $f : G \to H$ è un isomorfismo se e solo se

- f è biettiva.
- $f(g_1 g_2) = f(g_1) f(g_2)$ per ogni g_1, $g_2 \in G$.

Diciamo che una coppia di gruppi G e H sono isomorfi se e solo se esiste un isomorfismo $f : G \to H$, e in questo caso scriviamo $G \cong H$.
↳ isomorfo

Esempio 3.3. L'insieme $(0, \infty)$ è un gruppo rispetto alla moltiplicazione. La mappa esponenziale $\exp : \mathbb{R} \to (0, \infty)$ è un isomorfismo perché è biettiva (con inversa $\log$) e
$(\mathbb{R}, +)$

$$\exp(a + b) = \exp(a) \exp(b)$$

Esempio 3.4. Sia $U(\ell)$ il gruppo di unità in $\mathbb{Z}_\ell$ rispetto alla moltiplicazione. Nella lezione 7, abbiamo visto che se m e n sono interi positivi e $\mathrm{mcd}(m, n) = 1$ allora

$$f : \mathbb{Z}_{nm} \to \mathbb{Z}_m \times \mathbb{Z}_n, \qquad f([x]_{mn}) = ([x]_m, [x]_n) \quad (*) \tag{3.5}$$

$\phi(mn) = \phi(m)\phi(n)$

è una biezione che rispetta la moltiplicazione e si restringe a una biezione da $U(mn)$ a $U(n) \times U(m)$. Quindi, f è un isomorfismo da $U(mn)$ a $U(n) \times U(m)$.

Esempio 3.6. Anche la mappa (3.5) rispetta l'addizione, e quindi definisce un isomorfismo da $\mathbb{Z}_{nm} \to \mathbb{Z}_m \times \mathbb{Z}_n$. (Esercizio per la studentessa).

Il prossimo risultato è una forma debole del teorema cinese del resto:

(*) $f([x]_{mn}) = ([x]_m, [x]_n)$
$f([y]_{mn}) = ([y]_m, [y]_n)$
$\Rightarrow f([xy]_{mn}) = f([x]_{mn}) f([y]_{mn})$

Proposizione 3.7. *Siano $n_1, n_2, \ldots, n_k$ interi maggiori di 1 che siano primi l'uno con l'altro (in altre parole $\mathrm{mcd}(n_i, n_j) = 1$ se $i \neq j$). allora,*

$$\mathbb{Z}_{n_1 \cdots n_k} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

Dimostrazione. Poiché $n_1, \ldots, n_k$ sono primi l'uno con l'altro, non hanno fattori primi in comune. Allora, $\mathrm{mcd}(n_1 \cdots n_j, n_{j+1} \cdots n_k) = 1$ e quindi

$$\mathbb{Z}_{n_1 \cdots n_k} \cong \mathbb{Z}_{n_1} \times \underbrace{(\mathbb{Z}_{n_2} \cdots \times \mathbb{Z}_{n_k})}_{\text{NON HA UN FATTORE COMUNE CON } \mathbb{Z}_{n_1}} \cong \cdots \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

C.V.D.

Esempio 3.8. $\mathbb{Z}_{36} \cong \mathbb{Z}_4 \times \mathbb{Z}_9$.

Se U e V sono spazi vettoriali di dimensione finita, allora U e V sono isomorfi se e solo se hanno la stessa dimensione. Il prossimo risultato dice che, a meno di isomorfismi, i gruppi abeliani finiti sono determinati da una lista di interi positivi.

Teorema 3.9. *(Teorema del Fattore Invariante, Gauss et. al.) Sia G un gruppo abeliano non banale finito. Allora c'è un unico insieme di divisori d_1, d_2,..., d_r di $|A|$ tali che*

- $|G| = d_1 \cdots d_r$ *dove ogni* $d_j > 1$.
- $G \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$.
- $d_r | d_{r-1}, \ldots, d_2 | d_1$. ↳ SOMMA DIRETTA (O PROD. DIRETTO)

La lista $(d_1, \ldots, d_r)$ si chiama lista dei fattori invarianti di G. Una coppia di gruppi abeliani finiti G e H sono isomorfi se e solo se hanno gli stessi fattori invarianti.

Dimostrazione. Omesso per ora.

C.V.D.

Nota 3.10. Una possibile lista di fattori invarianti di un gruppo abeliano di ordine n è semplicemente (n).

L'algoritmo per trovare i possibili fattori invarianti di n è di semplicemente trovare la fattorizzazione prima di n e poi raggruppare questi fattori primi in un modo che rispetti la condizione di divisibilità $d_j | d_{j-1}$.

Esempio 3.11. Siano a e b due (distinti) numeri primi.

- Se $n = a^2 b^2$, allora i possibili fattori invarianti di un gruppo abeliano di ordine n sono:
$$(aabb), (abb, a), (aab, b), (ab, ab)$$
- se $n = a^2 b^3$ allora i possibili fattori invarianti di un gruppo abeliano di ordine n sono
$$(aabbb), \quad (abbb, a), \quad (aabb, b), \quad (abb, ab), \quad (aab, b, b), \quad (ab, ab, b)$$

Esempio 3.12.

- $n = 36$. Per l'esempio precedente, i fattori invarianti sono (36), $(18, 2)$, $(12, 3)$, $(6, 6)$.
- $n = 24$. I possibili fattori invarianti sono
$$(24) = (abbb), \qquad (12, 2) = (abb, b), \qquad (6, 2, 2) = (ab, b, b)$$
dove $a = 3$ e $b = 2$.

Esempio 3.13. Sia G un gruppo abeliano di ordine 30. Allora,

$$30 = 5 \times 3 \times 2$$

e quindi (30) è l'unico possibile fattore invariante.

Proposizione 3.14. *Sia $n > 1$ un intero positivo libero di quadrati. Allora, c'è esattamente un gruppo abeliano di ordine n.*

Dimostrazione. Come nell'esempio precedente con il gruppo di ordine 30, poiché n è libero di quadrati, ogni fattore primo di n appare con la potenza 1, e quindi (n) è l'unico possibile fattore invariante.

C.V.D.

Più generalmente, per calcolare il numero di possibili gruppi abeliani di ordine n, ricordiamo che una partizione di n è una somma della forma

$$n = a_1 + a_2 + \cdots + a_m$$

dove ogni a_j è un intero positivo. Due partizioni sono considerate equivalenti se sono uguali a meno di riordinamento.

Esempio 3.15. A meno di riordinamento, le possibili partizioni di 4 sono

$$4, \quad 3+1, \quad 2+2, \quad 2+1+1, \quad 1+1+1+1$$

Se ℓ è un intero positivo, sia $\pi(\ell)$ il numero di partizioni equivalenti di ℓ. Una conseguenza della dimostrazione del teorema del fattore invariante è:

Teorema 3.16. *Sia $n > 1$ un intero con fattorizzazione prima $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$. Allora, il numero di gruppi abeliani di ordine n è $\pi(k_1) \cdots \pi(k_r)$.*

Esempio 3.17. Se p è un numero primo allora ci sono $\pi(n)$ sottogruppi di ordine p^n. Per vedere ciò, cominciamo con

$$p^n = (p \cdots p)$$

e inseriamo virgole cominciando da destra verso sinistra in modo tale che ogni nuovo blocco contiene almeno tante copie di p quante l'ultimo blocco. In questo modo, otteniamo una decomposizione nel prodotto

$$p^n = p^{a_1} p^{a_2} \cdots p^{a_k}$$

dove $a_1 + \cdots + a_k$ è una partizione di n con $a_1 \geq a_2 \geq \cdots \geq a_k$. viceversa, dopo riordinamento, ogni partizione di n da una tele decomposizione come prodotto di p^n.

$MCD(n_j, n_k) = 1, \; n_j \neq n_k$

$\mathbb{Z}_{n_1 \cdots n_k} = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$

$\mathbb{Z}_{p_1^{k_1} \cdots p_r^{k_r}} = \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}}$

Esercizi

Esercizio 14. Verifica la Proposizione (3.1).

Esercizio 15. Determina tutti i possibili fattori invarianti di gruppi abeliani di ordine 144 e 360.

Esercizio 16. Verifica che (3.5) soddisfa $f(u+v) = f(u) + f(v)$.

Esercizio 17. Dimostra che

- Se $i > j$ allora $\pi(i) > \pi(j)$.
- $\pi(\ell) \geq \ell$.
- Non esiste un intero n tale che $\pi(n) = 13$.

4. Cosets, Teorema di Lagrange, Formula delle Classi di Coniugio

Sia H un sottogruppo di G. Sia $\sim$ la relaziona su G definita da

$$a \sim b \iff a^{-1}b \in H \tag{4.1}$$

Per il prossimo risultato, ricordiamo che come la moltiplicazione di matrici, se G è un gruppo allora $(xy)^{-1} = y^{-1}x^{-1}$ e $(x^{-1})^{-1} = x$.

Lemma 4.2. *L'equazione* (4.1) *è una relazione di equivalenza.*

Dimostrazione.

- $a \sim a$: $a^{-1}a = e \in H$.
- $a \sim b \implies b \sim a$: $a \sim b \iff a^{-1}b \in H$. Quindi,
$$a^{-1}b \in H \implies (a^{-1}b)^{-1} \in H \implies b^{-1}a \in H \implies b \sim a$$
- $a \sim b, b \sim c \implies a \sim c$: $a \sim b \iff a^{-1}b \in H$ e $b \sim c \iff b^{-1}c \in H$. Allora, $(a^{-1}b)(b^{-1}c) \in H \implies a^{-1}c \in H \implies a \sim c$.

C.V.D.

Esempio 4.3. Sia U be un sottospazio di V. Allora, U è un sottogruppo di $(V, +)$ e $v_1 \sim v_2 \iff v_1 - v_2 \in U$. In altre parole, $V/\sim$ è, come insieme, lo spazio vettoriale V/U. Ma, al momento non abbiamo una struttura di spazio vettoriale su V/U.

In luce di questo esempio, dato un sottogruppo H di G, il quoziente associato di G via la relazione di equivalenza $\sim$ è di solito scritta G/H.

Esempio 4.4. Sia $n > 1$ un intero. Allora, $n\mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}, +)$ e $a \sim b \iff a - b \in n\mathbb{Z}$. In altre parole, $a \sim b$ se e solo se $a \equiv b \mod n$. Al momento, questa e solo una costruzione di insiemi, quindi non sappiamo che $\mathbb{Z}/n\mathbb{Z}$ ha addizione e moltiplicazione modulo n. $\mathbb{Z}/n\mathbb{Z} = \{0, \dots, n-1\}$

Esempio 4.5. $\mathbb{Z}$ è un sottogruppo di $(\mathbb{R}, +)$. In questo caso, $x \sim y \iff x - y \in \mathbb{Z}$. Graficamente, possiamo pensare a $\mathbb{R}/\mathbb{Z}$ come segue: sia $x \in \mathbb{R}$. Allora, dopo una traslazione di x come un intero, possiamo supporre $x \in [0, 1]$. Questo ci da un unico rappresentante di $[x]$ a meno che $x \in \{0, 1\}$. In questo caso $[0] = [1]$, e quindi gli estremi di $[0, 1]$ vengono identificati via $\sim$. Quindi, $\mathbb{R}/\mathbb{Z}$ è un "loop". Per ottenere una mappa da $\mathbb{R}/\mathbb{Z}$ a un cerchio, sia

$$f(x) = e^{2\pi i x} = \cos(2\pi x) + \sqrt{-1}\sin(2\pi x)$$

allora, $f(x) = f(y) \iff x - y \in \mathbb{Z}$ e l'immagine di f è il cerchio unitario nel piano complesso.

Definizione 4.6. Sia H un sottogruppo di G e $a \in G$. Allora,

$$aH = \{\, ah \mid h \in H \}$$

è chiamato il coset (classe laterale) di sinistra di a.

Proposizione 4.7. *Sia H un sottogruppo di G e a, $b \in G$. Allora, $a \sim b$ se e solo se $b \in aH$.*

Dimostrazione.

- se $a \sim b$ allora $a^{-1}b = h \in H \implies b = ah \in aH$.
- se $b \in aH$ allora $b = ah$ per qualche $h \in H$ e quindi $a^{-1}b \in H$ che implica $a \sim b$.

C.V.D.

Definizione 4.8. Sia H un sottogruppo di G. Allora, l'indice $[G : H]$ è la cardinalità di G/H.

Esempio 4.9. Se $G = (\mathbb{Z}, +)$ e $H = n\mathbb{Z}$ allora $[G : H] = n$. se $G = (\mathbb{R}, +)$ e $H = \mathbb{Z}$ allora $[G : H]$ è infinito.

Teorema 4.10. *(Lagrange) Sia H un sottogruppo di un gruppo finito G. Allora*

$$|G| = [G : H]|H|$$

Dimostrazione. Per la Proposizione (4.7), ogni classe di equivalenza $[a] = aH$ ha cardinalità $|H| \leq |G| < \infty$. Poiché $\sim$ è una relazione di equivalenza, G è una unione disgiunta di classi di equivalenza. Allora, $|G| = [G : H]|H|$ poiché ci sono $[G : H]$ cosets.

C.V.D.

Corollary 4.11. *Sia g un elemento di un gruppo finito G. Allora, ord(g) divide ord$(G) = |G|$.*

Dimostrazione. $\text{ord}(g) = |\langle g \rangle$ e $H = \langle g \rangle$ è un sottogruppo di G. Quindi,

$$|G| = [G : H]|H| \implies \text{ord}(g)|\text{ord}(G)$$

C.V.D.

Nota 4.12. Il viceversa del teorema di Lagrange è falso: Il fatto che d sia un divisore di ord(G) non vuol dire che G ha un elemento di ordine d. Notiamo anche che che, per definizione, un gruppo finito G ha elemento di ordine $|G|$ se e solo se G è ciclico.

Esempio 4.13. Sia $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Allora,

$$\text{ord}((0,0)) = 1, \qquad \text{ord}((1,0)) = \text{ord}((0,1)) = 2$$

In particolare G non ha alcun elemento di ordine $|G| = 4$.

Corollary 4.14. *Sia p un primo e G un gruppo di ordine p. Allora, G è isomorfo a $(\mathbb{Z}_p, +)$.*

Dimostrazione. Sia $g \in G - \{e\}$. Per il teorema di Lagrange, ord(g) divide ord$(G) = p$. Allora, ord$(g) = 1$ o ord$(g) = p$. Poiché $g \neq e$, ord$(g) \neq 1$, e quindi $\langle g \rangle$ ha ordine p. In altre parole, $\langle g \rangle = G$. Come tale, $f(r) = g^r$ definisce un isomorfismo da $(\mathbb{Z}_p, +)$ a G.

C.V.D.

Corollary 4.15. *(Piccolo teorema di Fermat) Se p è un primo allora $U(p) = \mathbb{Z}_p - \{0\}$ è il gruppo di unità in $\mathbb{Z}_p$ rispetto alla moltiplicazione. Quindi, $[a] \in \mathbb{Z}_p - \{0\}$ implica che ord$([a])$ divide ord$(U(p)) = p - 1$. In altre parole, $[a]^{p-1} = [1]$, che implica $a^{p-1} \equiv 1 \mod p$. Moltiplicando per a, otteniamo $a^p - a \equiv 0 \mod p$.*

Corollary 4.16. *(Teorema di Eulero) Denotiamo con $U(n)$ il gruppo di unità $\mathbb{Z}_n$ rispetto alla moltiplicazione. Allora, ord$(U(n)) = \phi(n)$. Se $\text{mcd}(a, n) = 1$ allora $[a] \in U(n)$ e quindi $[a]^{\phi(n)} = [1]$.*

Continuando, ricordiamo che una coppia di matrici A e B di tipo $n \times n$ sono simili se e solo se esiste una matrice invertibile C di tipo $n \times n$ tale che $A = CBC^{-1}$. Più generalmente, se G è un gruppo, diciamo che $x, y \in G$ sono coniugati se esiste un elemento $g \in G$ tale che $x = gyg^{-1}$. In questo caso, scriviamo $x \simeq y$.

