Algebra

Fra

January 17, 2025

Abstract

Si descrivono in questo documento i contenuti del corso di Algebra per il corso di studi di informatica presso l'università di pisa. Sono presenti degli approfondimenti per facilitare la comprensione del materiale. Si terrà aperta la possibilità di ampliare il file con applicazione di carattere crittografico.

Contents

1 Concetti introduttivi

1.1 Insiemi

1.1.1 Introduzione alla teoria degli insiemi

Qualsiasi collezione di oggetti è considerato un insieme. incluso l'insieme vuoto: $\emptyset = \{\}$
Diciamo che A è un sottoinsieme di B se soltanto se ciascun membro di A fa anche parte di B

$$A \subseteq B \iff (x \in A \implies x \in B)$$

Definiamo inoltre

$$A = B \iff (A \subseteq B \text{ e } B \subseteq A)$$

Per ogni insieme è sempre vero dire

$$\emptyset \subseteq A \quad \forall A$$

Si può dimostrare ricordandoci un po' di logica. siccome nessun elemento può appartenere a un insieme 'vuoto',la prima proposizione P è sempre falsa $x \in \emptyset$ analizzando le tabelle per il calcolo proposizionale si nota che l'implicazione è sempre vera quando P è falsa.
Dunque $\emptyset \subseteq A \quad \forall A$

1.1.2 Operazioni su insiemi

- Unione

$$A \cup B = \{x \mid x \in A \text{ o } x \in B\}$$

$$\bigcup_{i\in I} A_i = \{x \mid x \in A_i \text{ per qualche } i \in I\} = \{x \mid \exists i \in I \text{ abbiamo } x \in A_i\}$$

- Intersezione

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}$$

$$\bigcap_{i\in I} A_i = \{x \mid x \in A_i \text{ per ogni } i \in I\} = \{x \mid \forall i \in I \text{ abbiamo } x \in A_i\}$$

- Complemento
  Dati Ω 'set universale' e A un sottoinsieme di Ω

$$A^C = \Omega - A = \{x \in \Omega \mid x \notin A\}$$

1.2 Richiami sulle funzioni

- informalmente, dati due insiemi A e B, diciamo che una certa regola di assegnamento f prende inuput da A (Dominio) e mappa ciascuno a un unico elemento appartenente a B.
- Scriviamo $f : A \to B$
- il set di tutti i possibili output viene chiamato immagine di f e si rappresenta some $f(A)$

- La funzione f è iniettiva se

$$(f(a_1) = f(a_2) \implies a_1 = a_2) \iff (a_1 \neq a_2 \implies f(a_1) \neq f(a_2))$$

- La funzione è suriettiva se

$$B = f(A) \iff (\forall b \in B \quad \exists a \in A \mid f(a) = b)$$

- se una funzione è iniettiva e suriettiva allora è invertibile e si può chiamare 'bigezione'

1.2.1 Composizione di funzioni

- Dati tre insiemi non vuoti A, B e C e le funzioni $\phi : A \to B$ e $\psi : B \to C$
- si definisce una nuova funzione $\phi \circ \psi$ chiamata 'composizione di ϕ e ψ
- si nota che $\phi \circ \psi : A \to C$
- Dato $\phi : A \to B$ e $\psi : B \to C$ se $A_1 \subseteq A$ e $A_2 \subseteq A$

$$\phi(A_1 \cup A_2) = \phi(A_1) \cup \phi(A_2)$$

$$\phi(A_1 \cap A_2) \subseteq \phi(A_1) \cap \phi(A_2)$$

  Si nota che per la seconda proprietà abbiamo un incluso e non un uguale. Possiamo fare una supposizione affinchè la relazione esista con l'uguale?
  Dimostrazione:

$$b \in \phi(A_1 \cap A_2) \implies (\exists a \in A_1 \cap A_2 \mid \phi(a))$$
$$(\exists a \in A_1 \cap A_2 \mid \phi(a)) \implies (a \in A_1 \text{ e } a \in A_2)$$
$$(a \in A_1 \text{ e } a \in A_2) \implies (b = \phi(a) \in \phi(A_1) \text{ e } b = \phi(a) \in \phi(A_2))$$

- se ϕ e ψ sono suriettive allora anche $\psi \circ \phi$ è suriettiva.
  Dimostrazione:
  Si nota che $(\psi \circ \phi)(a) = \psi(\phi(a))$ Dunque se f è suriettiva possiamo dire che per ogni $b \in B$ eiste $a \in A$ tale che $b = \phi(a)$. Siccome g è suriettiva possiamo dire che per ogni $c \in C$ eiste un $b \in B$ tale che $c = \psi(b) = \psi(\phi(a)$. Dunque per ogni $c \in C$ esiste $a \in A$ tale che $\psi(\phi(a)) = c$

- se ϕ e ψ sono iniettive allora anche $\psi \circ \phi$ è iniettiva
  Dimostrazione:
  Si nota che $(\psi \circ \phi)(a) = \psi(\phi(a))$. Dunque se ϕ si può dire che dati a_1 e a_2

$$\phi(a_1) = f(a_2) \iff a_1 = a_2$$

  . siccome anche ψ è iniettva si può dire che dati b_1 e b_2

$$\psi(b_1) = \psi(b_2) \iff b_1 = b_2$$

  allora

$$\psi(\phi(a_1)) = \psi(\phi(a_2)) \implies \phi(a_1) = \phi(a_2) \implies a_1 = a_2$$

  Dunque $\psi \circ \phi$ è iniettiva

- se ϕ e ψ sono bigezioni allora anche $\psi \circ \phi$ è una bigezione
  Dimostrazione:
  Se ψ è una bigezione vuol dire che è sia iniettiva che suriettiva.
  se ϕ è una bigezione vuol dire che è sia iniettiva che suriettiva.
  Per quanto dimostrato prima $\psi \circ \phi$ è sia iniettiva che suriettiva. Perciò $\psi \circ \phi$ è a sua volta una bigezione

- Inoltre $(\phi \circ \psi)^{-1} = \psi^{-1} \circ \phi^{-1}$

Proprietà Sock-Shoes
Chiamiamo la funzione a togliersi le calze. Chiamiamo la funzione b togliersi le scarpe. è chiaro che la funzione $a \circ b$ fa si che ci togliamo sia le scarpe che la calze. Per le regole della composizione è chiaro che ci sitamo levando prima le scarpe e poi le calze come è giusto che sia. Definiamo la funzione 'rimettersi calze e scarpe' questa sarà l'inverso di togliersi calze e scarpe. Siccome prima devo mettermi le calze a^{-1} e poi le scarpe b^{-1} abbiamo:

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$$

Controlliamo :

$$a \circ b \circ (b^{-1} \circ a^{-1})$$

$$a \circ (b \circ b^{-1}) \circ a^{-1}$$

$$a \circ e \circ a^{-1} = a \circ a^{-1} = e$$

Nell'altro senso:

$$(b^{-1} \circ a^{-1}) \circ a \circ b$$

$$b^{-1} \circ (a \circ a^{-1}) \circ b$$

$$b \circ e \circ b^{-1} = b \circ b^{-1} = e$$

Dunque abbiamo dimostrato che

$$(a \circ b)^{-1} = b^{-1} a^{-1}$$

Questa proprietà sarà necessaria per la teoria dei gruppi. Si pensi a un gruppo di funzioni sulla composizione. Se il gruppo è commutativo tutto ciò è abbastanza inutile.