Proposizione 4.17. *$\simeq$ è una relazione di equivalenza.*

Dimostrazione.

- $x \simeq x$: $x = exe^{-1}$.
- $x \simeq y \implies y \simeq x$: $x = gyg^{-1} \implies g^{-1}xg = y \implies y = (g^{-1})x(g^{-1})^{-1}$.
- $x \simeq y, y \simeq z \implies x \simeq z$: $x \simeq y \implies x = gyg^{-1}, y \simeq z \implies y = hzh^{-1}$. allora,

$$x = gyg^{-1} = ghzh^{-1}g^{-1} = (gh)z(gh)^{-1} \implies x \simeq z$$

C.V.D.

Denotiamo con $\mathrm{Cl}(x)$ la classe di equivalenza di $x \in G$ via $\simeq$. Questa è chiamata di solito la classe di coniugio di x.

Esempio 4.18. Sia G il gruppo di matrici unitarie di ordine n.Allora, per il teorema spettrale, ogni elemento $A \in G$ è unitariamente simile a una matrice diagonale. In altre parole, c'è una matrice unitaria U tale che $UAU^{-1} = D$ è una matrice diagonale. Quindi, ogni classe di coniugio $\mathrm{Cl}(A)$ ha un unica rappresentante D che è diagonale.

Esempio 4.19. Sia G un gruppo, e supponiamo che $x \in G$ e $|\mathrm{Cl}(x)| = 1$. Allora, $gxg^{-1} = x$ per ogni elemento $g \in G$. In altre parole, x commuta con ogni elemento di G. L'insieme

$$Z(G) = \{x \in G \mid gx = xg \ \ \forall g \in G\}$$

è chiamato il centro di G. $Z(G)$ è un sottogruppo di G. (Esercizio per la studentessa).

In particolare, poiché $\simeq$ è una relazione di equivalenza, quando G è finto, esiste una collezione finita di elementi $x_1, \ldots, x_n \in G$ tale che

$$|G| = \mathrm{Cl}(x_1) \cup \mathrm{Cl}(x_2) \cup \cdots \cup \mathrm{Cl}(x_n) \tag{4.20}$$

dove $\mathrm{Cl}(x_i) \cap \mathrm{Cl}(x_j) = \emptyset$ se $i \neq j$. In luce dell'esempio precedente, possiamo raffinare (4.20) a

$$|G| = Z(G) \cup \left(\bigcup_{|\mathrm{Cl}(x_j)|>1} \mathrm{Cl}(x_j) \right) \tag{4.21}$$

Per calcolare la cardinalità di $\mathrm{Cl}(x)$ quando $x \notin Z(G)$, notiamo che abbiamo una mappa suriettiva

$$f : G \to \mathrm{Cl}(x), \qquad f(g) = gxg^{-1}$$

Supponiamo che $f(g) = f(h)$. Allora,

$$gxg^{-1} = hxh^{-1} \implies x = (g^{-1}h)x(h^{-1}g) \implies x = (g^{-1}h)x(g^{-1}h)^{-1}$$

e quindi $g^{-1}h$ appartiene al centralizzante $C(x)$ di x (vedi l'equazione (2.21)). Quindi, f determina una mappa biettiva (PERCHÉ SURIETTIVA E INIETTIVA) (*)

$$F : G/C(x) \to \mathrm{Cl}(x), \qquad F(gC(x)) = gxg^{-1}$$

e quindi (se G è finito)

$$|\mathrm{Cl}(x)| = |G/C(x)| = [G : C(x)]$$

In particolare, per il teorema di Lagrange, $|\mathrm{Cl}(x)|$ è un divisore di $|G|$.

Teorema 4.22. *(Formula delle Classi di Coniugio): Sia G un gruppo finito. Allora,* (4.21) *può essere riscritto nella forma seguente,*

$$|G| = |Z(G)| + \sum_{|Cl(x_j)|>1} [G : C(x_i)]$$

(*) $|Cl(x)| = |G/C(x)| < \infty$
$\Rightarrow$ INIETTIVA È EQUIV. A BIETTIVA

DIM. CHE È UNA BIGEZIONE:
$F([g]) = F([g']) \Rightarrow gxg^{-1} = g'x(g')^{-1} \Rightarrow (g')^{-1}gx = x(g')^{-1}g$
$\Rightarrow (g')^{-1}g = c \in C(x) \Rightarrow g = g'c$
$\Rightarrow gC(x) = g'C(x)$, cioè $[g] = [g']$

che è di solito chiamata la formula delle classi di coniugio di G.

Una applicazione di base della formula delle classi è dimostrare che il numero di classi di coniugio limita l'ordine del gruppo. Per questo, torniamo a (4.20) e dividiamo l'equazione per $|G|$ e usiamo $|G| = [G : \mathrm{Cl}(x)]|C(x)|$ per ottenere

$$1 = \sum_{j=1}^{n} \frac{1}{|C(x_j)|} \tag{4.23}$$

Inoltre, $C(e) = G$, quindi $1/|G|$ appare come la più piccola frazione in (4.23).

Supponiamo adesso di sapere solo che G è un gruppo che ha $n > 1$ classi di coniugio. allora, possiamo considerare tutte le possibili soluzioni dell'equazione

$$1 = \sum_{j=1}^{n} \frac{1}{a_j} \tag{4.24}$$

dove ciascun $a_j > 1$ è un intero. Per un fissato valore di n, c'è solo un numero finito di soluzioni di (4.24), e il valore più grande di a_j che appare è un limite sull'ordine di G.

Esempio 4.25. Se $n = 3$, le uniche possibili soluzioni sono

$$1 = \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{4}\right) = \left(\frac{1}{3} + \frac{1}{3} + \frac{1}{3}\right) = \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6}\right)$$

allora, 6 è il più grande possibile ordine di un gruppo che ha solo 3 classi di coniugio.

Esempio 4.26. Il più piccolo gruppo non abeliano è S_3, che ha 6 elementi, ed è isomorfo al gruppo di matrici listato nell'Esercizio 1. In questo caso, un calcolo diretto mostra che $\mathrm{Cl}(T_1) = \{T_1, T_2, T_3\}$. Similmente $\mathrm{Cl}(I) = \{I\}$. allora, per l'equazione delle classi abbiamo

$$6 = 1 + 3 + |\mathrm{Cl}(x_1)| + \cdots$$

Le rimanenti possibilità sono $\mathrm{Cl}(R_1) = \{R_1, R_2\}$ o $\mathrm{Cl}(R_j) = \{R_j\}$, nel cui caso $R_j \in Z(S_3)$ che è falso.

Proposizione 4.27. *Sia p un primo e G un gruppo di ordine $p^r > 1$. allora, $Z(G) \neq \{e\}$.*

Dimostrazione. se $r = 1$ allora $G \cong \mathbb{Z}_p$ e $Z(G) = G$. Supponiamo allora che $r > 1$ e $Z(G) = \{e\}$. Sia $g \in G - Z(G)$. Allora $\mathrm{Cl}(g) \neq 1$ e è un divisore di $|G| = p^r$. Quindi, $|\mathrm{Cl}(g)| = p^j$ per qualche $j > 0$. Poiché g era un elemento arbitrario di $G - Z(G)$, dalla formula delle classi segue che

$$p^r = |G| = |Z(G)| + |\mathrm{Cl}(g_1)| + \cdots + |\mathrm{Cl}(g_r)| = 1 + pk$$

per qualche intero k poiché ciascun $|\mathrm{Cl}(g_i)| > 1$ è una potenza di p. Ma,

$$p^r = 1 + kp \implies kp = p^r - 1 = (p-1)(1 + p + \cdots + p^{r-1})$$

e quindi

$$p|kp \implies p|(p-1)(1 + p + \cdots + p^{r-1}) \implies (p|p-1 \ \ o \ \ p|1 + p + \cdots + p^{r-1}) \implies p| \pm 1$$

che è un contraddizione. E allora, $|Z(G)| \neq 1$.

C.V.D.

Esercizi

Esercizio 18. Quali sono i possibili ordini degli elementi di un gruppo di ordine 60?

Esercizio 19. Mostra che $Z(G)$ è un sottogruppo di G.

Esercizio 20. Qual'è il massimo ordine possibile di un gruppo G che ha solo 4 classi di coniugio? *Suggerimento*: Per la formula delle classi,

$$1 = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \frac{1}{n_4}$$

che possiamo ordinare come $2 \leq n_1 \leq n_2 \leq n_3 \leq n_4$. Allora, $1 \leq 4/n_1$ poiché $n_j \geq n_1 \implies 1/n_j \leq 1/n_1$, e quindi $n_1 \in \{2, 3, 4\}$.

Esercizio 21. Sia p un primo e G be un gruppo di ordine p^2. Se G ha un elemento di ordine p^2 allora $\mathbb{Z}_{p^2}$. Altrimenti, possiamo scegliere $u \in Z(G) - \{e\}$ e $v \in G - \{e, u\}$ (perché?). Mostra che la mappa

$$f : \mathbb{Z}_p \times \mathbb{Z}_p \to G, \qquad f(j, k) = u^j v^k$$

è un isomorfismo, (Parte dell'esercizio è di mostrare che f è ben definita).

Esercizio 22. Sia G il gruppo di movimenti rigidi che preservano un quadrato S in $\mathbb{R}^2$ con vertici $\{(\pm 1, \pm 1)\}$. Allora, G è di ordine 8, ed è isomorfo al gruppo di matrici:

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad r^2 = -e, \quad r^3 = -r$$

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad rs = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad -s, \quad -rs$$

Mostra che l'equazione delle classi di G è $|G| = 2 + 2 + 2 + 2$.

5. Omomorfismos e Gruppi Quoziente

Se U e V sono spazi vettoriali, allora $f : U \to V$ è una mappa lineare se e solo se $f(cu) = cf(u)$ e $f(u_1 + u_2) = f(u_1) + f(u_2)$. Il concetto analogo per gruppi è:

Definizione 5.1. Siano G e H gruppi. Allora, una mappa $f : G \to H$ è un omomorfismo di gruppi se e solo se $f(g_1 g_2) = f(g_1) f(g_2)$ per ogni $g_1, g_2 \in G$.

Analizzando la definizione (3.2), vediamo che un isomorfismo di gruppi è la stessa cosa di un omomorfismo biettivo.

Esempio 5.2. Sia $L : U \to V$ una mappa lineare tra spazi vettoriali. Allora, L è anche un omomorfismo di gruppi da $(U, +)$ a $(V, +)$.

Esempio 5.3. Se S è un sottogruppo di G, allora la mappa inclusione $i : S \to G$, $i(s) = s$ è un omomorfismo di gruppi. ($i(s_1 s_2) = i(s_1) i(s_2) = s_1 s_2$)

Esempio 5.4. Sia $K = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Allora, $K^* = GL_1(K)$ è il gruppo moltiplicativo di elementi non nulli di K. Per la formula di Binet, $\det : GL_n(K) \to K^*$ è un omomorfismo di gruppi. $D(A) = \det(A) \neq 0$ PERCHÉ LE MAT. SONO INVERTIBILI
$D(AB) = \det(AB) = \det(A)\det(B) = D(A)D(B)$ PER BINET

Esempio 5.5. Sia S_n il gruppo di permutazioni di $\{1, \ldots, n\}$ e $e_1, \ldots, e_n$ la base standard di $\mathbb{R}^n$. Dato $\sigma \in S_n$ sia $L_\sigma : \mathbb{R}^n \to \mathbb{R}^n$ la mappa lineare definita da

$$L_\sigma(e_i) = e_{\sigma(i)}$$

Allora, L_σ è invertibile, e $f : S_n \to GL_n(\mathbb{R})$ definita da $f(\sigma)$ sia la matrice di L_σ rispetto a $\{e_1, \ldots, e_n\}$ è un omomorfismo di gruppi.

Proposizione 5.6. *Se $f : G \to H$ è un omomorfismo di gruppi allora $f(e_G) = e_H$ e $f(g^{-1}) = f(g)^{-1}$.*

Dimostrazione.

$$e_G = e_G e_G \implies f(e_G) = f(e_G)f(e_G) \implies f(e_G)f(e_G)^{-1} = f(e_g)f(e_g)f(e_g)^{-1} \implies e_H = f(e_G).$$

La dimostrazione che $f(g^{-1}) = f(g)^{-1}$ è un esercizio per lo studente.

C.V.D.

Se $L : U \to V$ è una mappa lineare allora $\ker(L)$ è un sottospazio di U e $\mathrm{Im}(L)$ è un sottospazio di V. Lo stesso è vero di omomorfismi di gruppi:

Proposizione 5.7. *Sia $f : G \to H$ be un omomorfismo di gruppi. Allora, $\ker(f) = f^{-1}(e_H)$ è un sottogruppo di G e $Im(f)$ è un sottogruppo di H.*

Dimostrazione. Per il Lemma (2.6), dobbiamo mostrare che $\ker(f)$ e $\mathrm{Im}(f)$ sono non vuoti e chiusi per l'operazione $a, b \mapsto a^{-1}b$.

- $\ker(f)$ è un sottogruppo di G poiché $e_G \in \ker(f)$ e

$$\begin{aligned} a, b \in \ker(f) &\implies f(a^{-1}b) = f(a^{-1})f(b) = f(a)^{-1}f(b) = e_H\, e_H = e_H \\ &\implies a^{-1}b \ker(f) \end{aligned}$$

- $\mathrm{Im}(f)$ è un sottogruppo di H: poiché $e_H = f(e_G) \in H$ e

$$\begin{aligned} a = f(\alpha), b = f(\beta) \in \mathrm{Im}(f) &\implies a^{-1}b = f(\alpha)^{-1}f(\beta) = f(\alpha^{-1})f(\beta) = f(\alpha^{-1}\beta) \\ &\implies a^{-1}b \in \mathrm{Im}(f) \end{aligned}$$

C.V.D.

Esempio 5.8. Il kernel di $\det : GL_n(K) \to K^*$ sono le matrici con determinante 1. L'immagine di $\det$ è K^*: Considera la matrice $A = (a_{ij})$ tali che $a_{11} = \alpha$, $a_{jj} = 1$ per $i > 1$ e $a_{ij} = 0$ altrimenti. Allora, $\det(A) = \alpha$.

Esempio 5.9. Sia $f : S_n \to GL_n(\mathbb{R})$ l'omomorfismo definito nell'Esempio (5.5). Allora, $\ker(f)$ è la permutazione identità. L'immagine di f, è il gruppo di $n \times n$ matrici permutazioni Perm_n. La mappa $f : S_n \to \mathrm{Perm}_n$ è un isomorfismo.

Sia $P = f(\sigma)$ una matrice permutazione. Allora,

$$(PP^t)_{ij} = \sum_k P_{ik}(P^t)_{kj} = \sum_k P_{ik}P_{jk}$$

Poiché P è una matrice permutazione $P_{uv} = 0$ a meno che $u = \sigma(v)$. allora, $P_{ik}P_{jk} = 0$ a meno che $i = j$. Di conseguenza, $PP^t = I$ da cui si deduce che $\det(P) = \pm 1$.

Esempio 5.10. L'insieme $\{-1, +1\}$ è un gruppo rispetto a moltiplicazione, che è isomorfo al $\mathbb{Z}_2$ tramite la mappa $\mathbb{Z}_2 \to \{-1, 1\}$ data da $j \mapsto (-1)^j$. La mappa $\det : \mathrm{Perm}_n \to \{-1, 1\}$ è un omomorfismo, che è solitamente chiamato il segno della permutazione. Il sottogruppo di permutazioni nel kernel è chiamato gruppo alternato.

Nella sezione precedente, abbiamo visto che è dato un sottogruppo H di G, potremmo formare lo spazio G/H (cosets, classi laterali). In molti esempi, tale come spazio vettoriale quoziente V/U e $\mathbb{Z}/n\mathbb{Z}$, G/H ha anche la struttura di un gruppo.

Se R e S are sottoinsiemi di un gruppo G definiamo

$$RS = \{rs \mid r \in R,\, s \in S\}$$

In particolare, se H è un sottogruppo di G allora $HH = H$ poiché H è chiuso per la moltiplicazione di gruppo.

La regola ovvia per definire una struttura di gruppo su G/H è

$$(aH)(bH) = (ab)H \tag{5.11}$$

se G è un gruppo abeliano, allora questa formula funziona per definire un prodotto poiché possiamo semplicemente muovere b dopo H. Quando G non è abeliano questa definizione non sempre funziona.

Definizione 5.12. Sia H un sottogruppo di G. Allora, H è un sottogruppo normale di G se e solo se $gHg^{-1} = H$ per ogni $g \in G$. In questo caso, scriviamo $H \lhd G$.

Esempio 5.13. Sia H un sottogruppo di G. Se $[G : H] = 2$ allora H è un sottogruppo normale di G. Ovvero, se $g \in H$ allora $ghg^{-1} \in H$ poiché H è un sottogruppo di G. Supponiamo ora che $g \in G - H$. Allora,

$$[G : H] = 2 \implies G = gH \cup H, \qquad gH \cap H = \emptyset$$

Supponiamo ora che anche g' è un elemento di $G - H$. Se $gg' \notin H$ allora $gg' = gh$ per qualche elemento di H, e quindi $g' = h \in H$, che è un contraddizione. Per finire la dimostrazione, sia h un elemento arbitrario di H e sia $g' = hg^{-1}$. Se $g' \in H$ allora anche g lo è poiché H è chiuso per inversi. Allora, $gg' = ghg^{-1} \in H$.

Se H è un sottogruppo normale di G allora

$$(aH)(bH) = a(bHb^{-1})(bH) = (abH)(b^{-1}bH) = (abH)H = abH$$

e (5.11) definisce un'operazione binaria su G/H. Poiché G è un gruppo, questa operazione è asssociativa. Similmente, $eH = H$ è l'identità e $(aH)(a^{-1}H) = H$.

Teorema 5.14. *Sia H un sottogruppo di G. Allora,* (5.11) *definisce una struttura di gruppo sul G/H se e solo se H è un sottogruppo normale di G.*

Dimostrazione. Se H è un sottogruppo normale di G allora G/H has una struttura di gruppo come indicato sopra. Se (5.11) definisce una struttura di gruppo allora $H = (aa^{-1}H) = (aH)(a^{-1}H) \implies H = aHa^{-1}$.

C.V.D.

Lemma 5.15. *Sia $f : G \to H$ un omomorfismo di gruppi. Allora, $\ker(f)$ è un sottogruppo normale di G.*

Dimostrazione. sia $k \in \ker(f)$ e $g \in G$. Allora,

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)e_H f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$$

e quindi $gkg^{-1} \in \ker(f)$.

C.V.D.

Lemma 5.16. *Sia $f : G \to H$ be un omomorfismo di gruppi e $K = \ker(f)$. Allora, G/K è isomorfo al Im(f).*

Dimostrazione. Sia $g \in G$ e $k \in K$. Allora, $f(gk) = f(g)f(k) = f(g)$. Allora

$$F : G/K \to H, \qquad F(gK) = f(g)$$

è ben definita, e $\mathrm{Im}(F) = \mathrm{Im}(f)$. Inoltre, $F(gK) = F(gK') \iff f(g) = f(g')$ e

$$f(g) = f(g') \implies e_H = f(g)^{-1}f(g') = f(g^{-1}g') \implies g^{-1}g' \in K \implies gK = g'K$$

Allora, F è una biezione da G/K a $\mathrm{Im}(f)$. Infine, poiché K è un sottogruppo normale di G,

$$F((gK)(g'K)) = F(gg'K) = f(gg') = f(g)f(g') = F(gK)F(g'K)$$

e quindi F è un omomorfismo.

C.V.D.

Ci sono altri tre teoremi standard di isomorfismo per gruppi, che hanno analoghi per anelli commutativi con identità, quindi discuteremo quei teoremi nella lezione su anelli commutativi con identità.

Per chiudere questa sezione, ora presentiamo un passo chiave nella dimostrazione del teorema del fattore invariante per gruppi abeliani finiti:

Proposizione 5.17. *Sia A un gruppo abeliano finito e p un fattore primo di $|A|$. Allora, A ha un elemento di ordine p.*

Dimostrazione. Sia $P(q)$ l'affermazione che se $|A| = pq$ con $q \geq 1$ allora A contiene un elemento di ordine p. Allora, la proposizion può essere dimostrata per induzione su q come segue:

- $P(1)$: $P(1)$: Questo è vero perché $|A| = p$ e quindi $A \cong \mathbb{Z}_p$ che è ciclico di ordine p.
- $P(1), \ldots, P(q) \implies P(q+1)$: Sia $a \in A$ un elemento di ordine $d > 1$. Se p è un fattore primo di d allora $a^{d/p}$ è un elemento di ordine p.

  Supponiamo quindi che p non sia un fattore primo di d. Di Teorema di Lagrange, $d|p(q+1)$ e quindi $d|(q+1)$. Sia $C = \langle a \rangle$ e $q' = (q+1)/d$. Poiché A è un gruppo abeliano di ordine $p(q+1)$, A/C è un gruppo abeliano di ordine pq' dove $q' < q+1$. Pertanto, per l'ipotesi di induzione, A/C ha un elemento (non-identità) y di ordine p. Sia $f : A \to A/C$ l'omomorfismo quoziente. Poiché f è suriettiva, ecco esiste un elemento $x \in A$ tale che $f(x) = y$.

  Sia $v > 0$ l'ordine di x, e scriviamo $v = pu + r$ dove $0 \leq r < p$. Allora,

  $$f(e) = f(x^v) = f(x)^v = y^v = y^{pq+r} = y^r$$

  è l'elemento di identità di A/C. Dunque $r = 0$ perché y ha ordine p. Pertanto $p|x$ e quindi $x^{v/p} \in A$ è un elemento di ordine p.

C.V.D.

Nota 5.18. In fatti, il teorema di Cauchy per gruppi finiti afferma che se p è un fattore dell'ordine di un gruppo finito G allora G contiene un elemento di ordine p. I teoremi di Sylow teoremas affermano che p^n è la massima potenza di p che divide $|G|$, e allora G has a sottogruppo di ordine p^n.

Esercizi

♉ **Esercizio 23.** Verifica che se $f : G \to H$ e $g : H \to K$ sono un gruppo homomorphisms allora $g \circ f : G \to K$ è un omomorfismo di gruppo. Quando $H = G$ scriviamo f^k per la composizione di f con se stessa k volte.

♉ **Esercizio 24.** Sia A un gruppo abeliano e n un numero intero positivo. Mostra che $f(a) = a^n$ (o $f(a) = na$ se scritto in modo additivo) è un gruppo omomorfismo.

♊ **Esercizio 25.** Sia A un gruppo abeliano finito. Sia $f : A \to A$ a omomorfismo. Quindi, il teorema di decomposizione di Fitting dice che c'è esiste un intero positivo k tale che $A = \ker(f^k) \times \mathrm{Im}(f^k)$.

- Verifica il teorema di decomposizione di Fitting per il gruppo $\mathbb{Z}_{36}$ e l'omomorfismo $f(x) = 3x$.
- Se p è un fattore primo di $|A|$ $\in f(x) = px$ mostrare che $\ker(f^j) \neq \{e\}$ per tutti $j > 0$.

♉ **Esercizio 26.** Mostra che se H e K sono normali sottogruppi di G allora

$$HK = \{hk \mid h \in H, \ \ k \in K\}$$

è un normale sottogruppo di G.

♊ **Esercizio 27.** Sia G un gruppo finito. Mostra che se H e K sono sottogruppi normali tali che $|G| = |H||K|$ e $\mathrm{mcd}(|H|, |K|) = 1$ allora $HK = G$.

♉ **Esercizio 28.** Mostra che nel contesto del problema precedente, se $hk = kh$ per tutti $h \in H$ e $k \in K$ quindi $f : H \times K \in G$ dati per $f(hk) = hk$ è un isomorfismo di gruppo.

ESERCIZIO 1

Dim. che le seguenti 6 matrici formano un gruppo rispetto alla moltiplicazione di matrici.

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad T_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

NOTA: le mat. sono uguali a meno di perm. di righe

ASSOCIATIVITÀ: $(T_1 T_2) T_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

$$\parallel \quad \checkmark$$

$$T_1 (T_2 T_3) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

IDENTITÀ: $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

INVERSO: $\left(\overbrace{\begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{matrix}}^{T_1} \middle| \overbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}^{I}\right) \xrightarrow{R_1 = R_1 + R_2} \left(\begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{matrix} \middle| \begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}\right) \xrightarrow{R_2 = R_2 - R_1}$

$$\left(\begin{matrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{matrix} \middle| \begin{matrix} 1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{matrix}\right) \xrightarrow{R_2 = R_2 \cdot -1} \left(\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \middle| \begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{matrix}\right) \xrightarrow{R_1 = R_1 - R_2}$$

$$\left(\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \middle| \underbrace{\begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{matrix}}_{T_1^{-1}}\right)$$

ESERCIZIO 2

Dim. che l'insieme di elementi unità in $\mathbb{Z}_n$ rispetto alla moltiplicazione mod n forma un gruppo.

$U_n = \{\text{unità in } \mathbb{Z}_n\}$

Siano $a, b \in U_n$.

Allora a ha un inverso molt. a^{-1}, così come b (b^{-1}).

$$\left.\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b = b^{-1}b = 1\\ (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} = aa^{-1} = 1\end{aligned}\right\} \Rightarrow a, b \in U_n \Rightarrow ab \in U_n$$

ASSOCIATIVITÀ: $a(bc) = ab(c)$

IDENTITÀ: $1 \in U_n$

INVERSO: $\exists$ per def. perché gli elem. di U_n sono unità

ESERCIZIO 3

Sia G un gruppo e $g \in G$.

Dim. che $(g^{-1})^{-1} = g$.

$gg^{-1} = g^{-1}g = e$ perché g^{-1} è l'inverso di g

$\Rightarrow$ g è l'inverso di g^{-1}, cioè $g = (g^{-1})^{-1}$

ESERCIZIO 4

Sia G un gruppo con elemento identità e.

Dim. che e è unico.

Supponiamo per assurdo che esistono due id. in G: e, e'

$\Rightarrow$ $\forall g \in G \quad g \cdot e = e \cdot g = g$

$\forall g \in G \quad g \cdot e' = e' \cdot g = g$

$\Rightarrow$ $\cancel{g} \cdot e = \cancel{g} \cdot e' \Rightarrow e = e'$

ESERCIZIO 5

Sia G un gruppo e $a \in G$.
Dim. che a^{-1} è unico.

Sia $a \in G$, a^{-1} e b^{-1} entrambi inversi di a.
$a^{-1} = a^{-1} \cdot e = a^{-1}(a \cdot b^{-1}) = (a^{-1} \cdot a) b^{-1} = e \cdot b^{-1} = b^{-1}$
$\Rightarrow a^{-1} = b^{-1}$

ESERCIZIO 6

Dim. che gli interi non neg. non formano un gruppo rispetto all'addizione.

Affinché $\mathbb{N}^*$ formi un gruppo rispetto all'addizione deve esistere l'inverso per ogni elemento:
$\forall a \in \mathbb{N}^* \; \exists b \in \mathbb{N}^*$ t.c. $a + b = e = 0 = b + a$
ma $a + b = 0 \Rightarrow b = -a \notin \mathbb{N}^*$, inoltre $0 \notin \mathbb{N}^*$
$\therefore$ $\mathbb{N}^*$ non ha gli inversi e non ha l'identità

ESERCIZIO 7

Dim. che la tavola di moltipl. per la morra cinese non è associativa.

$T = \{C, F, S\}$, $* : T \times T \to T$

*	C	F	S
C	C	F	C
F	F	F	S
S	C	S	S

$(CF)S = FS = S$
$C(FS) = CS = C$
$\neq$

ESERCIZIO 8

Dim. che gli interi non formano un gruppo rispetto alla sottrazione $a * b = a - b$

$\mathbb{Z}$ non forma un gruppo rispetto alla sottrazione perché non vale la propr. associativa, infatti:

Siano $a, b, c \in \mathbb{Z}$

$$\left.\begin{aligned}(a-b)-c &= (a+(-b))+(-c) = a+(-b)+(-c)\\ a-(b-c) &= a+(-(b+(-c))) = a+(-b)+c\end{aligned}\right\} \neq$$

ESERCIZIO 9

Dim. il seguente lemma:

Siano H e K sottogruppi di G.

Allora $H \cap K$ è un sottogruppo di G.

<u>DIM</u>

H sottogruppo di $G \Rightarrow e \in H$

K sottogruppo di $G \Rightarrow e \in K$

$\Rightarrow e \in H \cap K \Rightarrow H \cap K \neq \emptyset$ ($\therefore H \cap K$ contiene l'identità e)

Siano $x, y \in H \cap K$

$\Rightarrow x, y \in H,\ x, y \in K$

H sottogruppo di $G \Rightarrow H$ chiuso rispetto all'operazione su G

$\Rightarrow xy \in H$

K sottogruppo di $G \Rightarrow K$ chiuso rispetto all'operazione su G

$\Rightarrow xy \in K$

$\Rightarrow xy \in H \cap K$ ($\therefore H \cap K$ è chiuso rispetto all'op. su G)

Sia $z \in H \cap K$.

$\Rightarrow z \in H,\ z \in K$

H sottogruppo di $G \Rightarrow H$ chiuso rispetto agli inversi

$\Rightarrow z^{-1} \in H$

K sottogruppo di $G \Rightarrow K$ chiuso rispetto agli inversi

$\Rightarrow z^{-1} \in K$

$\Rightarrow z^{-1} \in H \cap K$ ($\therefore H \cap K$ è chiuso rispetto agli inversi)

$\Rightarrow H \cap K$ è un sottogruppo di G

$\square$

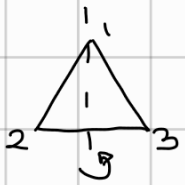
ESERCIZIO 10

Trovare un elemento di ordine 2 e un elemento di ordine 3 tra le seguenti matrici:

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad T_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

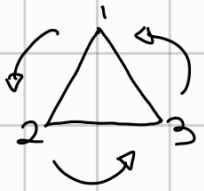
T_3 ha ordine 2 perché:



$\sigma : \{1,3,2\} \to \{1,2,3\}$

$ord(\sigma) = |\langle \sigma \rangle| = |\{\sigma, \sigma^2 = I\}| = 2$

R_2 ha ordine 3 perché:



$\rho : \{2,3,1\} \to \{1,2,3\}$

$ord(\rho) = |\langle \rho \rangle| = |\{\rho, \rho^2, \rho^3 = I\}| = 3$

ESERCIZIO 11

Descrivere il centralizzante dell' esempio (2.22) in termini di condizioni algebriche sulle entrate della matrice A.