1.3 $P \neq NP$

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.
- 'Una data matrice quadrata con elementi ineri è invertibile?' è un problema P in quanto calcolare il determinanti con l'algoritmo di gauss ha una complessità $O(n^3)$.
- 'Data una coppia di numeri interi positivi a e b vale $mcd(a, b) = 1$' è un problema P, l'algoritmo di euclide è nella classe di complessità polinomiale.
- NP è l'insieme dei problemi decisionali con la seguente proprietà: se la risposta è SI, allore esiste una dimostrazione di questo fatto che può essere verificata in tempo polinomiale. Intuitivamente NP è l'insieme dei problemi decisionali in cui è possibile verificare una risposta 'SI' se si dispone della soluzione.
- Decidere se un dato grafo ammette una colorazione con un insieme di k colori per un dato $k > 2$ è un problema NP (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.
- Dato un insieme di numeri interi S, esiste un sottoinsieme non vuoto di S la cui somma di elementi è zero (o un altro valore fisso)? è un problema $NP - Difficile$

Il test di primalità di Agrawal-Kayal-Saxena determina se un dato intero positivo è primo in tempo polinomiale.

1.4 Divide et Impera

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

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

Esempio:
Calcolo $x^2 8$:

- $x^2 8 = (x^1 4)^2$
- $x^1 4 = (x^7)^2$
- $x^7 = x \cdot (x^3)^2$
- $x^3 = x \cdot (x)^2$

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

```
int exp(int x, int n){
    int y;
    if(n == 0) return 1;
    else{
        y = exp(x, n/2);
        if( n % 2 == 0 ) return y*y;
        else return y*y*x;
    }
}
```

Un esempio di applicazione può essere in un anello quoziente $\mathbb{Z}_n$, ('metodo delle quadrature successive').

2 Aritmetica

2.1 Principi di induzione e teoremi di base

Principio di Buon Ordinamento:
Sia $\mathbb{N}$l'insieme degli interi non negativi e S un sottoinsieme di 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

- $0 \in S$
- $n \in S \implies n+1 \in S$

Allora $S = \mathbb{N}$

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 implichi che $P(k+1)$ sia vera. Allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Dimostrazione:
Supponiamo che l'insieme

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

sia non vuoto. Allora S ha un elemento minimo s. Per ipotesi 0 non è un elemento di S. Quindi $s \geq 1$. In particolare $s-1$ non è un elemento di S, poichè s è il più piccolo elemento di S e $s \geq 1$. Ma dunque $P(s-1)$ è vera. Per ipotesi ciò implica che $P(s)$ è vera. Dunque s non appartiene a S. Questa è una contraddizione $\implies S = \emptyset$. Dunque sia S', l'insieme contenente i naturali k per i quali $P(k)$ è vera, allora $S = \mathbb{N}$.

Definizione: (1.1)
Siano a e b interi diversi da zero. Allora l'insieme $S = \{c \in \mathbb{N}^* \text{ t.c. } a \mid c,\ b \mid c\}$ è non vuoto siccome $\pm ab \in S$. L'elemento più piccolo di S si chiama minimo comune multiplo.

Nota: 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: La forma completa del principio d' induzione implica la seguente forma forte di induzione:
Sia $P(n)$ una proposizione con $n \in \mathbb{N}$. Supponiamo che

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

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

Utilizzo del Principio d'induzione

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Dimostrazione $\forall n \geq 1$
Dato S l'insieme si tutti gli interi positivi per i quali la formula è corretta.

Caso base
Siccome per $n = 1$ troviamo che la formula da il risultato corretto $1 \in S$

passo induttivo

supponiamo $n \geq 1$ allora $n \in S$ dobbiamo dimostrare che $n+1 \in S$

$$\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + n + 1 = \frac{n^2 + n + 2n + 2}{2}$$

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

Per il primo principio dell' induzione abbiamo dimostrato la formula di Gauss.

Dimostrazione per Assurdo:
Un modo per dimostrare che un proposizione P è vera è assumere che $\neg P \implies Q \wedge (\neg Q)$ è vera poichè $Q \wedge (\neg Q)$ è sempre falsa, segue che P è vera.

Definizione numero primo: (1.2)
Un numero primo p è un intero maggiore di 1 che non ha divisori interi diversi da 1 e p

Lemma: (1.5)
Ogni intero maggiore di 1 ha un fattore primo.

dimostrazione:
Si dimostra per induzione forte che ogni intero $n > 1$ ha un fattore primo. Per il caso base $n = 2$, abbiamo che 2 è primo ed è un fattore di se stesso. Supponiamo ora che tutti i numeri maggiori di 1 e minori di n abbiano un fattore primo. Per dimostrare che n ha un fattore primo distinguiamo due casi

- n **primo**
  Poichè n è fattore di se stesso, n ha un fattore primo quando n è primo.
- n **composto**
  Poichè n non è primo, ha una fattorizzazione $n = ab$ dove $1 < a, b < n$. Allora per l'ipotesi induttiva forte a ha un fattore primo. Dunque se $p \mid a$ e $a \mid n$ allora n ha un fattore primo

Teorema: (1.6)
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 in S. Chiaramente nessun elemento di S può dividere $m+1$. Dunque o m è primo o esiste un fattore primo che non è contenuto in S. Ma questo contraddice l'ipotesi perciò S è infinito.

2.1.1 Esercizi

Esercizio 1:
Dimostrare che $n > 3 \implies n! > 2^n$.

Usiamo il primo principio d'induzione riordinando e partendo da 4. si verifica che $4! > 2^4$. Ora supponiamo che $n! > 2^n$ sia vera. se ciò implica la condizione per $n+1$ allora per il principio di induzione abbiamo dimostrato questa proprietà:

$$n + 1! > 2^{n+1} \implies n + 1 \cdot n! > 2 \cdot 2^n$$

Siccome n è maggiore o uguale a 4, abbiamo $n+1 > 2$ e dunque grazie alla supposizione di prima abbiamo verificato la proposizione per $n+1$

Esercizio 2:
Dimostrare che per ogni $n \in \mathbb{N}$ vale

$$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

caso base:

$$\sum_{i=0}^{1} i^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$$

passo induttivo:

$$\frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{n+1(n+2)(2n+3)}{6}$$
$$\frac{n(n+1)(2n+1)+6(n^2+2n+1)}{6} = \frac{n+1(n+2)(2n+3)}{6}$$
$$\frac{(n^2+n)(2n+1)+6(n^2+2n+1)}{6} = \frac{(n^2+3n+2)(2n+3)}{6}$$
$$\frac{2n^3+9n^2+13n+6}{6} = \frac{2n^3+3n^2+6n^2+9n+4n+6}{6}$$

Esercizio 3:
Dimostrare che per ogni intero positivo maggiore di 1 è un prodotto di numeri primi

caso base:
Osserviamo che $n = 2$ è primo dunque è perciò prodotto di fattori primi in quanto è se stesso primo.
passo induttivo:
Supponiamo che esistano a, b per cui è vera la proposizione. Dunque deve valere $a = p_1^{\delta_1} \cdots p_k^{\delta_k}$ e $b = q_1^{\epsilon_1} \cdots q_m^{\epsilon_m}$ con p_i e q_i primi. Se n è primo allora è fattore di se stesso dunque vale la proprietà. se n è composto lo possiamo scrivere come il prodotto di due a, b con $1 < a, b < n$. Siccome la supposizione ci porta a dire che$n$ è a sua volta un prodotto di primi allora in teorema è confermato per ogni $n \in \mathbb{N}$ per la forma forte del principio d'induzione.