$G = SL_2(\mathbb{R})$ = insieme delle mat. invertibili 2×2 a coeff. reali

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} ; \quad C(X) = \{A \in G : AX = XA\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \Rightarrow \begin{cases} b = -c \\ -a = -d \\ d = a \\ -c = b \end{cases} \Rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

$$\Rightarrow \det\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 = 1$$

ESERCIZIO 12

Dim. il seguente lemma:

Sia H un sottogruppo di $(G, *)$.

Allora H è un gruppo rispetto alla restrizione di $*$ ad H.

<u>DIM</u>

Dobbiamo dim. che $(H, *_H)$ è un gruppo dove $*_H$ è definita come $*_H : H \times H \to H$.

- H sottogruppo di $(G, *) \Rightarrow *_H$ è associativa
- H sottogruppo di $(G, *) \overset{\text{PER DEF.}}{\Rightarrow} a \in H \Rightarrow a^{-1} \in H$
- $\exists e \in H$ t.c. $e = a *_H a^{-1} \in H \quad \forall a \in H$ $\square$

ESERCIZIO 13

Usa il th della divisione e il principio di buon ordinamento per mostrare che ogni sottogruppo di $(\mathbb{Z}, +)$ è della forma $n\mathbb{Z}$.

Supponiamo che $H \leq \mathbb{Z}$ sia un sottogruppo.

$H = \{0\} \Rightarrow H = 0\mathbb{Z}$

Supponiamo quindi $H \neq \{0\}$.

Per il principio del buon ordinamento:

$\exists n \in H, n \neq 0$ t.c. n è minimo

Poiché H è un sottogruppo, tutti i multipli di n devono $\in H$

$\Rightarrow n\mathbb{Z} \subset H$

Supponiamo $\exists m \in H$ t.c. $m \notin n\mathbb{Z}$

Per il th della divisione, $\exists q, r \in \mathbb{Z}$ t.c. $m = qn + r$, $0 \leq r < n$

$m \notin n\mathbb{Z} \Rightarrow r \neq 0$

$m \in H, qn \in H \Rightarrow -qn \in H \Rightarrow m - qn \in H \Rightarrow r \in H$

ma $r < n$ contraddice la minimalità di $m \Rightarrow \nexists m$

$\Rightarrow H = n\mathbb{Z}$

ESERCIZIO 14

Dim. la seguente proposizione:

Siano H e K dei gruppi.

Allora, $H \times K$ é un gruppo rispetto all'operazione binaria $(h_1, k_1) * (h_2, k_2) = (h_1 h_2, k_1 k_2)$ con elemento identitá $e = (e_H, e_K)$.

Se H e K sono gruppi finiti, allora $ord(H \times K) = ord(H) \cdot ord(K)$

Altrimenti $H \times K$ ha ordine infinito.

DIM

- H, K gruppi $\Rightarrow H \times K$ gruppo rispetto a $*$

  i) $((h_1, k_1)(h_2, k_2))(h_3, k_3) = (h_1 h_2, k_1 k_2)(h_3 k_3) =$
  $= (h_1 h_2 h_3, k_1 k_2 k_3)$

  $(h_1, k_1)((h_2, k_2)(h_3, k_3)) = (h_1, k_1)(h_2 h_3, k_2 k_3) =$
  $= (h_1 h_2 h_3, k_1 k_2 k_3)$

  $= \checkmark$

  ii) $(e_H, e_K)(h_1, k_1) = (h_1, k_1)(e_H, e_K) = (h_1, k_1)$ $\checkmark$

  iii) $(h_1, k_1)(h_1, k_1)^{-1} = (h_1, k_1)^{-1}(h_1, k_1) = (e_H, e_K)$ $\checkmark$

- H, K gruppi finiti $\Rightarrow ord(H \times K) = ord(H) \times ord(K)$

  $H \times K = \{(h, k) : h \in H, k \in K\}$

  Si hanno $\binom{ord(H)}{1} = ord(H)$ scelte per h e $\binom{ord(K)}{1} = ord(K)$ scelte per K.

  Le scelte di h e K sono indipendenti, quindi possiamo moltiplicare: $ord(H) \cdot ord(K)$.

  $\Rightarrow ord(H \times K) = ord(H) \cdot ord(K)$

$\square$

ESERCIZIO 15

Determina tutti i possibili fattori invarianti di gruppi abeliani di ordine 144 e 360.

$n = 144 = 2^4 \cdot 3^2 \Rightarrow$ $4, 3+1, 2+2, 2+1+1, 1+1+1+1$
$2, 1+1$ $\Big\} \Rightarrow$ ci sono $5 \cdot 2 = 10$ gruppi di ordine 144

144	2
72	2
36	2
18	2
9	3
3	3
1	

FATTORI INVARIANTI:

$(144), (72,2), (36,4), (36,2,2),$
$(18,2,2,2), (12,12), (24,6), (48,3),$
$(6,6,2,2), (12,6,2)$

$n = 360 = 3^2 \cdot 2^3 \cdot 5 \Rightarrow$ $2, 1+1$
$3, 2+1, 1+1+1$ $\Big\} \Rightarrow$ ci sono $3 \cdot 2 = 6$ gruppi di ordine 360

360	2
180	2
90	2
45	5
9	3
3	3
1	

FATTORI INVARIANTI:

$(360), (180,2), (90,2,2), (120,3),$
$(60,6), (30,6,2)$

ESERCIZIO 16

Verifica che $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f([x]_{mn}) = ([x]_m, [x]_n)$ soddisfa $f(u+v) = f(u) + f(v)$.

Supponiamo che $x \equiv x' \bmod mn$.

$\Rightarrow x' = x + \alpha mn \Rightarrow x' \equiv x \bmod m \Rightarrow x' \equiv x \bmod n$

Supponiamo che $y \equiv y' \bmod mn$

$\Rightarrow y' = y + \beta mn \Rightarrow y' \equiv y \bmod m \Rightarrow y' \equiv y \bmod n$

$\Rightarrow f([x+y]_{mn}) = f([x]_{mn}) + f([y]_{mn})$

ESERCIZIO 17

Dimostra che:

i) $i > j \Rightarrow \pi(i) > \pi(j)$

ii) $\pi(\ell) \geq \ell$

iii) $\nexists n \in \mathbb{Z}$ t.c. $\pi(n) = 13$

i) R = insieme di partizioni di i

S = insieme di partizioni di j

$\alpha = \{\alpha_1 + \dots + \alpha_m\} \in S$

$\beta = \{\alpha_1 + \dots + \alpha_m + (i-j)\} \in R$

Allora $f: S \to R$ è una mappa iniettiva, perché c'è sempre una partizione di i che non compare in R, ovvero $\{i\}$.

$\therefore i > j \Rightarrow \pi(i) > \pi(j)$

ii) Per induzione:

$P(\ell): \pi(\ell) \geq \ell$

$P(1) \Rightarrow 1 \geq 1$ ✓

Supponiamo $P(1), \dots, P(\ell)$ vere.

$P(\ell+1) \Rightarrow$ le partizioni di $\ell+1$ sono: $\underbrace{\{\ell+1\}}_{1 \text{ PART.}}, \underbrace{\{1, \pi\}}_{\ell \text{ PART.}}$

dove π è una partizione di ℓ

$\therefore$ ci sono almeno $\ell+1$ partizioni di $\ell+1$, ovvero:

$\pi(\ell+1) \geq \ell+1$

iii) $\pi(1) = 1$, $\pi(2) = 2$, $\pi(3) = 3$, $\pi(4) = 5$, $\pi(5) = 7$,

$\pi(6) = 11$, $\pi(7) = 15$

$i \geq 7 \Rightarrow \pi(i) \geq 15 \Rightarrow 13 \neq \pi(n) \ \forall n$

ESERCIZIO 18

Quali sono i possibili ordini degli elementi di un gruppo di ordine 60?

Poiché $G = \mathbb{Z}_{60}$ è ciclico di ordine 60, gli elementi possono avere come ordine tutti i divisori di 60.
Infatti:

$\mathbb{Z}_{60} = \{0, 1, 2, \dots, 59\} = \langle g \rangle = \{g^1, g^2, g^3, \dots, g^{60}\}$

$ord(g) = ord(\langle g \rangle)$

$\langle g^1 \rangle = \{0, \dots, 59\} \Rightarrow ord\langle 1 \rangle = 60$

$ord\langle g^2 \rangle = 30$

$ord\langle g^3 \rangle = 20$

...

ESERCIZIO 19

Mostra che $Z(G) = \{x \in G : gx = xg \ \forall g \in G\}$ è un sottogruppo di G.

- $eg = ge \ \forall g \in G \Rightarrow e \in Z(G)$
- $x, y \in Z(G)$

PERCHÉ $y \in Z(G)$ — PROPRIETÀ ASSOCIATIVA

$$(xy)g = x(yg) = x(gy) = xg(y) = (gx)y = g(xy) \quad \forall g \in G$$

- $x \in Z(G)$

$$x^{-1}g = x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} = egx^{-1} = gx^{-1} \quad \forall g \in G$$

ESERCIZIO 20

Qual'è il massimo ordine possibile di un gruppo che ha solo 4 classi di coniugio?

Per la formula delle classi di coniugio:

$$1 = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \frac{1}{n_4} = \left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right) = \left(\frac{1}{3}, \frac{1}{4}, \frac{1}{4}, \frac{1}{6}\right) =$$

$$= \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{6}, \frac{1}{6}\right) = \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{4}, \frac{1}{12}\right) =$$

$$= \left(\frac{1}{2}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}\right) = \left(\frac{1}{2}, \frac{1}{5}, \frac{1}{5}, \frac{1}{10}\right) =$$

$$= \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}\right) = \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{6}, \frac{1}{12}\right) =$$

$$= \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{5}, \frac{1}{20}\right) = \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{12}, \frac{1}{12}\right) =$$

$$= \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{10}, \frac{1}{15}\right) = \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{9}, \frac{1}{18}\right) =$$

$$= \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{8}, \frac{1}{24}\right) = \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{7}, \frac{1}{42}\right)$$

$$\Rightarrow |G| \leq 42$$

ESERCIZIO 21

Sia p un primo e G un gruppo di ordine p^2.
Se G ha un elemento di ordine p^2 allora $\mathbb{Z}_{p^2}$.
Altrimenti possiamo scegliere $u \in Z(G) - \{e\}$ e $v \in G - \{e, u\}$.
Mostra che la mappa

$$f: \mathbb{Z}_p \times \mathbb{Z}_p \to G, \quad f(j,k) = u^j v^k$$

è un isomorfismo.

f è ben definita perché:

$j, k \in \mathbb{Z}_p \times \mathbb{Z}_p$

$u^j v^k \in G$

$f \subseteq \mathbb{Z}_p \times \mathbb{Z}_p \times G$

$|\mathbb{Z}_p \times \mathbb{Z}_p| = |G| = p^2 < \infty$

$\Rightarrow f$ biettiva $=$ iniettiva

- $f(j,k) = f(r,s) \Leftrightarrow (j,k) = (r,s)$
  $u^j v^k = u^r v^s \Leftrightarrow j = r, k = s$
- $f((j,k)(r,s)) = f(j,k) f(r,s)$
  $u^{j+r} v^{k+s} = u^j u^r v^k v^s = (u^j v^k)(u^r v^s)$

$\therefore f$ è un isomorfismo

ESERCIZIO 22

Sia G il gruppo di movimenti rigidi che preservano un quadrato S in $\mathbb{R}^2$ con vertici $\{(\pm 1, \pm 1)\}$.
Allora, G è di ordine 8, ed è isomorfo al gruppo di matrici:

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad r^2 = -e = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad r^3 = -r = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad rs = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad -s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -rs = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Mostra che l'eq. delle classi di coniugio è:
$|G| = 2 + 2 + 2 + 2$

$Z(G) = \{x \in G : gx = xg \ \forall g \in G\} = \{e, -e\}$
$\Rightarrow |Z(G)| = 2$

$$|G| = |Z(G)| + \sum_{|C(x_j)|>1} \underbrace{[G : C(x_j)]}_{|G/C(x_j)| = 2 \ \forall j} =$$

$$= 2 + 2 + 2 + 2$$

porché $C(x_j) = \{g \in G : gx_j = x_j\}$
$= \{e, -e\} \ \forall j$
$\therefore C(x_j) = Z(G)$

ESERCIZIO 23

Verifica che se $f: G \to H$ e $g: H \to K$ sono omomorfismi allora $g \circ f: G \to K$ è un omomorfismo di gruppi.
(Quando $H = G$ scriviamo f^k per la composizione di f con sé stessa k volte).

f, g omomorfismi $\Rightarrow f(xy) = f(x)f(y) \quad \forall x, y \in G$
$g(rs) = g(r)g(s) \quad \forall r, s \in H$

$(g \circ f)(x) = g(f(x))$

$$\forall x, y \in G, \quad (g \circ f)(xy) = g(f(xy)) = \\ = g(f(x)f(y)) = \\ = g(f(x))g(f(y)) = \\ = (g \circ f)(x)(g \circ f)(y)$$

$\therefore g \circ f$ è un omomorfismo di gruppi

ESERCIZIO 24

Sia A un gruppo abeliano e n un num. intero positivo.
Mostra che $f(a) = a^n$ (o $f(a) = na$ se scritto in modo additivo) è un omomorfismo di gruppi.

$(A, +)$ gruppo abeliano $\Rightarrow$:

$$\left.\begin{array}{l} \cdot\ (a+b)+c = a+(b+c) \quad \forall a, b, c \in A \\ \cdot\ \exists e \in A \text{ t.c. } e+a = a+e = a \quad \forall a \in A \\ \cdot\ \forall a \in A \ \exists b \in A \text{ t.c. } a+b = b+a = e \end{array}\right\} \text{(gruppo)}$$

$\cdot\ a+b = b+a \quad \forall a, b \in A$ (abeliano)

$f(a) = na$ omom. di gruppi $\iff f(ab) = f(a)f(b)$
$\forall a, b \in A$

$$f(ab) = nanb \overset{\text{PROPR. ASSOCIATIVA}}{=} n(anb) = (na)(nb) = f(a)f(b)$$

ESERCIZIO 25

Sia A un gruppo abeliano finito.
Sia $f: A \to A$ un omomorfismo.
Il th di decomposizione di Fitting dice che $\exists k \in \mathbb{Z}, k > 0$ t.c. $A = \ker(f^k) \times \operatorname{Im}(f^k)$

i) Verifica il th di decomposizione di Fitting per il gruppo $\mathbb{Z}_{36}$ e l'omomorfismo $f(x) = 3x$

ii) Sia $f(x) = px$.
Mostrare che se p è un fattore primo di $|A|$, $\ker(f^j) \neq \{e\}$ $\forall j > 0$

i) $A = \mathbb{Z}_{36}$, $f(x) = 3x$

$\ker(f) = \{a \in A : f(a) = \overset{=0}{e_A}\} = \{0, 12, \overset{3 \cdot 24 \bmod 36 = 0}{24}\}$ perché $\cancel{3}x = \overset{12}{\cancel{36}}m$
$x = 12m$

$\operatorname{Im}(f) = \{f(a) : a \in A\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\}$

$|\ker(f)| = 3$; $|\operatorname{Im}(f)| = 12$

$\ker(f^2) = \{0, 4, 8, 12, 16, 20, 24, 28, 32\}$ perché $\cancel{9}x = \overset{4}{\cancel{36}}m$
$x = 4m$

$\operatorname{Im}(f^2) = \{0, 9, 18, 27\}$

$|\ker(f^2)| = 9$; $|\operatorname{Im}(f^2)| = 4$

$MCD(9, 4) = 1 \implies \mathbb{Z}_{36} = \mathbb{Z}_9 \times \mathbb{Z}_4$

$\implies A \cong \ker(f^2) \times \operatorname{Im}(f^2)$

ii) Per induzione su j:

$P(j) = p$ primo $\mid |A| \Rightarrow \ker(f^j) \neq \{e\} \ \forall j > 0$

$P(1) \Rightarrow \ker(f) = \{e, \frac{|A|}{p}, \dots\} \neq \{e\}$ ✓

Supponiamo $P(1), \dots, P(n)$ vere.