Esercizio 4:
Dimostrare che il principio di buon ordinamento implica il principio d'induzione.

Supponiamo che il principio di buon ordinamento sia vero. Definiamo $S \subseteq \mathbb{N}$ tale che $0 \in S$ e $n \in S \implies n+1 \in S$. Prendiamo l'insieme $S' = \mathbb{N} - S$. Esso dovrebbe avere un elemento minimo m se supponessimo per assurdo che non sia vuoto e dunque negassimo il principio d'induzione. Per ipotesi $0 \in S$ dunque $0 \notin S'$. m a sua volta può essere sempre scritto come un $q + 1$ dove $q \in \mathbb{N}$. q non può appartenere a S' perchè abbiamo definito m essere l'elemento minimo di S'.Se $q \in S$ avremmo $q + 1 \in S$ per ipotesi e dunque concluderemmo $m \notin S$. Siccome siamo incorsi in una contraddizione $S' = \emptyset$ che implica $S = \mathbb{N}$

Esercizio 5:
Dimostrare che il principio d'induzione completo è implicato dal principio d'induzione debole.

Supponiamo che il prcincipio di induzione debole sia vero. Dato $S \subseteq \mathbb{N}$ tale che $0 \in S$ e $\{0, 1, ..., n\} \subseteq S \implies n+1 \in S$ Definiamo la funzione booleana'proposizione' $P(n)$ che risulta vera quando $\{0, 1, ..., n\} \subseteq S$. Definiamo l'insieme $S' = \{n \in \mathbb{N} \text{ t.c. } P(n) \text{ è vera}\}$ $P(0)$ è vera per ipotesi. $P(k)$ è vera quando $k \geq 0$. Si ha che $\{0, 1, ..., k\} \subseteq S$ dunque per ipotesi abbiamo $k + 1 \in S \implies \{0, 1, ..., k, k + 1\} \subseteq S$ dunque $P(k + 1)$ è vera. Questo significa che $k + 1 \in S'$. Ritroviamo che $0 \in S'$ e che $n \in S' \implies n + 1 \in S'$ dunque $S' = \mathbb{N}$ dunque $P(n)$ è valida per ogni $n \in \mathbb{N}$. ma per definizione $P(n)$ descrive gli n per cui è valido il principio d'induzione forte. Quindi il principio d'induzione debole implica il principio d'induzione forte.

2.2 Teorema della Divisione con Resto

Teorema Esistenza (2.1)
Siano a e b interi non negativi tale che $a > 0$. Allora esistono interi $q \geq 0$ e $0 \leq r < 0$ tale che $b = qa + r$

Dimostrazione:

Sia
$$S = \{b - ax \text{ t.c. } x \text{ è un intero non negativo e } b - ax \geq 0\}$$
Allora S è non vuoto perchè $b - ax = b \geq 0$ se $x = 0$. Allora il principio di buon ordinamento implica che S ha un elemento minimo r. Per costruzione $r = b - qa$ per qualche $q \geq 0$. Supponiamo $r \geq a$ allora $r - a = b - qa - a = b - a(q + 1) \geq 0$ che contraddice la minimalità implicata dal principio di buon ordinamento. Segue $0 \leq r < a$ con $b = qa + r$

Teorema Unicità (2.2)

Siano a e b interi non negativi tale che $a > 0$. Sia $b = qa + r$ con $q \geq 0$ e $0 \geq r < a$ si ha che la coppia (q, r) è unica.

Dimostrazione:
Supponiamo che esista (q', r') un altra coppia che soddidsfa $b = q'a + r'$ con $q' \geq 0$ e $0 \leq r' < a$. Dopo aver scambiato (q, r) con (q', r'), se necessario, si supponga $r \geq r'$. Allora

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

$$a(q' - q) = (r - r') \geq 0 \implies 0 \leq r - r' < a \implies 0 \leq \frac{r - r'}{a} < 1$$

$$q' - q = \frac{r - r'}{a}$$

Siccome $q' - q$ è un intero allora $q' - q = 0$ e dunque

$$r' = b - q'a = b - qa = r$$

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

2.2.1 Esercizi

Esercizio 8: Sia d l'elemento minimo di $S = \{s \in \mathbb{N}^* \text{ t.c.} s = au + bv \text{ con } u, v \in \mathbb{Z}\}$.
Dimostrare che $d \mid a$ e $d \mid b$.
Supponiamo per assurdo che $d \nmid a$. Allora

$$a = qd + r \implies a = q(au + bv) + r$$

$$r = a(1 - qu) + (-qv)b \text{ con } 0 < r < d$$

Dunque $r \in S$ ciò contraddice la minimalità perciò $d \mid a$.
Ripetendo lo stesso procedimento per b si ottiene $d \mid a \wedge d \mid b$

2.3 Basi

Sia $n \in \mathbb{N}$. Esiste allora una sequenza di numeri interi $\{a_0, ..., a_k\}$ tale che ogni $a_j \in \{0, ..., 10\}$ e

$$n = a_k 10^k + ... + a_1 10 + a_0$$

La stringa $\{a_k, ..., a_0\}$ si chiama rappresentazione in base 10 dell 'intero positivo n.

Nota: (3.1) Se $k > 0$, si assume che $a_k \neq 0$ per evitare di aggiungere una serie di zeri eccessiva
Siano $n \geq 0$ e $b \geq 2$ interi. Allora, si dice che n ha una rappresentazione in base b se esiste una sequenza di interi $\{a_0, ..., a_k\}$ tale che ogni $a_j \in \{0, ..., b - 1\}$

$$n = a_k b^k + ... + a_0$$

La stringa $\{a_k, ..., a_0\}$ si chiama rappresentazione in base b dell'intero n.

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

$$216 = 2^7 + 2^6 + 2^4 + 23 = 128 + 64 + 16 + 8$$

La rappresentazione di 216 in base 3 è 22000

$$216 = 3^4 \cdot 2 + 3^3 \cdot 2 = 162 + 54$$

La rappresentazione di 216 in base 60 è $(3, 36)$

$$216 = 3 \cdot 60 + 36$$

Teorema: (3.3)
Fissato un intero $b \geq 2$, ogni intero positivo può essere rappresentato in base b: cioè, n può essere univaocamente scritto come

$$n = a_k b^k + ... + a_0$$

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

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

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

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

$$q = q_m b^m + ... + q_0$$

Ne segue che

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

Siccome $r < b$ abbiamo che $\{q_m, ..., q_0, r\}$ è una rappresentazione in base b. Per l'unicità, sia S l'insieme di tutti gli interi positivi n che non hanno rappresentazione unica in base b. Se S non è vuoto, ha un elemento minimo n. È chiaro che $n \geq b$. Siano,

$$n = a_k b^k + .. + a_1 b + a_0$$

$$n = c_l b^l + .. + c_1 b + c_0$$

due diverse rappresentazioni di n in base b. Allora

$$n = (a_l b^{k-1} + ... + a_1)b + a_0 = Aq + a_0$$

$$n = (c_l b^{l-1} + ... + c_1)b + c_0 = Cq + c_0$$

Dove $0 \leq a_0 < b$ e $0 \leq c_0 < b$. Ma per il teorema della divisione quoziente e resto sono unici. Ricaviamo $a_0 = c_0$, e quindi $A = C$ha due diverse rappresentazioni in bse b. Ma $A < n$ dunque S è vuoto.