$P(j+1) \Rightarrow \ker(f^{j+1}) = \{e, \frac{|A|}{p^{j+1}}, \dots\} \neq \{e\}$ ✓

ESERCIZIO 26

Mostra che se H e K sono sottogruppi normali di G, allora $HK = \{hk : h \in H, k \in K\}$ è un sottogruppo normale di G.

H sottogruppo normale di $G \Rightarrow gHg^{-1} = H \ \forall g \in G$

K " " di $G \Rightarrow gKg^{-1} = K \ \forall g \in G$

$$gHKg^{-1} = \underbrace{(gHg^{-1})}_{=H}\underbrace{(gKg^{-1})}_{=K} = HK$$

ESERCIZIO 27

Sia G un gruppo finito.

Mostra che se H e K sono sottogruppi normali t.c. $|G| = |H||K|$ e $MCD(|H|, |K|) = 1$, allora $HK = G$

$$\underbrace{H \times K}_{\text{ord} = HK} \xrightarrow{e} \underbrace{G}_{\text{ord} = HK} \Rightarrow e(h,k) = hk \quad \text{surg} \Leftrightarrow \text{inj}$$

$$e(h_1, k_1) = e(h_2, k_2) \Rightarrow h_1 k_1 = h_2 k_2$$

$$\Rightarrow \underbrace{h_2^{-1} h_1}_{\in H} = \underbrace{k_2 k_1^{-1}}_{\in K}$$

$g \in H \cap K \Rightarrow g \in H \Rightarrow ord(g) \mid ord(H)$
$g \in K \Rightarrow ord(g) \mid ord(K)$

$MCD(|H|, |K|) = 1 \Rightarrow g = e$

$$\left.\begin{array}{l} e = h_2^{-1} h_1 \Rightarrow h_2 = h_1 \\ e = k_2 k_1^{-1} \Rightarrow k_2 = k_1 \end{array}\right\} \Rightarrow e \text{ è iniettiva}$$

ESERCIZIO 28

Mostra che, nel contesto del problema precedente, se $hk = kh \ \forall h \in H \ \forall k \in K$ allora:
$f : H \times K \to G$, $f(hk) = hk$ è un isomorfismo di gruppi.

$|HK| = |G| < \infty$
$\Rightarrow f$ biettiva $= f$ iniettiva

- $f(hk) = f(rs) \Rightarrow hk = rs$
  $hk = rs \Leftrightarrow hk = rs$
- $f(hk \cdot rs) = hkrs = h(krs) = (hk)(rs) = f(hk)f(rs)$

Lezione 10

In questa lezione, tutti gli anelli sono commutativi con identità. Vedere le sezioni 1 e 2 della lezione 7 per le definizioni. Di solito indichiamo gli anelli con R. Ricordiamo che $0_R \neq 1_R$.

Nota 0.1. Se r è un elemento di R, allora

$$0 + 0 = 0 \implies (0+0)r = (0)r \implies (0)r + (0)r = (0)r \implies (0)r = 0$$

In analogia con le mappe lineari e gli omomorfismi di gruppo, un omomorfismo di anelli commutativi con identità è una mappa $f : R \to S$ che conserva tutte le strutture inerenti a tale anello. In altre parole,

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y), \qquad f(1_R) = 1_S$$

Esercizio 1. Verificare che se $f : R \to S$ è un omomorfismo di anelli commutativi con indentiá, allora $f(0_R) = 0_S$.

Esercizio 2. Come abbiamo visto nelle lezioni precedenti, se n e m sono interi positivi >1 tali che $\mathrm{mcd}(m, n) = 1$ allora

$$\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \qquad \phi([x]_{mn}) = ([x]_m, [x]_n)$$

è un isomorfismo di gruppi abeliani. Verificare che questa mappa è in realtà un omomorfismo (isomorfismo) di anelli commutativi con identità.

Esercizio 3. Usando l'induzione, estendi l'esercizio precedente al caso in cui $\{n_1, \ldots, n_k\}$ è una collezione di interi > 1 e coprimi a coppie. In altra parole,

$$\phi : \mathbb{Z}_{n_1 \cdots n_k} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, \qquad \phi([x]_{n_1 \cdots n_k}) = ([x]_{n_1}, \ldots, [x]_{n_k})$$

è un isomorfismo di anelli commutativi con identità. Questo risultato è solitamente chiamato teorema cinese del resto.

1. Campi – Parte I

Definizione 1.1. Sia R un anello commutativo con identità. Allora, R è un campo se ogni elemento diverso da zero di R ha un inverso moltiplicativo. Di solito indichiamo un campo con K o L.

Esempio 1.2. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ dove p è un numero primo. Se $n = ab$ con $a, b > 1$ allora $\mathbb{Z}_n$ non è un campo perché $[a][b] = [ab] = 0$.

Un omomorfismo di campi $f : K \to L$ è un caso particolare di un omomorfismo di anelli commutativi con identità, in altre parole:

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y), \qquad f(1_K) = 1_L$$

Proposizione 1.3. *Un omomorfismo di campi $f : K \to L$ è iniettivo.*

Dimostrazione. $f(x) = f(y) \implies f(x-y) = 0_L$. Se $z = x - y \neq 0$ allora

$$1_L = f(1_K) = f(zz^{-1}) = f(z)f(z^{-1}) = 0_L f(z^{-1}) = 0_L$$

che è una contraddizione.

C.V.D.

Pertanto, un omomorfismo di campi suriettivo è un isomorfismo.

(*) $K(\sqrt{-1}) = \{a+b\sqrt{-1} : a,b \in K\}$

- $(a+b)\sqrt{-1} + (c+d)\sqrt{-1} = (a+c) + (b+d)\sqrt{-1}$
- $(a+b\sqrt{-1})(c+d\sqrt{-1}) = (ac-bd) + (ad+bc)\sqrt{-1}$
- $\frac{1}{a+b\sqrt{-1}} \cdot \frac{a-b\sqrt{-1}}{a-b\sqrt{-1}} = \frac{a-b\sqrt{-1}}{a^2+b^2}$, a^2+b^2 NON HA SOL. IN K

Definizione 1.4. Sia L un campo. Allora un sottoinsieme $K \subseteq L$ si chiama un sottocampo se $1 \in K$ ed K è chiuso rispetto all'addizione, la moltiplicazione, l'inverso additivo e all'inversione moltiplicativa di elementi diversi da zero.

Esempio 1.5. $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ è una successione di sottocampi.

Quanto segue è un analogo dell'affermazione che l'intersezione dei sottospazi vettoriali è un sottospazio vettoriale e l'immagine dello spazio vettoriale attraverso una mappa lineare è un sottospazio.

Proposizione 1.6.

- *L'immagine di un omomorfismo di campi $f : K \to L$ è un sottocampo di L.*
- *L'intersezione di due sottocampi di K è anch'essa un sottocampo di K.*

Dimostrazione. Un esercizio per lo studente.

C.V.D.

Esempio 1.7. Sia K un sottocampo di L e S un sottoinsieme di L. Allora l'intersezione di tutti i sottocampi di L che contengono K e S è il sottocampo $K(S)$ di L, e si chiama il sottocampo ottenuto annettendo S a K.

SOTTOINSIEME + PICCOLO DI $\mathbb{R}$ = CHE CONTIENE $\mathbb{Q}$ E $\sqrt{2}$

Esempio 1.8. $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ La chiusura rispetto ad addizione, sottrazione e moltiplicazione è chiara. Per la divisione usiamo un trucco dalla costruzione dei numeri complessi:

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}}\frac{c-d\sqrt{2}}{c-d\sqrt{2}} = \frac{(ac-2bd)+(bc-ad)\sqrt{2})}{c^2-2d^2}$$

MA $c^2 - 2d^2 = 0$ NON HA SOL. PER $c,d \in \mathbb{Q}$

Possiamo usare questo trucco anche al contrario: Supponiamo che $x^2+1=0$ non abbia soluzioni nel campo K. Siano $e=(1,0)$ e $f=(0,1)$ le basi standard di K^2. Allora possiamo definire una struttura di campo su $L = K^2$ utilizzando l'addizione vettoriale e definendo la moltiplicazione tramite l'equazione

$$(ae+bf)(ce+df) = (ac-bd)e + (ad+bc)f \tag{1.9}$$

Allora, $e = 1_L$ e

$$\frac{ae+bf}{ce+df} = \frac{ae+bf}{ce+df}\frac{ce-df}{ce-df} = \frac{(ae+bf)(ce+df)}{(c^2+d^2)e} = \frac{(ae+bf)(ce+df)}{(c^2+d^2)}$$

Se $(c,d) \neq (0,0)$, allora $c^2+d^2=0$ dá una soluzione a $x^2+1=0$ dopo averla divisa per c o per d. Di solito questo campo si scrive $K(\sqrt{-1})$. Questo non è in conflitto con la nostra notazione precedente $K(S)$, nel senso che $L = K(\sqrt{-1})$ è un campo che contiene K e una radice quadrata di -1.

(*) **Esempio 1.10.** $x^2+1=0$ non ha una soluzione in $\mathbb{Z}_3$. Quindi, possiamo costruire $K(\sqrt{-1})$. ES: $\mathbb{C} = \mathbb{R}(\sqrt{-1})$, $\sqrt{-1}$ NON È REALE, MA SE LO ANNETTO A $\mathbb{R}$, OTTENGO $\mathbb{C}$

L'intersezione di tutti i sottocampi di K è anch'essa un campo, che viene chiamato il sottocampo primo $\mathbb{F}$ di K.

Lemma 1.11. *Il sottocampo primo $\mathbb{F}$ di K è isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}_p$ per qualche numero primo p.*

PERCHÉ È CHIUSO RISPETTO ALLA MOLT.

ES: $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$

Dimostrazione. Sia $f : (\mathbb{Z}, +) \to (K, +)$ l'omomorfismo di gruppi tale che $f(1) = 1_K$. Si può facilmente verificare che $f(ab) = f(a)f(b)$. Se $\ker(f) \neq 0$ sia n il più piccolo intero positivo tale che $f(n) = 0$. Se n non è un numero primo, scriviamo $n = ab$ con a, $b > 1$. Allora $f(a)f(b) = f(ab) = 0 \implies f(a) = 0$ o $f(b) = 0$ che è una contraddizione. Quindi $\mathrm{Im}(f) \cong \mathbb{Z}/p\mathbb{Z}$. Se f è iniettiva allora $\phi(a/b) = f(a)/f(b)$ un omomorfismo da $\mathbb{Q}$ a K. Quindi $\phi(\mathbb{Q})$ è un sottocampo isomorfo a $\mathbb{Q}$.

C.V.D.

Se il campo primo di K è $\mathbb{Z}_p$, diciamo che K ha caratteristica p (char$(K) = p$). Altrimenti, diciamo che K ha caratteristica zero (char$(K) = 0$).

Esercizi

Esercizio 4. Verificare Proposizione (1.6).

Esercizio 5. Dimostrare che se $x^2 + a = 0$ non ha una soluzione nel campo K, allora possiamo costruire $K(\sqrt{-a})$ in analogia con $K(\sqrt{-1})$. Verificare che $x^2 + 2 = 0$ non ha una soluzione in $\mathbb{Z}_5$ e quindi abbiamo $\mathbb{Z}_5(\sqrt{-2})$. Spiega perché $x^2+1 = 0$ non ha soluzioni mod p quando p è congruente a 3 mod 4. (Vedi lezione 7).

Esercizio 6.

- Mostra che se K è un campo di caratteristica 3 allora
$$f : K \to K \qquad f(x) = x^3$$
Nel caso in cui $K = \mathbb{Z}_3(\sqrt{-1})$, quali elementi soddisfano $f(x) = x$?
- Mostra che in generale, se K ha caratteristica p, allora $f : K \to K$ data da $f(x) = x^p$ è un omomorfismo.

Esercizio 7. Dimostrare che se R è un dominio di integritá e $|R|$ è finito allora R è un campo.

2. Algebra Lineare

Sia K un campo. Allora uno spazio vettoriale sul campo K è un insieme V dotato di due operazioni, dette moltiplicazioni scalari
$$K \times V \to V, \qquad (c, v) \mapsto cv$$
e addizione vettoriale
$$V \times V \to V, \qquad (u, v) \mapsto u + v$$
che soddisfano tutti i soliti assiomi di uno spazio vettoriale dopo aver sostituito il solito insieme di scalari $\mathbb{R}$ o $\mathbb{C}$ con K.

Algebra matriciale, eliminazione gaussiana, sottospazi, mappe lineari (omomorfismi), determinante, indipendenza lineare, estensione, base, dimensione e molti altri aspetti dell'algebra lineare che non implica prodotti scalari.

Esempio 2.1. K^n è uno spazio vettoriale su K rispetto all'addizione vettoriale componentistica e alla moltiplicazione scalare componentistica.

Esempio 2.2. Sia S un insieme. Allora, l'insieme K^S di tutte le funzioni $S \to K$ è uno spazio vettoriale rispetto a
$$(f + g)(x) = f(x) + g(x), \qquad (cf)(x) = cf(x)$$
dove $f, g \in K^S$ e $c \in K$.

Come nel caso degli spazi vettoriali sui numeri reali, se U e V sono spazi vettoriali sul campo K di dimensione finita, e $\dim U = \dim V$ allora U e V sono isomorfi come spazi vettoriali.

Lemma 2.3. *Se K è un sottocampo di L, allora L è uno spazio vettoriale su K rispetto alle operazioni*

$$(x, y) \in L \times L \mapsto x + y \quad (\textit{addizione in } L)$$
$$(c, x) \in K \times L \mapsto kx \quad (\textit{moltiplicazione in } L)$$

In questo caso, diciamo che L è un'estensione di K e scriviamo $L : K$.

Dimostrazione. Un esercizio per gli studenti.

C.V.D.

Se K è un sottocampo di L, scriviamo $[L : K]$ per la dimensione di L come un spazio vettoriale su K (potrebbe essere ∞). Diciamo che L è un'estensione finita di K se $[L : K]$ è finito.

Esempio 2.4.