Nota: (3.4) La dimostrazione fornisce anche un algoritmo per calcolare la rappresentazione in bse b del numero n:

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

dove $\{r_k, ..., r_0\}$ è la rappresentazione di n in base b.

2.4 Massimo comun divisore

Definizione: (1.1)
Sia S un sottoinsieme di numeri reali, $\mathbb{R}$. Allora $m \in \mathbb{R}$ è un elemento massimo di S se

- $m \in S$
- $s \in S \implies s \leq m$

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' elemento massimi di S. Allora $m \leq m'$ perchè m' è massimo. Allo stesso modo $m' \leq m$ perchè 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. Scegliamo un elemento $s \in S$ e sia $S' = S - \{s\}$. Quindi S' ha $n \geq 1$ elementi. Poiche $P(n)$ è vera, ne consegue che S' ha un elemento massimo, chiamiamolo s'. Chiaramente il massimo m di s e s' è un elemento massimo di S. Dunque $P(n+1)$ è vera. Per il principio d'induzione abbiamo dimostrato la tesi.

Nota: Se n è un intero, sia $D(n) = \{d \in \mathbb{Z} \text{ t.c. } d \mid n\}$. Si nota che $D(0) = \mathbb{Z}$

Proposizione: (1.4)
Sia n un intero diverso da zero. Allora $D(n) \subseteq \{-|n|, ..., |n|\}$. 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 $m \neq 0$ perchè $n \neq 0$. Allora

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

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

Nota: (1.6) Se $a = 0$ e $b \neq 0$ allora $mcd(a, b) = b$. La definizione di $mcd(a, b) = b$.

Nota: (1.7) Si può trovare l'mcd fattorizzando gli interi a e b vedremo poi come ci si arriva dal teorema fondamentale dell'aritmetica.

Esempio: (1.8)
mcd(60, 256) [Si ommettono gli elementi negativi di $D(n)$ in questi esempi]

$$D(60) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$

$$D(256) = \{1, 2, 4, 8, 16, 32, 64, 128, 256, \}$$

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

2.5 Algoritmo di Euclide e Identità di Bezout

2.5.1 Algoritmo di Euclide

Lemma: (2.1)
Siano a e b interi diversi da zero. Allora $\text{mcd}(a \bmod b, b) = mcd(a, b)$

Dimostrazione:
Siano $m = mcd(r, b)$ e $\mu = mcd(a, b)$ dato $a = bq + r$

$$m = mcd(r, b) \implies m \mid r \;\; m \mid b \implies a = m(nq + k) \implies m \mid a \implies m \leq \mu$$

$$\mu = mcd(a, b) \implies \mu \mid a \;\; \mu \mid b \implies r = \mu(k' - qn') \implies m \mid a \implies \mu \leq m$$

Quindi, $m = \mu$ Vale lo stesso $mcd(a + b, b) = mcd(a, b)$. Difatti si può implementare una versione meno veloce utilizzando solo sottrazioni. in questo caso si scrive a come $a + b - b$. Da qui si procede identicamente.

Algoritmo di Euclide:

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

Quando $r = 0$ l'algoritmo si ferma. abbiamo trovato il massimo comun divisore

Esempio: (2.2)

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

Algoritmo e Teorema di Divisione
Siano a e b interi diversi da zero. Applicare il teorema di divisione come segue

$$a = bq + r_1$$

$$b = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$r_2 = r_3 q_4 + r_4$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1} + 0$$

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

Esempio: (2.2)

- $mcd(54, 36)$

  $$54 = 36 + 18, \quad r_1 = 18$$
  $$36 = 18 \cdot 2 + 0 \quad r_2 = 0$$

  L'algoritmo è terminato perchè $r = 0$.
  Si nota che se pensassimo $mcd(54, 36)$ come un risultato di un primo passaggio dato dalla applicazione dell'algoritmo rispetto per $mcd(36, 54)$ dove avremmo come resto 36 noteremo che $18 \mid 36$ e avremmo potuto arrestare l'algoritmo un passo prima.

- $mcd(256, 60)$

$$256 = 4 \cdot 60 + 16, \quad r_1 = 18$$
$$60 = 16 \cdot 3 + 12 \quad r_2 = 12$$
$$16 = 12 + 4 \quad r_3 = 4$$

L'algoritmo è terminato perchè $r_3 \mid r_2$

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

2.5.2 Costruzione dell'identità di Bezout

Siano a, b interi tali che $(a, b) \neq (0, 0)$. Sia

$$S = \{au + bv \text{ con } u, v \in \mathbb{Z}\} \cap \mathbb{N}^*$$

Allora, S è non vuoto perchè $|a|, |b| \in S$. Pertanto S ha un elemento minimo m che mostreremo essere il massimo comun divisore di a e b. Abbiamo già mostrato che $m \mid a$ e $m \mid b$. Chiamando $\mu = mcd(a, b)$ osserviamo che $\mu \geq m$ in quanto m è divisore.

$$m = au + bv \implies m = \mu nu + \mu n'v \implies m = \mu(nu + n'v) \implies \mu \mid m$$

Questa breve dimostrazione è stata già svolta per spiegare il funzionamento dell'algoritmo di euclide. Quindi $\mu \mid m$, allora $\mu \leq m \implies \mu = m$ per quanto detto prima.

2.5.3 Identità di Bezout

Se a, b sono interi (entrembi non nulli e il loro massimo comun divisore è d, allora esistono due interi u, v tale che $d = au + bv$

2.5.4 Costruzione algoritmo di euclide esteso

Per trovare gli interi u e v tali che $m = au + bv$ dove $m = mcd(a, b)$, scriviamo $a = qb + r$ con $0 \leq r < b$ e facciamo la seguente osservazione.

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

Quindi si ricorda che questo processo per calcolare l'$mcd(a, b)$per riduzione termina con $mcd(m, 0)$. A quel punto, abbiamo $m = m(1) + 0(0)$. Pertanto, possiamo calcolare gli interi u e v utilizzando il seguente algoritmo di euclide

$$mcd(a, b|u, v) = mcd(qb + r, b|u, v)$$
$$mcd(r, b|u, v + qu) = mcd(b, r|v + qu, u)$$
$$mcd(m, 0|l_1(u, v), l_2(u, v))$$

Data la terminazione $m = m(1) + 0(0)$ avremmo un sistema lineare in due equazioni in u e v

$$l_1(u, v) = m$$
$$l_2(u, v) = 0$$

Esempio: (2.2)

$$mcd(4 \cdot 60 + 16, 60|u, v) = mcd(16, 60|u, v + 4u) = mcd(60, 16|v + 4u, u)$$
$$mcd(16 \cdot 3 + 12, 16|v + 4u, u) = mcd(12, 16|v + 4u, u + 3(v + 4u))$$
$$mcd(16, 12|13u + 3v, v + 4u) = mcd(12 + 4, 12|13u + 3v, v + 4u) = mcd(4, 12|13u + 3v, v + 4u + (13u + 3v))$$
$$mcd(12, 4|17u + 4v, 13u + 3v) = mcd(3 \cdot 4, 4|17u + 4v, 13u + 3v)$$
$$mcd(0, 4|17u + 4v, 13u + 3v + 3(17u + 4v)) = mcd(4, 0|64u + 15v, 17u + 4v)$$
$$64u + 15v = 1$$

$$17u + 4v = 0$$

Notiamo che le soluzioni per la prima equazione risultano avere la forma $c(\beta, -\alpha)$.In questo caso $c(4, -17)$. Inserendo nella seconda equazione risulta

$$c(64 \cdot 4 - 17 \cdot 15) = 1$$

Si ricava che $c = 1$

Algoritmo di Euclide Esteso

```
#include <bits/stdc++.h>
using namespace std;
// x and y will be given by reference to make things easier.
// Function for extended Euclidean Algorithm
int gcdExtended(int a, int b, int *x, int *y)
{
    // Base Case
    if (b == 0)
    {
        *x = 1;
        *y = 0;
        return a;
    }

    int x1, y1; // To store results of recursive call
    int gcd = gcdExtended(b, a % b, &x1, &y1);

    // Update x and y using results of
    // recursive call
    *x = y1
    *y = x1 - floor(a/b) * y1;

    return gcd;
}
```

2.5.5 Algoritmo di Euclide Esteso e equazioni diofantee

Si definisce un equazione diofantea lineare nelle incognite $x \in \mathbb{Z}$ e $y \in \mathbb{Z}$, ogni equazione del tipo

$$ax + by = c \text{ con } a, b, c \in \mathbb{Z}$$

Si nota una certa somiglianza con l'identità di bezout. Se b è d dove d è l'$mcd(a, b)$ possiamo trovare y e x tramite l'algoritmo di euclide esteso. Vediamo cosa possiamo dire sulle soluzioni di questa equazione diofantea lineare.

Teorema:(2.3)
l'equazione diofantee $ax + by = c$ ammette soluzioni se solo se $mcd(a, b)$ è un divisore di c. In particolare, se a e b sono primi tra loro. L'equazione ammette sempre soluzioni.

Dimostrazione:
poniamo $m = mcd(a, b)$ e supponiamo che x_0, y_0 sia una soluzione dell' equazione data, cioè che $ax_0 + by_0 = c$. Poichè $m \mid a$ e $m \mid b$ per si ha che $d \mid ax_0 + by_0$ e quindi $d \mid c$. Viceversa supponiamo che $d \mid c$ e dimostriamo che l'equazione ammette soluzioni intere. Essendo d un divisore di c, esiste $u \in \mathbb{Z}$ tale che $c = du$. Inoltre per l'identità di Bezout $d = ah + bk$ per qualche $h, k \in \mathbb{Z}$. Moltiplicando i membri di questa uguaglianza per u e si ottiene

$$du = ahu + bku \text{ con } h, k, u \in \mathbb{Z}$$

$$c = a(hu) + b(ku)$$

perciò $(hu, ku) \in \mathbb{Z}^2$ è una soluzione dell'equazione.

Lemma:(2.4.a)

Dati due interi a,b e $d = mcd(a,b)$ allora $mcd(\frac{a}{d}, \frac{b}{d}) = 1$

Dimostrazione:
Dato $d = mcd(a,b)$ è esprimible come combinazione lineare per l'identità di bezout. Dunque abbiamo $as + bt = d$, dividiamo entrambi i membri per d e ricaviamo $\frac{a}{d}s + \frac{b}{d}t = 1$. Siccome $d \in D(a)$ e $d \in D(b)$ allora $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Poniamo per assurdo che $mcd(\frac{a}{d}, \frac{b}{d}) = \delta > 1$ δ in quanto $mcd(a,b)$ deve dividere la combinazione lineare $\frac{a}{d}s + \frac{b}{d}t$ ma siccome la combinazione lineare è uguale a 1 allora deve dividere anche 1. impossibile siccome abbiamo supposto $\delta > 1$.

Lemma:(2.4.b)
Verificare: Se $a \mid bc$ e a e b coprimi allora $a \mid c$

dimostrazione: controllare esercizio a fine capitolo

Proposizione: (2.4)
Sia $ax + by = c$ una equazione diofantea tale che $d = mcd(a,b)$ sia un divisore di c. Detta (x_0, y_0) una soluzione particolare dell'equazione, tutte e sole le infinite soluzioni sono scrivibili come

$$\left(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}\right)$$

al variare di $k \in \mathbb{Z}$ con $\left(k\frac{b}{d}, -k\frac{a}{d}\right)$ le soluzioni dell' equazione omogenea associata $ax + by = 0$

Dimostrazione:
Sia (x_0, y_0) una fissata soluzione dell'equazione $ax+by = c$. è facile verificare che la coppia $\left(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}\right)$ è a sua volta soluzione dell'equazione al variare di $k \in \mathbb{Z}$. Infatti, sostituendo nell' equazione si ottiene $ax_0 + ak\frac{b}{d} + by_0 - bk\frac{b}{d}$ siccome $\left(k\frac{b}{d}, -k\frac{a}{d}\right)$ è soluzione dell 'omogenea abbiamo $ak\frac{b}{d} + -bk\frac{b}{d} = 0$ e quindi $ax_0 + ak\frac{b}{d} + by_0 - bk\frac{b}{d} = ax_0 + by_0 = c$. Viceversa sia $x'y'$ una soluzione. dell' equazione assegnata. Si ha quindi $ax' + by' = c = ax_0 + by_0$ cioè $a(x' - x_0) = b(y_0 - y')$ da cui $\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$. Essendo $\frac{a}{d}$ e $\frac{b}{d}$ coprimi. Da ciò segue che $\frac{b}{d}$ divide $(x' - x_0)$ e quindi esiste $k \in \mathbb{Z}$ tale che $x' - x_0 = k\frac{b}{d}$ cioè $x' = x_0 + \frac{b}{d}$. Sostituendo $k\frac{b}{d}$ in $\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$ si ottiene

$$k\frac{b}{d}\frac{a}{d} = \frac{b}{d}(y_0 - y')$$

$$\therefore y' = y_0 - k\frac{a}{d}$$

In definitiva le soluzioni dell' equazione si ottengono sommando una soluzione particolare alle soluzioni dell'omogenea associata.

Esempio: (2.5)
Dire se $132x+51y = 9$ ammette soluzioni e, in tal caso, determinarle tutte $mcd(132, 51) = mcd(51, 30) = mcd(30, 21) = mcd(21, 9) = mcd(9, 3) = mcd(3, 0) = 3$ Dunque assume soluzione in quanto $9 = 3 \cdot 3$. Prendo l'omogenea $132x + 51y = 0$ ricaviamo che le soluzioni sono del tipo $\left(k\frac{b}{d}, -k\frac{a}{d}\right)$. Dunque abbiamo $k(17, -44)$. Tramite l'algoritmo di euclide esteso troviamo le soluzioni u, v alla equazione diofantea $132x + 51y = 3$

$$mcd(2 \cdot 51 + 30, 51|u, v) = mcd(30, 51|u, v + 2u) = mcd(51, 30|v + 2u, u)$$

$$mcd(30 \cdot 1 + 21, 30|v + 2u, u) = mcd(21, 30|v + 2u, u + v + 2u$$

$$mcd(30, 21|v + 3u, v + 2u) = mcd(21 + 9, 21|v + 3u, v + 2u) = mcd(9, 21|v + 3u, v + 2u + (v + 3u))$$

$$mcd(21, 9|2v + 5u, v + 3u) = mcd(2 \cdot 9 + 3, 9|2v + 5u, v + 3u)$$

$$mcd(3, 9|2v + 5u, v + 3u + 2(2v + 5u)) = mcd(9, 3|5v + 13u, 2v + 5u)$$

$$mcd(3 \cdot 3, 3|5v + 13u, 2v + 5u) = mcd(0, 3|5v + 13u, 2v + 5u + 3(5v + 13u)$$

$$mcd(3,0|17v+44u,5v+13u)$$
$$44u+17v=1$$
$$13u+5v=0$$

Si nota che si identificano le soluzioni $c(5,-13)=(u,v)$ dalla seconda equazione. Dalla prima equazione invece ricaviamo
$$c(44\cdot 5-13\cdot 17)=1 \implies c=-1 \implies (u,v)=(-5,13)$$
$$132\cdot -5+51\cdot 13=3$$

Abbiamo trovato una soluzione valida. Ma osservando meglio notiamo per il teorema (2.3).
$$c(132\cdot -5,51\cdot 13)=c3$$

Dunque per $c=3$ soddisfiamo l'eq di partenza e non l'identità di bezout. Ricaviamo che le soluzioni saranno $-5c+17k,13c-44k$. Dove $cd=b=9 \implies c=3 \implies (x',y')=(-15+17k,39+44k)$.