- $\mathbb{C}$ è una estensione di $\mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$.
- $\mathbb{Z}_3(\sqrt{-1})$ è una estensione di $\mathbb{Z}_3$ e $[\mathbb{Z}_3(\sqrt{-1}) : \mathbb{Z}_3] = 2$.
- $\mathbb{R}$ è una estensione di $\mathbb{Q}$ e $[\mathbb{R} : \mathbb{Q}] = \infty$. Ciò deriva dal fatto che $\mathbb{R}$ non è numerabile mentre $\mathbb{Q}$ è numerabile. (Questo fa parte della teoria degli insiemi).

Sia A una matrice quadrata con voci reali o complesse con polinomio caratteristico p. Allora, per il teorema di Cayley-Hamilton, $p(A) = 0$. Una versione semplificata di questo per una matrice quadrata con coefficienti in un campo K è che esiste un polinomio non-costante f tale che $f(A) = 0$. Per vedere questo, osserviamo che lo spazio vettoriale K di tutte le matrici $n \times n$ con voci in K ha dimensione n^2. Dunque, l'insieme

$$1, A, A^2, \ldots, A^{n^2}$$

non può essere linearmente indipendente, poiché contiene $n^2 + 1$ elementi. La relazione di dipendenza

$$\sum_{j=0}^{n^2} c_j A^j$$

può essere riscritta come $p(A) = 0$ per qualche polinomio $p(t)$ con coefficienti in K. Senza perdita di generalità, possiamo supporre che $p(t)$ sia un polinomio monico.

Nota 2.5. Infatti, il teorema di Cayley-Hamilton è vero per qualsiasi matrice quadrata A con elementi in un anello commutativo R. La dimostrazione parte dall'osservazione che $\text{adj}(M)M = \det(M)I$ e quindi ponendo $M = tI - A$. Il resto della dimostrazione è algebra di matrici.

Sia L un'estensione di campo di K. Allora, $\alpha \in L$ si dice essere algebrico su K se esiste un polinomio non-costante $f(t)$ tale che $f(\alpha) = 0$.

Lemma 2.6. *Se L è un'estensione di campo di K e $[L : K]$ è finito, allora ogni elemento $\alpha \in L$ è algebrico su K.*

Dimostrazione. Sia $\alpha \in L$. Come nella dimostrazione che ogni matrice quadrata soddisfa un'equazione polinomiale, si nota solo che se $[L : K] = n$ allora $\{1, \alpha, \ldots, \alpha^n\}$ non può essere un insieme linearmente indipendente.

C.V.D.

Definizione 2.7. Sia L un'estensione di K e supponiamo che $\alpha \in L$ sia algebrico su K. Allora, il polinomio minimo $m = m_\alpha$ di α è il polinomio monico di grado minimo in $K[t]$ tale che $m(\alpha) = 0$.

Nota 2.8. La definizione implica che il polinomio minimo è unico. Questo è un argomento che abbiamo fatto molte volte: Se ci fossero due di questi polinomi monici, la differenza è zero o un polinomio di grado strettamente inferiore che valuta zero su α.

Esempio 2.9. Se $\alpha \in K$ allora $m_\alpha(t) = t - \alpha$ e $K(\alpha) = K$. In particolare, il polinomio minimo di 0 è t. ES. $m_{\sqrt{2}} = t^2 - 2$

Supponiamo che $L : K$ e $M : L$ siano estensioni di campi. Allora M è un estensione di K. In questo caso, diciamo che $F \subseteq K \subseteq L$ è una torre di estensioni di campi.

Teorema 2.10. *(Legge della Torre) Siano $K \subseteq L \subseteq M$ una torre di estensioni di campi. Se $M : L$ e $L : K$ sono finite allora $M : K$ è finita e $[M : K] = [M : L][L : K]$.*

Dimostrazione. Un esercizio per lo studente.

C.V.D.

Esempio 2.11. Se $[M : K] = 4$ e $K \subsetneq L \subsetneq M$ è una torre di estensioni di campi allora $[M : L] = 2$ e $[L : K] = 2$.

Proposizione 2.12. *Sia K un campo con campo primo $\mathbb{F}$. Se K contiene un numero finito di elementi allora char$(K) = p$ per qualche numero primo p e $|K| = p^n$ dove n è la dimensione di K su $\mathbb{F}$.*

Dimostrazione. Se char$(K) = 0$ allora K ha un sottocampo isomorfo a $\mathbb{Q}$ e quindi K contiene infiniti elementi. Così, char$(K) = p$. Se la dimensione di K su $\mathbb{F}$ non è finita allora K contiene un insieme infinito di elementi linearmente indipendenti. Dunque, la dimensione di K su k è finita. In quantotale, come un spazio vettoriale, $K \cong \mathbb{F}^n$ e quindi $|K| = |\mathbb{F}^n| = p^n$

C.V.D.

Nota 2.13. A meno di isomorfismi, c'è solo un campo di ordine p^n. L'idea della dimostrazione è che l'insieme K^* di elementi diversi da zero di un campo K è un gruppo abeliano rispetto alla moltiplicazione. Quando K è finito, questo gruppo è ciclico, e quindi $K^* = \langle \alpha \rangle$. Questo ci dà un modo per costruire K come il campo ottenuto unendo le radici di $x^{p^n-1} - 1 = 0$ a $\mathbb{Z}_p$. I generatori di K^* sono detti elementi primitivi di K.

Esercizi

Esercizio 8. Supponiamo che $M : K$ sia un'estensione di campo tale che $[M : K]$ è un numero primo p. Esiste un campo intermedio L tra K e M, in altre parole $K \subsetneq L \subsetneq M$?

Esercizio 9. Mostra che se $f : L \to L$ è un omomorfismo allora

$$K = \{x \in L \mid f(x) = x\}$$

è un sottocampo di L.

Esercizio 10. Trova gli elementi primitivi di $\mathbb{Z}_7$ e $\mathbb{Z}_3(\sqrt{-1})$ (vedi nota (2.13)).

Esercizio 11. Verificare (2.3)

ɣ **Esercizio 12.** Verificare Teorema (2.10).

ɣ **Esercizio 13.** Trova un polinomio monico $f(t) \in \mathbb{Q}[t]$ di grado 4 tale che $f(\sqrt{2}+\sqrt{3}) = 0$. Mostra che f non ha radici razionali.

3. Polinomi

Sia R un anello commutativo con identità. Ricordiamo dalla lezione 7 che $R[x]$ è l'insieme dei polinomi nella variabile x con coefficienti nell'anello R. Informalmente, ciò significa che ogni elemento $f \in R[x]$ può essere scritto come

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \qquad a_n, \ldots, a_0 \in R$$

La definizione del grado di un polinomio, termine di ordine massimo, termine di ordine massimo e polinomio monico sono esattamente le stesse del caso di $\mathbb{Q}[x]$ discusso nella lezione 4. La definizione formale è la seguente:

Definizione 3.1. Sia $R^{\mathbb{N}}$ l'insieme di tutte le funzioni $\mathbb{N} \to R$ dove $\mathbb{N} = \{0, 1, \ldots, \}$. Dato $f \in R^{\mathbb{N}}$ sia $\text{supp}(f) = \{x \in \mathbb{N} \mid f(x) \neq 0\}$. Allora, $R[x] = \{f \in R^{\mathbb{N}} \mid |\text{supp}(f)| < \infty\}$. In notazione convenzionale,

$$f \in R[x] \subset R^{\mathbb{N}} \longleftrightarrow \sum_k f(k)x^k$$

dove la somma a destra ha solo un numero finito di termini.

Nota 3.2. $K[x]$ è uno spazio vettoriale sul campo K. Il sottoinsieme $P_d[x]$ dei polinomi di grado minore o uguale a d (incluso il polinomio nullo, che non ha grado) è un sottospazio di $K[x]$ di dimensione $d+1$. Dato $r \in K$, l'insieme

$$\{1, x-r, (x-r)^2, \ldots, (x-r)^d\}$$

è una base di $P_d[x]$.

Ripetiamo il nostro avvertimento della lezione 7: Un polinomio $f \in R[x]$ definisce una funzione $\text{ev}_f : R \to R$ secondo la regola:

$$\text{ev}_f(a) = f(a)$$

ma in generale il polinomio f contiene più informazioni di ev_f.

Rivedendo la lezione 4, vediamo che possiamo sostituire ovunque $\mathbb{Q}$ con un campo arbitrario K fino a raggiungere il teorema delle radici razionali. A quel punto, utilizziamo davvero il fatto che gli elementi di $\mathbb{Q}$ sono frazioni intere p/q.

In particolare, abbiamo:

TH DI DIVISIONE PER POLINOMI CON COEFF. IN UN CAMPO

Teorema 3.3. *Siano f e $g \in K[x]$ e supponiamo che $\deg(g) > 0$. Allora, esistono elementi unici q, $r \in K[x]$ tali che*

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

dove (i) $r(x) = 0$ oppure (ii) $r(x) \neq 0$ e $\deg(r) < \deg(g)$.

Nello stesso modo siano f, $g \in K[x]$ due polinomi tali che $(f, g) \neq (0, 0)$. Sia

$$T = \{\, af + bg \in K[x] - \{0\} \mid a, b \in K[x] \,\} \tag{3.4}$$

Lemma 3.5. *T contiene un unico polinomio monico di grado minimo.*

Lemma 3.6. *Siano f, $g \in K[x]$ due polinomi tali che $(f, g) \neq (0, 0)$. Sia h l'unico polinomio monico di T di grado minimo. Allora, $h|f$ e $h|g$.*

Proof. (La stessa dimostrazione della lezione 4): Se $f = 0$ allora h è l'unico polinomio monico che è un multiplo scalare di g. Allo stesso modo, se $g = 0$ allora h è l'unico polinomio monico che è un multiplo scalare di f. Rimane quindi da considerare il caso in cui sia f che g siano diversi da zero. Chiaramente,

$$f,\, g \in T \implies \deg(h) \leq \min(\deg(f), \deg(g))$$

Siano $h = af + bg$ e $f = qh + r$ dove $r = 0$ oppure $\deg(r) < \deg(h)$. Se $r = 0$ allora $h|f$. Altrimenti,

$$f = q(af + bg) + r \implies r = (1 - qa)f - qbg \in T$$

Per la minimalità del grado di h, dobbiamo avere $r = 0$ ($\implies h|f$). Allo stesso modo, $h|g$ scambiando i ruoli di f e g. C.V.D.

Definizione 3.7. L'unico polinomio h di grado minimo in (3.4) si chiama massimo comune divisore $\mathrm{mcd}(f, g)$ di f e g.

Per calcolare $\mathrm{mcd}(f, g)$, usiamo l'algoritmo euclideo per $K[x]$:

$$f = qg + r \implies \mathrm{mcd}(f, g) = \mathrm{mcd}(r, g) = \mathrm{mcd}(g, r)$$

Un polinomio costante è un polinomio della forma $f(x) = f_0$ per qualche $f_0 \in K$. In particolare, un polinomio non-costante ha grado maggiore di zero.

Definizione 3.8. Un polinomio $f \in K[x]$ non-costante è irriducibile se non esistono polinomi non-costanti g, $h \in K[x]$tale che $f = gh$. Altrimenti, f è riducibile.

Esempio 3.9.

- Un polinomio di grado 1 è irriducibile. $\deg(h) \geq 1$.
- Se $f \in K[x] - \{0\}$ ha un radice $r \in K$ allora f è riducibile perché $(x - r)|f$.
- Sia $f \in K[x]$ un polinomio di grado 2. Allora, f è irriducibile se e sole se f non ha una radice $r \in K$.

Lemma 3.10. *Siano f, $g \in K[x]$. Se f è irriducibile allora $\mathrm{mcd}(f, g) = 1$ oppure $f|g$.*

Proof. Sia $m = \mathrm{mcd}(f, g)$. Allora, $m|f$ e quindi $f = mq$ per qualche $\cancel{m}$ q $\in K[x]$. Per definizione, poiché f è irriducibile, segue che o m o q ha grado 0, cioè o (i) $m = 1$ o (ii) $m = uf$ per qualche $u \in K - \{0\}$. Nel caso (i), $m = \mathrm{mcd}(f, g) = 1$. Nel caso (ii), $m = \mathrm{mcd}(f, g) = uf|g \implies f|g$. C.V.D.

Il risultato seguente è l'analogo del lemma di Euclide per i polinomi:

Lemma 3.11. *Sia $f \in K[x]$ irriducibile. Se $f|gh$ allora $f|g$ o $f|h$.*

Proof. In base al lemma precedente, se f non divide g allora $\mathrm{mcd}(f, g) = 1$. Pertanto, esistono a, $b \in K[x]$ tali che $1 = af + bg$ e quindi $h = afh + bgh$. Per ipotesi $f|gh$ e $f|afh$ segue che $f|h$ C.V.D.

Combinando i risultati precedenti, si può dimostrare che gli elementi in $K[x]$ hanno un'unica fattorizzazione in prodotti di polinomi irriducibili.

Teorema di Fattorizzazione Unica. *Ogni polinomio non-costante $f \in K[x]$ può essere scritto come prodotto di polinomi irriducibili. Inoltre, questa fattorizzazione è unica: Se*

$$f(x) = p_1(x) \cdots p_r(x), \qquad f(x) = q_1(x) \cdots q_s(x) \tag{3.12}$$

sono due fattorizzazioni in un prodotto di irriducibili allora (i) $r = s$ e (ii) Esiste una permutazione $sigma$ di $\{1, \ldots, r\}$ e una collezione di costanti non nulle $\{c_j\}$ tali che

$$q_j(x) = c_j p_{\sigma(j)}(x)$$

per $j = 1 \ldots, r$.

La trattazione del minimo comune multiplo di due polinomi è stata omessa, ma si può facilmente verificare che si ha il seguente risultato, proprio come nella lezione 4:

Corollario 3.13. *Siano f, $g \in \overset{K}{\cancel{\mathbb{Q}}}[x]$ polinomi monici non-costanti. Allora,*

$$fg = \mathrm{mcm}(f, g)\,\mathrm{mcd}(f, g)$$

Torniamo ora alla nostra discussione sui polinomi minimi:

Lemma 3.14. *Sia L un'estensione del campo K e sia $\alpha \in L$ un elemento algebrico. Allora, il polinomio minimo $m \in K[t]$ di α è irriducibile.*

Dimostrazione. Supponiamo che $m = fg$ dove f e g non siano costanti. Allora, poiché $K[t]$ è un dominio integrale,

$$0 = m(\alpha) = f(\alpha)g(\alpha) \implies f(\alpha) = 0, \quad o \quad g(\alpha) = 0$$

che contraddice la minimalità del grado di m.

C.V.D.

Al contrario, abbiamo:

Lemma 3.15. *Sia L un'estensione del campo K e $\alpha \in L$ sia un elemento algebrico, con polinomio minimo m. Supponiamo che $f \in K[t]$ sia un polinomio monico irriducibile tale che $f(\alpha) = 0$. Allora, $f = m$.*

Dimostrazione. Poiché m è il polinomio monico di grado minimo che annulla α, possiamo scrivere $f = qm + r$ dove $r = 0$ $\deg(r) < \deg(m)$. Valutando a α si ottiene:

$$0 = f(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = r(\alpha)$$

Se $r \neq 0$, questo contraddice la minimalità del grado di m. Se $r = 0$ questo contraddice l'irriducibilità di f, a meno che q non sia un polinomio costante. Poiché sia f che m sono monici, questo implica $q = 1$.

C.V.D.

Esempio 3.16. $x^3 - 2 \in \mathbb{Q}[x]$ annulla $\sqrt[3]{2}$ ed è irriducibile in $\mathbb{Q}[x]$. Pertanto, $x^3 - 2$ è il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$. Per vedere che $x^3 - 2$ è irriducibile, notiamo che, essendo di grado 3, se $x^3 - 2$ è riducibile allora ha almeno un fattore lineare. Ma per il test della radice razionale, $x^3 - 2$ non ha radici razionali.