Nota: (2.5) Dunque l'algoritmo di euclide esteso trova sempre la soluzione con $k=0$ ovvero la soluzione particolare dell'equazione diofantea.Studiando l'omogenea troviamo tutte le altre soluzioni.

Nota: (2.5) Si nota che se vogliamo trovare la soluzione particolare della seguente equazione diofantea:
$$ax+by=gcd(a,b)\cdot c=b$$
basta sostituire alla prima equazione del sistema lineare il multiplo c a 1 tale che $b=cd$ dove d è l'$mcd(a,b)$. Si verifica dopo aver trovato u,v che soddisfano l'identità di bezout:
$$(nu+n'v)=1 \implies d(nu+n'v)+0=cd \implies nu+n'v=c$$

2.5.6 Lemma di Euclide

Enunciato:
Un intero $p>1$ è un numero prima se e solo se $p|ab \implies p|a \vee p|b$ per ogni intero a e b.
dimostrazione:
Supponiamo che p sia primo e $p \mid ab$. Mettiamo che $p \nmid a$ allora $mcd(a,p)=1$. Possiamo dunque scrivere per l'identità di bezout
$$ps+at=1 \text{ con } s,t\in\mathbb{Z}$$
Moltiplicando entrambi i lati per b troviamo $bps+bat=b$ ma siccome $p\mid ab$ per ipotesi $p(bs+nt)=b$ dunque $p\mid b$.
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 $a>1 \implies b<p$ perciò $p\nmid b$. Allo stesso modo $p\nmid a$.

2.5.7 Esercizi

Esercizio 1:
Sia p un numero primo. Mostra che se a è un intero e $mcd(p,a)\neq 1$ allora $p\mid a$.
Per quanto dimostrato precedentemente $D(a)=\{-|a|,...,|a|\}$, $D_(p)=\{-p,1,-1,p\}$ e $mcd(p,a)=max(D_(a)\cap D_(p)$.Mcd esiste sempre in quanto 1 divide tutti i numeri interi. Siccome $mcd(a,p)\neq 1 \implies mcd(a,p)=p$ per l'esistenza dell'mcd.
$$D(a)\cap D(p)=\{1,p\}$$
Dunque $p\in D(a) \implies p\mid a$

Esercizio 2:
Verificare: Se $a\mid bc$ e a e b coprimi allora $a\mid c$
Se a,b sono coprimi tra loro allora $mcd(a,b)=1$ possiamo perciò scrivere $as+bt=1$. A questo punto notiamo che $c=1\cdot c=(as+bt)c$. Siccome $a\mid bc$ possiamo dire $c=cas+cbt=a(cs+nt) \implies a\mid c$

Esercizio 3:
Scrivere un implementazione iterativa dell'algoritmo di euclide. E scrivere perchè termina in un numero finito di passi.

```
int mcd_euclid(int a, int b)
{
    int c;
    while(b != 0){
        c = b;
        b = a  % b;
        a = c;
    }
    return a;
}
```

L'algoritmo termina in un numero finito di passi perchè passando da $mcd(a, b) \rightarrow mcd(b, r)$ si applica il teorema di divisione col resto perciò $0 \leq r < b$. Procedendo con l'algoritmo si nota $mcd(b, r) \rightarrow mcd(r, r')$ con $0 \leq r' < r$ sempre per il th. di div col resto. Si dovrà per forza arrivare alla forma $mcd(r_i, 0)$ siccome per il teorema di divisione $0 \leq r_i < r_{i-1} < ... < b$

Esercizio 4:
Data la successione di fibonacci dove $f_{n+1} = f_n - f_{n-1}$ dimostrare che $mcd(f_{n+1}, f_n)$.

Per induzione $mcd(f_1, f_0) = mcd(1, 1) = 1$ dunque $1 \in S$.
Supponiamo che $n \in S$ in altre parole $mcd(f_n, f_{n-1}) = 1$.
$mcd(f_{n+1}, f_n) = mcd(f_{n-1}+f_n, f_n)$ ricordiamo a questo punto il lemma $mcd(b, a) = mcd(a, b) = mcd(a+b, b)$ che dimostra $mcd(f_{n-1} + f_n, f_n) = mcd(f_{n+1}, f_n) = 1$ dunque $n + 1 \in S$. Per il principio d'induzione $mcd(f_i, f_{i-1})$vale per ogni $i > 0$ con $i \in \mathbb{Z}$

Esercizio 5:
Scrivere un implementazione iterativa dell'algoritmo di euclide esteso.

```
void mcd_euclid_ext(int a, int b, int*res)
{
    int swap[3];/* swap aux vector*/
    int mat[2][2]={{1,0},{0,1}};/*aux matrix*/
    while(b != 0){
        /* update matrix */
        swap[0]=mat[0][0]; swap[1]=mat[0][1];
        mat[0][0]=mat[1][0]+(a/b)*mat[0][0];
        mat[0][1]=mat[1][1]+(a/b)*mat[0][1];
        mat[1][0]=swap[0]; mat[1][1]=swap[1];
        /* finish update*/
        /* classic ecl algo*/
        swap[2] = b;
        b = a % b;
        a = swap[2];
        /* classic ecl algo*/
    }
    bool sign=(mat[1][1]*mat[0][0]-mat[1][0]*mat[0][1]< 0);
    /* chossing c given by second row solutions*/
    res[0]=a;
    res[1]=(sign == 1)?-mat[1][1]:mat[1][1];
    res[2]=(sign == 1)?mat[1][0]:-mat[1][0];
    /* returining vars*/
}
```

Nota: La seconda equazione del algoritmo di euclide esteso è a sua volta una equazione diofantea omogenea $as + bt = 0$.

2.6 Teorema Fondamentale dell'Aritmetica

Enunciato:
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

Dimostrazione:
(Esistenza) già dimostrata negli esercizi del primo capitolo
(Unicità) Sia S l'insieme degli interi > 1 per i quali la parte di unicità del teorema fondamentale dell'aritmetica fallisce. Se S è non vuoto allora ha un elemento più puccolo n. Siano

$$n = p_1 \cdots p_k \quad n = q_1 \cdots p_l$$

due distinte fattorizzazione prime di n. Allora poichè $p_1 \mid n$ per il lemma di euclide p_1 deve dividere qualche q_j. Dopo aver riordinato i fattori possiamo scegliere $j = 1$ senza perdere di generalità. Poichè p_1 e q_1 sono entrambi primi ne consegue $p_1 = q_1$. Allora

$$m = p_2 \cdots p_k = q_2 \cdots q_l$$

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

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

- Se $a, b \in \mathbb{R}$ e $b \neq 0$ allora esistono $q, r \in R$ tali che $a = bq + r$e $r = 0$ oppure $\delta(r) < \delta(b)$
- Se a e b sono diversi da zero allora $\delta(a) \leq \delta(ab)$

Nel caso degli interi, abbiamo utilizzato $\delta(a) = a$. Altro caso in cui si può verificare la fattorizzazione in pezzi "irriducibili" riguarda i polinomi. Anche in questo caso, abbiamo il teorema di divisione, con la finzione di grado al posto del valore assoluto: $deg(p) \leq deg(pq)$. Torneremo si questo argomento più avanti.

Come prima applicazione, abbiamo la seguente proposizione utile, che mostra che possiamo calcolare l'mcm efficientemente 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

$$|ab| = mcm(a, b)mcd(a, b)$$

Dimostrazione:
Senza perdità di generalità possiamo assumere che a e b sono interi positivi (si cambia il segno di a e b se sono negativi). Sia A l'insieme dei fattori primi di a e B l'insieme dei fattori primi di b. Sia $P = \{p_1, ..., p_k\}$=$A \cup B$. Allora

$$a = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$$
$$b = p_1^{\delta_1} \cdots p_k^{\delta_k}$$

dove permettiamo agli esponenti δ_i, ϵ_j di essere zero. Allora

$$mcm(a, b) = p_1^{max(\epsilon_1, \delta_1)} \cdots p_k^{max(\epsilon_k, \delta_k)}$$

$$mcd(a, b) = p_1^{min(\epsilon_1, \delta_1)} \cdots p_k^{min(\epsilon_k, \delta_k)}$$

Dunque

$$mcm(a, b)mcd(a, b) = p_1^{min(\epsilon_1, \delta_1) + max(\epsilon_1, \delta_1)} \cdots p_k^{min(\epsilon_k, \delta_k + max(\epsilon_k, \delta_k)}$$
$$p_1^{\delta_1 + \epsilon_1} \cdots p_k^{\delta_k + \epsilon_k} = ab$$

Proposizione:
Dato $mcd(a, b) = d$ possiamo dire che la fattorizzazione in primi di d è

$$mcd(a, b) = p_1^{min(\epsilon_1, \delta_1)} \cdots p_k^{min(\epsilon_k, \delta_k)}$$

Dimostrazione:

Innanzitutto $d \mid a$ e $d \mid b$ per definizione. Infatti $\frac{a}{d} = p_1^{\epsilon_1 - min(\epsilon_1, \delta_1)} \cdots p_k^{\epsilon_k - min(\epsilon_k, \delta_k)}$ e $\frac{b}{d} = p_1^{\delta_1 - min(\epsilon_1, \delta_1)} \cdots p_k^{\delta_k - min(\epsilon_k, \delta_k)}$ risultano essere interi. A questo punto dobbiamo dimostrare che ogni divisore comune z divide d. Un divisore comune z ha una fattorizzazione in primi: $z = p_1^{\omega_1} \cdots p_k^{\omega_1}$ tale che per ogni $i = 1, ..., k$ si ha $\epsilon_i - \omega_i \geq 0$ e $\delta_i - \omega_i \geq 0$. Siccome per costruzione di z $min(\delta_i, \epsilon_i) \geq \omega$ abbiamo che $z \mid d$

Un discorso simile si può fare per $mcm(a, b) = m$ la cui fattorizzazione in primi è

$$mcm(a, b) = p_1^{max(\epsilon_1, \delta_1)} \cdots p_k^{max(\epsilon_k, \delta_k)}$$

Dimostrazione:
Innanzitutto $a \mid m$ e $b \mid m$ per definizione. Infatti $\frac{m}{a} = p_1^{max(\epsilon_1, \delta_1) - \epsilon_1} \cdots p_k^{max(\epsilon_k, \delta_k) - \epsilon_k}$ e $\frac{m}{b} = p_1^{max(\epsilon_1, \delta_1) - \delta 1} \cdots p_k^{max(\epsilon_k, \delta_k) - \delta k}$ sono interi. A questo punto dobbiamo mostrare che ogni multiplo comune z è multiplo di m. Un multiplo comune ha fattorizzazione in primi: $z = p_1^{\omega_1} \cdots p_k^{\omega_1}$ tale che per ogni $i = 1, ..., k$ si ha $\omega_i - \epsilon_i \geq 0$ e $\omega_i - \delta_i \geq 0$. Siccome per costruzione $\omega_i \geq max(\epsilon_i, \delta_i)$ abbiamo che $m \mid z$.

Esempio: (1.3)
Dalla lezione precedente

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

Allora dalla proposizione (1.2) ricaviamo

- $mcm(60, 256) = \frac{60 \cdot 256}{4} = 3840$
- $mcm(54, 36) = \frac{54 \cdot 36}{18} = 108$
- $mcm(133, 27) = 133 \cdot 27 = 3591$
- $mcm(56, 24) = \frac{56 \cdot 24}{3} = 168$

Le fattorizzazioni in primi sono:

$$24 = 3 \cdot 2^3 \quad 27 = 3^3 \quad 36 = 3^2 \cdot 2^2 \quad 60 = 2^2 \cdot 5 \cdot 3$$

$$56 = 7 \cdot 2^3 \quad 133 = 7 \cdot 19 \quad 54 = 3^3 \cdot 2 \quad 256 = 2^8$$

Allora dalla proposizione precedente ricaviamo

- $mcm(60, 256) = 2^8 \cdot 5 \cdot 3 = 3840 \quad mcd(60, 256) = 2^2 = 4$
- $mcm(54, 36) = 3^3 \cdot 2^2 = 108 \quad mcd(54, 36) = 3^2 \cdot 2 = 18$
- $mcm(133, 27) = 7 \cdot 19 \cdot 3^3 = 3591 \quad mcd(133, 27) = 1$
- $mcm(56, 24) = 2^3 \cdot 3 \cdot 7 = 168 \quad mcd(56.24) = 2^3 = 8$

Si nota inoltre che, grazie alla scorsa proposizione, possiamo definire il massimo comun divisore tra tre interi diversi da zero scrivendo

$$a = p_1^{\delta_1} \cdots p_m^{\delta_m}$$
$$b = p_1^{\epsilon_1} \cdots p_m^{\epsilon_m}$$
$$c = p_1^{\omega_1} \cdots p_m^{\omega_m}$$

con $P = \{p_1, ..., p_m\} = P_a \cup P_b \cup P_c$, e ponendo

$$mcd(a, b, c) = p_1^{min(\delta_1, \epsilon_1, \omega_1)} \cdots p_m^{min(\delta_m, \epsilon_m, \omega_m)}$$

perchè $min(a, b, c) = min(min(a, b), c)$.
Per qualsiasi insieme finito $s = \{s_1, ..., s_k\}$ di interi diversi da zero possiamo definire il massimo comune divisore e otteniamo la stessa formula.