Proposizione 3.17. *Se $\alpha \in L$ è algebrico su K con polinomio minimo m di grado d allora $\{1, \alpha, \ldots, \alpha^{d-1}\}$ sono linearmente indipendenti. (Se $\alpha \in K$ allora questo insieme è solo $\{1\}$).*

Dimostrazione. Supponiamo che $\sum_{k=0}^{d-1} c_k \alpha^k = 0$ sia una relazione di dipendenza lineare (non banale). Allora, $f(t) = \sum_{k=0}^{d-1} c_k t^k$ è un polinomio non-costante che annulla α. Dopo aver riscalato, possiamo supporre che f sia un polinomio monico di grado minore di $d = \deg(m)$ tale che $f(\alpha) = 0$, che contraddice la minimalità di m.

C.V.D.

Per continuare, dato $\alpha \in L$ che è algebrico su K con polinomio minimo m di grado d, sia

$$W = \text{span}_K(1, \ldots, \alpha^{d-1})$$

Allora W è un sottospazio DI L SU K ~~K di L~~, e quindi W è chiuso rispetto all'addizione, sottrazione e moltiplicazione per scalari di K. Per vedere che W è chiuso rispetto alla moltiplicazione (come sottoinsieme di L), siano w_1, $w_2 \in W$. Allora esistono i polinomi f_1 e $f_2 \in K[t]$ di grado minore di d tale che $w_1 = f_1(\alpha)$ e $w_2 = f_2(\alpha)$. Se $\deg(f_1 f_2) < d$ allora $w_1 w_2 = f_1(\alpha) f_2(\alpha) \in W$. Se $\deg(f_1 f_2) \geq d$ allora

$$f_1 f_2 = qm + r, \qquad r = 0 \quad \deg(r) < d$$

e quindi

$$f_1(\alpha) f_2(\alpha) = q(\alpha) m(\alpha) + r(\alpha) = r(\alpha) \in W$$

Infine, dato $w = f(\alpha) \in W$ con $\deg(f) < d$ possiamo calcolare $1/f(\alpha) \in W$ come segue: Poiché $\deg(f) < \deg(m)$ e m è irriducibile, segue che $\text{mcd}(f, m) = 1$. Quindi, per il teorema di Bézout esistono u, $v \in K[t]$ tali che $u(t)f(t) + v(t)m(t) = 1$. Senza perdita di generalità, possiamo supporre che $\deg(u) < \deg(m)$ scrivendo $u = qm + r$ se $\deg(u) \geq \deg(m)$. Valutazione di questa identità in $t = \alpha$ dà

$$1 = u(\alpha) f(\alpha) + v(\alpha) m(\alpha) = u(\alpha) f(\alpha)$$

In sintesi, abbiamo dimostrato:

Proposizione 3.18. *Sia $\alpha \in L$ algebrico su K con a polinomio minimo di grado d e $W = \text{span}_K(1, \alpha, \ldots, \alpha^{d-1})$. Quindi, $K(\alpha) = W$.*

Dimostrazione. Per il paragrafo precedente, W è un sottocampo di L che contiene α e K. Pertanto, $K(\alpha) \subseteq W$ perché $K(\alpha)$ è il sottocampo più piccolo di L che contiene α e K. Per vederlo $W \subseteq K(\alpha)$ osserviamo che poiché $K(\alpha)$ è un campo che contiene K e α, deve contenere tutte le combinazioni K-lineari di $1, \alpha, \ldots, \alpha^{d-1}$.

C.V.D.

Esempio 3.19. Il polinomio minimo di $\alpha = \sqrt[3]{2}$ su $\mathbb{Q}$ è $x^3 - 2$. Quindi,

$$\begin{aligned} &1 = (x+1)(x^2 - x + 1)/3 + (x^3 - 2)(-1/3) \implies \\ &1 = (\alpha+1)(\alpha^2 - \alpha + 1)/3 + (\alpha^3 - 2)(-1/3) = (\alpha+1)(\alpha^2 - \alpha + 1)/3 \\ &\implies \frac{1}{\alpha+1} = (\alpha^2 - \alpha + 1)/3 \end{aligned}$$

Esercizi

Esercizio 14. Verifica le asserzioni dell'Esempio (3.9) usando le dimostrazioni corrispondenti della lezione 4.

ESERCIZIO 1

Verificare che se $f: R \to S$ è un omomorfismo di anelli commutativi con identità, allora $f(0_R) = 0_S$.

$f(x + 0_R) = f(x)$

$f(x) + f(0_R) = f(x)$ PER LA DEF. DI OMOMORFISMO

$\cancel{f(x)} + f(0_R) = \cancel{f(x)} + 0_S$

$\Rightarrow f(0_R) = 0_S$

ESERCIZIO 2

Se n e m sono interi positivi > 1 t.c. $MCD(m,n) = 1$, allora:

$\phi: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $\phi([x]_{mn}) = ([x]_m, [x]_n)$

è un isomorfismo di gruppi abeliani.

Verificare che questa mappa è un omomorfismo di anelli commutativi con identità.

i) $\phi([x+y]_{mn}) = \phi([x]_m) + \phi([y_n])$

$[x] = x + \alpha mn$, $\alpha \in \mathbb{Z}$

$[y] = y + \beta mn$, $\beta \in \mathbb{Z}$

$\phi([x+y]_{mn}) = ([x + \alpha mn + y + \beta mn]_{mn})$

$= \phi([x + \alpha mn + y + \beta mn]_m, [x + \alpha mn + y + \beta mn]_n)$

$\phi([x]_m) + \phi([y_n]) = \phi([x + \alpha mn]_{mn}) + \phi([y + \alpha mn]_{mn})$

$= \phi([x + \alpha mn]_m, [x + \alpha mn]_n) +$

$+ \phi([y + \beta mn]_m, [y + \beta mn]_n)$

$= \phi([x+y]_{mn})$

ii) $\phi([xy]_{mn}) = \phi([x]_m)\phi([y]_n)$

$\phi([xy]_{mn}) = \phi([(x + \alpha mn)(y + \beta mn)]_{mn}) =$

$= \phi([xy + \gamma mn]_m, [xy + \underbrace{\gamma mn}_{\text{MULTIPLO DI } mn}]_n)$

$\phi([x]_m)\phi([y]_n) = \phi([x + \alpha mn]_m)\phi([y + \beta mn]_n) =$

$= \phi([x + \alpha mn]_m [y + \beta mn]_n) =$

$= \phi([xy + \gamma mn]_m, [xy + \gamma mn]_n)$

ESERCIZIO 3

Usando l'induzione, estendi l'esercizio precedente al caso in cui $\{n_1, \dots, n_k\}$ è una collezione di interi >1 e coprimi a coppie.

In altre parole, dimostra che:

$\phi: \mathbb{Z}_{n_1 \cdots n_k} \to \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$, $\phi([x]_{n_1 \cdots n_k}) = ([x]_{n_1}, \dots, [x]_{n_k})$

è un isomorfismo di anelli commutativi con identità.

(TH CINESE DEL RESTO)

$n_1, \dots, n_k$ coprimi $\Rightarrow$ $\mathbb{Z}_{n_1 \times \underbrace{(n_2 \cdots n_k)}_{m}} = \mathbb{Z}_{n_1} \times \mathbb{Z}_m$

$P(k)$: $\mathbb{Z}_{n_1 \cdots n_k} = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$

$P(2)$: $\mathbb{Z}_{n_1 \cdot n_2} = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ ✓

Supponiamo $P(k)$ vera

$P(k+1)$: $\mathbb{Z}_{n_1 \cdots n_{k+1}} = \underbrace{(\mathbb{Z}_{n_1 \cdots n_k})}_{m} \times \underbrace{\mathbb{Z}_{n_{k+1}}}_{n} = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \times \mathbb{Z}_{n_{k+1}}$

$MCD(m, n) = 1$

ESERCIZIO 4

Verificare la seguente proposizione:

i) L'immagine di un omomorfismo di campi $f: K \to L$ è un sottocampo di L.

ii) L'intersezione di due sottocampi di K è anch'essa un sottocampo di K.

i) $Im(f) = \{f(x) : x \in K\}$

- $f(1_K) = 1_L \in Im(f)$
- $a = f(\alpha)$, $b = f(\beta) \in Im(f)$
  $\Rightarrow ab = f(\alpha)f(\beta) = f(\alpha\beta) \in Im(f)$
- $a = f(\alpha)$, $b = f(\beta) \in Im(f)$
  $\Rightarrow a+b = f(\alpha) + f(\beta) = f(\alpha+\beta) \in Im(f)$
- $a = f(\alpha)$, $a \neq 0 \Rightarrow \exists a^{-1} \in Im(f)$ t.c. $a^{-1}a = aa^{-1} = 1_K$
- $a = f(\alpha)$, $a \neq 0 \Rightarrow \exists a' \in Im(f)$ t.c. $a'+a = a+a' = 0_K$

ii) Sia $S = \bigcap_i F_i$, F_i sottocampi di K

- $0, 1 \in F_i \ \forall i \Rightarrow 0, 1 \in S$
- $\forall a \neq 0 \in F_i \ \exists a^{-1} \in F_i$ t.c. $aa^{-1} = a^{-1}a = 1_{F_i} \Rightarrow a^{-1} \in S$
- $\forall a \neq 0 \in F_i \ \exists a' \in F_i$ t.c. $a+a' = a'+a = 0_{F_i} \Rightarrow a' \in S$
- $a, b \in F_i \Rightarrow ab \in F_i \Rightarrow ab \in S$
- $a, b \in F_i \Rightarrow a+b \in F_i \Rightarrow a+b \in S$

ESERCIZIO 5

i) Dim. che se $x^2+a=0$ non ha soluzione nel campo K, allora possiamo costruire $K(\sqrt{-a})$.

ii) Verificare che $x^2+2=0$ non ha soluzione in $\mathbb{Z}_5$ e quindi abbiamo $\mathbb{Z}_5(\sqrt{2})$.

iii) Spiega perché $x^2+1=0$ non ha soluzione mod p quando $p \equiv 3 \bmod 4$

i) $K(\sqrt{-a}) = \{u+v\sqrt{-a} : u,v \in K\}$

Verifica assiomi di un campo:

i) $K(\sqrt{-a})$ é un gruppo abeliano per l'addizione

$\Rightarrow (u+v\sqrt{-a}) + (u'+v'\sqrt{-a}) = (u+u') + (v+v')\sqrt{-a}$

ii) IDENTITÁ: $0 = 0 + \sqrt{-a}$

iii) INVERSO: $(u+v\sqrt{-a}) + (-u + (-v)\sqrt{-a}) = 0$

iv) P. ASSOCIATIVA: $((u+v\sqrt{-a}) + (u'+v'\sqrt{-a})) + (u''+v''\sqrt{-a}) =$

$= (u+u'+u'', (v+v'+v'')\sqrt{-a})$

PERCHÉ K È UN CAMPO

$= (u+v\sqrt{-a}) + ((u'+v'\sqrt{-a}) + (u''+v''\sqrt{-a}))$

Verifica assiomi di un anello comm. con identitá:

v) P. COMMUTATIVA: $(u+v\sqrt{-a})(u'+v'\sqrt{-a}) = (u'+v'\sqrt{-a})(u+v\sqrt{-a})$

vi) IDENTITÁ: $1(u+v\sqrt{-a}) = u+v\sqrt{-a}$

vii) P. DISTRIBUTIVA: $(u+v\sqrt{-a})((u'+v'\sqrt{-a})(u''+v''\sqrt{-a})) =$

$= ((u+v\sqrt{a})(u'+v'\sqrt{-a})) + ((u+v\sqrt{-a})(u''+v''\sqrt{-a}))$

viii) INVERSO: $\dfrac{1}{u+v\sqrt{-a}} \cdot \dfrac{u-v\sqrt{-a}}{u-v\sqrt{-a}} = \dfrac{u-v\sqrt{-a}}{u^2+av^2}$ $\quad (u,v) \neq (0,0)$

$u^2+av^2 = 0 \longrightarrow v=0 \Rightarrow u^2=0 \Rightarrow (u,v)=(0,0)$ ×

$\searrow v \neq 0 \Rightarrow \left(\frac{u}{v}\right)^2 + a = 0$ che non ha sol. in K

ii) $\mathbb{Z}_5 = \{0,1,2,3,4\}$

$0^2 + 2 \neq 0 \pmod 5$

$1^2 + 2 \neq 0$ "

$2^2 + 2 \neq 0$ "

$3^2 + 2 \neq 0$ "

$4^2 + 2 \neq 0$ "

$\Rightarrow x^2 + 2$ non ha soluzione in $\mathbb{Z}_5$

iii) $x^2 \equiv -1 \mod p$ ha sol. $\Leftrightarrow p \equiv 1 \mod 4$

ESERCIZIO 6

i) Mostra che se K è un campo di caratteristica 3 allora $f: K \to K$, $f(x) = x^3$ è un omomorfismo.
Nel caso in cui $K = \mathbb{Z}_3(\sqrt{-1})$, quali elementi soddisfano $f(x) = x$?

ii) Mostra che in generale, se K ha caratteristica p, allora $f: K \to K$, $f(x) = x^p$ è un omomorfismo

i) · $f(x+y) = f((x+y)^3) = f(x^3 + \underbrace{\cancel{3x^2y} + \cancel{3xy^2}}_{\mod 3 = 0} + y^3) =$
$= f(x^3 + y^3) = f(x^3) + f(y^3)$

· $f(xy) = f((xy)^3) = f(x^3y^3) = f(x^3)f(y^3)$

· $f(1_K) = 1_K$

$K = \mathbb{Z}_3(\sqrt{-1}) = \{0, 1, 2, \sqrt{-1}\}$

$f(0) = 0$ ✓

$f(1) = 1$ ✓

$f(2) = 8$ ×

$f(\sqrt{-1}) = \sqrt{(-1)^3} = \sqrt{-1}$ ✓

ii) · $f(x+y) = f((x+y)^p) = f(x^p + y^p) = f(x^p) + f(y^p)$

· $f(xy) = f((xy)^p) = f(x^py^p) = f(x^p)f(y^p)$

· $f(1_K) = 1_K$

ESERCIZIO 7

Dim. che se R è un dominio di integrità e $|R| < \infty$, allora R è un campo.

Dobbiamo dim. che ogni $x \in R$, $x \neq 0$ ha un inverso moltiplicativo.

Sia $R^* = \{x \neq 0 : x \in R\}$

Sia $e : R^* \to R^*$, $e(x) = ax$

$e(x) = e(y) \Rightarrow ax = ay$, $a, x, y \in R^*$

$\Rightarrow ax - ay = 0 \Rightarrow a(x-y) = 0$

Poiché R è un dominio di integrità

$a(x-y) = 0 \Rightarrow a = 0$ oppure $x - y = 0$

ma $a = 0$ ↯ quindi $x = y$

$\therefore$ e è iniettiva ($|R^*| = |R^*| < \infty \Rightarrow e$ è anche bij e surj)

$\Rightarrow 1 \in R^*$, $\forall a \in R^* \ \exists x \in R^* : e(x) = 1$, ovvero $ax = 1$

$\Rightarrow a$ è un' unità

$\Rightarrow R$ è un campo

ESERCIZIO 8

Supponiamo che $H : K$ sia un' estensione di campo t.c. $[H:K]$ è un numero primo p.

Esiste un campo intermedio L tra K e H ($K \subset L \subset H$)?

No, perché per la legge della torre:

$\underbrace{[H:K]}_{p} = \underbrace{[H:L]}_{\alpha}\underbrace{[L:K]}_{\beta}$, ma p è primo

<u>ES</u>: $\underbrace{\mathbb{Q}(\sqrt[3]{2})}_{H} : \underbrace{\mathbb{Q}}_{K}$, $\underbrace{[H:K]}_{3} = [H:L][L:K]$

perché $m_\alpha = x^3 - 2$

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$

ESERCIZIO 9

Mostra che se $f: L \to L$ è un omomorfismo allora $K = \{x \in L : f(x) = x\}$ è un sottocampo di L.

- $f(1) = 1 \in K$
- $f(x+y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $\forall x \in K \ \exists a \in K : ax = xa = 1$
- $\forall x \in K \ \exists a \in K : a + x = x + a = 0$

ESERCIZIO 10

Trova gli elementi primitivi di $\mathbb{Z}_7$ e $\mathbb{Z}_3(\sqrt{-1})$.

$\alpha \in K^*$ è primitivo $\iff$ α genera K^*

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$|\mathbb{Z}_7^*| = 6$

$\langle [1] \rangle = \{[1]\} \Rightarrow$ non è un generatore

$\langle [2] \rangle = \{[2], [4], [1]\}$

↳ PERCHÉ $2^2 \bmod 7 = 4$

$\langle [3] \rangle = \{[3], [2], [6], [4], [5], [1]\}$ ✓

$\langle [4] \rangle = \{[4], [2], [1]\}$

$\langle [5] \rangle = \{[5], [4], [6], [2], [3], [1]\}$ ✓

$\langle [6] \rangle = \{[6], [1]\}$

Gli elem. primitivi di $\mathbb{Z}_7$ sono $[3]$ e $[5]$.

ESERCIZIO 11

Dim. il seguente lemma:

Se K é un sottocampo di L, allora L é uno spazio vett. su K rispetto alle operazioni:

- $(x, y) \in L \times L \mapsto x + y$ (ADD. IN L)
- $(c, x) \in K \times L \mapsto Kx$ (MOLT. IN L)

In questo caso diciamo che L é un'estensione di K e scriviamo $L : K$.

DIM

$K \times L \to L$

i) $l_1 + l_2 = l_2 + l_1$

ii) $(l_1 + l_2) + l_3 = l_1 + (l_2 + l_3)$

iii) $0 + l = l + 0 = l$

iv) $l + (-l) = 0$

$(L, +)$ é un gruppo abeliano perché L é un campo $\Rightarrow$ gli assiomi relativi all'addizione sono verificati

v) $(k_1 k_2) l = k_1 (k_2 l)$

vi) $(k_1 + k_2) l = k_1 l + k_2 l$

vii) $k (l_1 + l_2) = k l_1 + k l_2$

viii) $1 l = l$

Gli assiomi relativi alla moltiplicazione sono tutti verificati perché K é un sottocampo di L ($\Rightarrow K$ é un campo $\Rightarrow K$ é un anello comm. con id.)

$\square$

ESERCIZIO 12

Dim. il seguente teorema:

Sia $K \subseteq L \subseteq M$ una torre di estensioni di campi.

Se $[M:L] < \infty$, $[L:K] < \infty$, allora $[M:K] < \infty$ e

$[M:K] = [M:L][L:K]$.

DIM

Siano $[M:L] = m$, $[L:K] = \ell$

Sia $\{\alpha_1, \dots, \alpha_m\}$ una base per M su L

Sia $\{\beta_1, \dots, \beta_\ell\}$ " " " L su K

i) Dobbiamo dim. che $B = \{\alpha_i \beta_j : 1 \leq i \leq m, 1 \leq j \leq \ell\}$ è una base per M su K:

$$\mu \in M \Rightarrow \mu = \sum_{i=1}^{m} a_i \alpha_i, \quad a_1, \dots, a_m \in L$$

in particolare $a_i = \sum_{j=1}^{\ell} b_{ij} \beta_j$, $b_{i1}, \dots, b_{i\ell} \in K$

$$\therefore \mu = \sum_{i=1}^{m} a_i \alpha_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{\ell} b_{ij} \beta_j \right) \alpha_i = \sum_{i=1}^{m} \sum_{j=1}^{\ell} b_{ij} \beta_j \alpha_i$$

$$\Rightarrow M = \mathrm{span}_K(B)$$

ii) Ora dobbiamo dim. che B è linearm. indipendente

Supp. $\sum_{i=1}^{m} \sum_{j=1}^{\ell} b_{ij} \beta_j \alpha_i = 0$, allora $\sum_{i=1}^{m} \left(\sum_{j=1}^{\ell} b_{ij} \beta_j \right) \alpha_i = 0$

Allora, poiché $\{\alpha_1, \dots, \alpha_m\}$ è lin. indip., $\sum_{j=1}^{\ell} b_{ij} \beta_j = 0$

Poiché $\{\beta_1, \dots, \beta_\ell\}$ è lin. indip., $b_{ij} = 0 \ \forall i, j$

$\therefore$ B è lin. indip.

$$\therefore [M:K] = |B| = m\ell = [M:L][L:K] \qquad \square$$

ESERCIZIO 13

Trova un polinomio monico $f(t) \in \mathbb{Q}[t]$ di grado 4 t.c. $f(\sqrt{2}+\sqrt{3}) = 0$.
Mostra che f non ha radici razionali.

$$m_{\sqrt{2}+\sqrt{3}} = t^4 - 10t^2 + 1$$

$$t^2 = x \Rightarrow x^2 - 10x + 1$$

$$x_{1,2} = \frac{10 \pm \sqrt{100-4}}{2} = \frac{10 \pm \sqrt{96}}{2}$$

$$\Rightarrow t_1, t_2 = \sqrt{\frac{10 \pm \sqrt{96}}{2}} \notin \mathbb{Q}$$

ESERCIZIO 14

Verificare le seguenti asserzioni:

i) Un polinomio di grado 1 è irriducibile

ii) $f \in K[x] - \{0\}$ ha una radice $r \in K \Rightarrow f$ riducibile

iii) Sia $f \in K[x]$ un polinomio di grado 2.
Allora f è irriducibile $\Leftrightarrow$ f non ha una radice $r \in K$

i) $f = gh$, $g, h \in K[x] - \{0\}$ non costanti
$\Rightarrow \deg(g) \geq 1$, $\deg(h) \geq 1 \Rightarrow \deg(f) = \deg(g) + \deg(h) > 1$ ↯

ii) $f(r) = 0 \Rightarrow (x-r) \mid f \Rightarrow f$ riducibile

iii) $P =$ f irriducibile ; $Q =$ f non ha una rad. razionale
Il contronominale di $P \Rightarrow Q$ è $(\neg Q) \Rightarrow (\neg P)$
cioè: se f ha una rad. razionale allora f è riducib.
Il contronominale di $Q \Rightarrow P$ è $(\neg P) \Rightarrow (\neg Q)$
cioè: se f è riducibile allora f ha una rad. raz.
$\deg(f) = 2$, f riducibile $\Rightarrow f = gh$, $\deg(g) = \deg(h) = 1$
$\Rightarrow$ f ha una radice razionale

Lezione 11

In questa lezione, tutti gli anelli sono commutativi con identità. Vedere le sezioni 1 e 2 della lezione 7 per le definizioni. Di solito indichiamo gli anelli con R.

1. Ideali e anelli quoziente

Sia $f : R \to S$ un omomorfismo di anelli commutativi, e

$$I = \ker(f) = \{r \in R \mid f(r) = 0\}$$

Allora, I non contiene 1_R poiché $f(1_R) = 1_S$. Pertanto, I non è un sottoanello di R. Tuttavia, se guardiamo solo alla struttura additiva di R, vediamo che I è un sottogruppo di $(R, +)$.

Lemma 1.1. *Sia $f : R \to S$ un omomorfismo di anelli commutativi e $I = \ker(f)$. Allora,*

$$r \in R, \quad s \in I \implies rs \in I$$

Dimostrazione. $f(rk) = f(r)f(s) = f(r)0 = 0$.

C.V.D.

Definizione 1.2. Un sottogruppo I di R è un ideale se e solo se

$$r \in R, \quad s \in I \implies rs \in I$$

Esempio 1.3.

- Sia n un intero positivo. Allora $n\mathbb{Z}$ è un ideale di $\mathbb{Z}$.
- Sia R un anello e r un elemento di R. Quindi, la valutazione $\mathrm{ev}_r(f) = f(r)$ in r definisce un omomorfismo da $R[x]$ a R, e $\ker(\mathrm{ev}_r) = \{\, f \in R[x] \mid f(r) = 0 \,\}$.
- Se $a \in R$ allora
$$(a) = \{\, ra \mid r \in R \,\}$$
è un ideale di R. Un tale ideale si chiama ideale principale.

Nota 1.4. Se $r \in I$ allora (r) è un sottoinsieme di I (che è anche un ideale di R).

In particolare, poichè ogni sottogruppo di un gruppo abeliano è normale, ne consegue che se I è un ideale di R allora R/I ha la struttura di un gruppo abeliano.

Lemma 1.5. *Sia I un ideale di R. Allora, il gruppo abeliano R/I è un anello commutativo con identità rispetto a $[r][s] = [rs]$.*

Dimostrazione. Dimostriamo che la moltiplicazione è ben definita. Il resto dei dettagli è lasciato allo studente. Supponiamo che $x, y \in [r]$ e $u, v \in [s]$. Allora, $x = y + j$ e $u = v + j'$ per $j, j' \in I$. Quindi,

$$\begin{aligned} xu - yv &= (y + j)(v + j') - yv = yv + jv + yj' + jj' - yv \\ &= jv + yj' + jj' = jv + j'y + jj' \in I \\ &\implies [xu] - [yv] = [xu - yv] = 0 \end{aligned}$$

C.V.D.

Definizione 1.6. Un ideale I di R è proprio se $I \neq R$. Un ideale I di R è massimale se e sole se

- I è proprio.
- Se J è un ideale di R che contiene I allora $J = I$ o $J = R$.

Esempio 1.7. Sia K un campo. Allora (x) è un ideale massimale di $K[x]$, poichè un ideale strettamente più grande includerebbe anche K, e quindi sarebbe uguale a $K[x]$.

Nell'esempio precedente, il quoziente dell'anello $K[x]$ per l'ideale massimale (x) era un campo. In generale abbiamo:

Proposizione 1.8. *I è un ideale massimale di R se e solo se R/I è un campo.*

Dimostrazione. Sia I un ideale massimale di R. Dobbiamo dimostrare che ogni elemento diverso da zero di R/I ha un inverso moltiplicativo. Per definizione, $[x] \in R/I$ è diverso da zero se e solo se $x \notin I$. Sia

$$J = \{i + rx \mid i \in I, \quad r \in R\}$$

Si verifica facilmente che questo è un ideale di R. Inoltre, poiché $x \in J$, I è un sottoinsieme proprio di J. Quindi $J = R$. In particolare, esiste $i \in I$ e $r \in R$ tale che

$$1 = i + rx$$

In altre parole $[1] = [r][x]$.

Viceversa, supponiamo che R/I sia un campo e J sia un ideale che contiene propriamente I. Sia $a \in J - I$. Allora, $[a]$ è diverso da zero e quindi esiste $b \in R$ tale che $[a][b] = [1]$. Quindi, esiste $i \in I$ tale che $ab + i = 1$. Poiché J è un ideale, abßJ. Poiché J è un gruppo abeliano $1 = ab + i \in J$. Poichè gli ideali sono chiusi sotto la moltiplicazione

$$r \in R \implies r = (r)(1) \in J \implies R = J$$

C.V.D.

Esempio 1.9. Sia n un intero positivo. Se $n = ab$ è composto allora $(n) \subsetneq (a)$, $(n) \subsetneq (b)$. Dunque (n) non è un ideale massimale di $\mathbb{Z}$. Se n è primo, allora $\mathbb{Z}/(n\mathbb{Z})$ è un campo, e quindi (n) è massimale.

Lemma 1.10. *Sia K un campo e I un ideale di $K[x]$. Allora esiste $f \in K[x]$ tale che $I = (f)$.*

Dimostrazione. Se $I = 0$ allora $I = (0)$. Supponiamo che $I \neq 0$ e sia $f \in I - \{0\}$ un elemento di grado minimo. Se $\deg(f) = 0$ allora $(f) = K[x]$ e $(f) \subseteq I$. Dunque $I = (f)$. Supponiamo che $\deg(f) > 0$ e $g \in I$. Per il teorema della divisione,

$$g = qf + r, \qquad r = 0 \quad o \quad \deg(r) < \deg(f)$$

In virtè della minimalità di $\deg(f)$, segue che $r = 0$. Così, $g \in (f)$.

C.V.D.

Proposizione 1.11. *Siano K un campo e $f \in K[x]$. Allora (f) è massimale se e solo se f è irriducibile.*

Dimostrazione. Il contropositivo di "f è irriducibile implica che (f) è massimale" è "(f) non è massimale implica che f è riducibile". Supponiamo che (f) non sia massimale e sia I un ideale che contiene propriamente (f). Per il lemma precedente, $I = (g)$ per qualche

$g \in K[x]$. Scrivi $f = gh$, $h \in K[x]$. Se $\deg(h) = 0$ allora $(f) = (g)$. Quindi, $\deg(h) > 0$ e così f è riducibile.

Viceversa, il contropositivo di "(f) è massimale implica che f è irriducibile è "f è riducibile implica che (f) non è massimale. Infatti se $f = gh$ dove sia g che h hanno grado positivo allora $(f) \subsetneq (g)$, $(f) \subsetneq (h)$.

C.V.D.

In generale, diciamo che un dominio d'integrità R è un dominio ad ideali principali (spesso abbreviato PID) se ogni ideale di R è della forma (r) per qualche $r \in R$.

Esempio 1.12. Sia K un campo allora $K[x]$ è un PID. Allo stesso modo, il teorema della divisione mostra che $\mathbb{Z}$ è un PID. L'anello $K[x, y]$ non è un PID, poiché x e y sono variabili indipendenti. Quindi $(x, y) \neq (z)$ per qualche $z \in K[x, y]$.

Definizione 1.13. Sia R un dominio d'integrità. Allora, un elemento $r \in R$ è irriducibile se e solo se (1) r è diverso da zero, (2) r non è un'unità, (3) ogni volta che $r = st$ allora o s o t è un'unità.

Esempio 1.14. Gli elementi irriducibili di $\mathbb{Z}$ sono i numeri primi ei loro inversi additivi. Gli elementi irriducibili di $K[x]$ sono i polinomi irriducibili.

Definizione 1.15. Un dominio a fattorizzaione unica è un dominio d'integritá R tale che

- Se $r \in R$ è un elemento diverso da zero che non è un'unità allora r può essere scritto come un prodotto $r = r_1 \dots r_n$ dove $r_1, \dots r_n$ sono irriducibili.
- Se $r = r'_1 \cdots r'_m$ è un'altra rappresentazione di r come prodotto di elementi irriducibili allora $m = n$ e c'è una permutazione π di $\{1, \dots, n\}$ tale che $r_j r'_{\pi(j)}$ è un'unità per $j = 1, \dots, n$.

Teorema 1.16. *Un PID è un dominio di fattorizzazione unica.*

Dimostrazione. Omessa (purtroppo).

C.V.D.