$$mcd(s_1, ..., s_k) = mcd(mcd(s_1, ..., s_{k-1}) s_k)$$

Allo stesso modo si può definire

$$mcm(a,b,c) = p_1^{max(\delta_1,\epsilon_1,\omega_1)} \cdots p_m^{max(\delta_m,\epsilon_m,\omega_m)}$$

ricavando la formula

$$mcm(a,b,c) = mcm(mcm(a,b),c)$$

perchè $max(a,b,c) = max(max(a,b),c)$. In generale abbiamo

$$mcm(s_1,...,s_k) = mcm(mcm(s_1,...,s_{k-1})s_k)$$

2.7 Teorema dei numeri primi

Come abbiamo visto nella lezione 1. l'insieme contenente i numeri primi è infinito. Detto questo, una domanda naturale è 'quanto densamente sono distribuiti i numeri primi?'
Sia $pi : (1, \inf) \to N^*$ una 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

$$\lim_{x\mapsto\infty} \frac{\pi(x)}{(\frac{x}{log(x)})} = 1$$

Questo teorema non dice niente sul limite della differenza delle due funzioni all' aumentare di x verso l'infinito, bensì 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 verso $+\infty$.
Sia p_n l'ennessimo numero primo. Allora, il teorema dei numeri primi è equivalente all'affermazione che

$$p_n \sim nlog(n)$$

nel senso che l'errore relativo di approssimazione di avvicina a 0 al crescere di n.

Nota: (2.1) Questo viene fuori da una sottile applicazione del teorema della funzione inversa basato sull'osservazione che $\pi(p_n) = n$. Pertanto, dobbiamo solo capire se la funzione inversa di $\frac{x}{log(x)}$ cresce asitonticamente come $xlog(x)$
L'ipotesi di Riemann irrisolta è equivalente alla seguente affermazione:

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

dove

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

2.8 Divergenza della serie dei reciproci dei primi

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

Dimostrazione
Sia p_j il j-esimo numero primo. Se la somma convergesse, esisterebbe un numero più piccolo tale che

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

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

- Limite superiore per la cardinalità di S_l: Ogni elemento di S_l può essere scritto come prodotto di a^2 e b dove b è un intero privo di quadrati. Il numero possibile di scelte per b è quindi 2^k, poichè:
$$b = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$$
dove ogni $\epsilon \in \{0, 1\}$. Il numero di possibilità di a è delimitato da $\sqrt{l}$ Quindi
$$|S_l| < \sqrt{l} 2^k$$

- Limite inferiore per la cardinalità di S_l: Sia $S'_l = \{1, ..., l\} - S_l$. Ogni elemento di S'_l ha un fattore primo maggiore di p_k. Sia
$$S'_l(j) = \{s \in S'_l \text{ t.c. } p_j \mid s\}$$
E si nota che $S'_l(j)$ è l'insieme non vuoto non appena $p_j > l$. Allora
$$S'_l = \cup_{j>k} S'_l(j)$$
Inoltre la cardinalità di $S'_l(j)$ è al massimo $\frac{l}{p_j}$. Allora
$$|S'_l| < \sum_{j=k+1}^{\infty} |S'_l(j)| < \sum_{j=k+1}^{\infty} \frac{l}{p_j} < \frac{l}{2}$$
Ma se $|S'_l| = l - |S_l|$ allora
$$l - |S_l| < \frac{l}{2} \implies \frac{l}{2} < |S_l|$$
Combinando i due bound si ottiene
$$\frac{l}{2} < |S_l| < \sqrt{l} 2^k$$
che è falso non appena $l > 2^{2^k+2}$

2.9 Richiami di combinatoria

Ricordiamo il triangolo di pascal

$$\begin{array}{ccccccccc} &&&& 1 &&&& \\ &&& 1 && 1 &&& \\ && 1 && 2 && 1 && \\ & 1 && 3 && 3 && 1 & \\ 1 && 4 && 6 && 4 && 1 \end{array}$$

ecc.

le cui voci sono i coefficienti bionimiali
$$\text{binomial}(n, k) = \binom{n}{k} = \frac{n!}{k!(n-k)!} \quad n \geq k$$
Ricorda che $0! = 1$. In particolare, *binomial*$(n, 0) = 1$ per ogni intero n non negativo. Ogni voce interna del triangolo è la somma delle due voci della riga precedente.
Questo è ricavato dalla

Regola di Pascal:
Siano $n, K \in \mathbb{N}^*$. Allora
$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$
Dimostrazione:
$$\binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!}$$

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

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 perchè:

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

dunque $0 \in S$. Supponiamo che $P(n)$ ovvero $n \in S$. Allora

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

Reindicizziamo $j=k+1$. Ovviamente segue che dobbiamo cambiare la partenza $j=1$ e la fine $n+1$ della serie di modo che non cambi.

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

Si estrae l'elemento con $j=n+1$ della prima serie (x^{n+1})e l'elemento con $l=0$ della seconda serie (y^{n+1})

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

per la regola di pascal infine

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

Se $k=0$ l'elemento corrispondente è y^{n+1} e se $k=n+1$ l'elemento corrispondente è x^{n+1}. Perciò scriviamo

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

Ciò equivale a dire che $P(n+1)$ è vera, dunque $n+1 \in S$ e per il principio d'induzione $\mathbb{N}=S$

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

Dimostrazione: Dato $\binom{p}{k}=\frac{p!}{k!(p-k)!}$, assumiamo $\binom{p}{k}=X$ e scriviamo l'equazione nel seguente modo.

$$p!=Xk!(p-k)!$$

Siccome $p \mid p! \implies p \mid Xk!(p-k)!$. Per il lemma di Euclide p deve dividiere almeno uno tra i termini del prodotto $Xk!(p-k)!$. Siccome p non ha divisori all'infuori di se e p non comparirà mai nei prodotti di $k!$ e $(p-k)!$ in quanto entrmbi minori di p per ipotesi allora $p \mid X$.

2.10 Piccolo Teorema di Fermat

Enunciato:
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 $n^p - n$. Per prima cosa dimostriamo che se $P(n)$ è vero per $n > 0$ allora è vero per $n < 0$

- Caso $p = 2$: $f(n) = n^2 - n \implies f(-n) = n^2 + n = f(n) + 2n$ dunque se $2 \mid f(n) \implies 2 \mid f(-n)$
- caso $p > 2$: In questo caso p è sempre dispari per ovvie ragioni. Allora

$$f(n) = n^p - n \implies f(-n) = -n^p + n = -f(n)$$

Ne segue che basta dimostrare $P(n)$ per $n \geq 0$. L'affermazione $P(0)$ è vera. Supponiamo che $P(n)$ è vera. Allora

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

Estraiamo l'elemento n^p e l'elemento 1 dalla serie. Rispettivamente per $k = p$ e $k = 0$.

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

$$(n^p - n) + \sum_{k=1}^{p-1} \binom{p}{k} n^k$$

Per ipotesi $p|(n^p - n)$. p divide anche ogni termine $\binom{p}{k}$ dunque $p \mid (n+1)^p - (n+1)$ e quindi $P(n+1)$ è confermata.

2.10.1 Esercizi

Esercizio 1:
Dimostra che, come conseguenza della regola di pascal, $\binom{n}{k}$ è sempre un intero

Ragioniamo per induzione dove la proposizione $P(n)$ è vera se $\binom{n}{k} \in \mathbb{Z}$. $P(0$ è vera siccome $\binom{0}{0} = 0$. Supponiamo che $P(n)$ sia vera. Perciò $\binom{n}{k}$ è sempre intero.

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

$\binom{n+1}{k}$ risulta essere intero in quanto somma di numeri interi. Dunque $P(n+1)$ è vera.

Esercizio 2:
Dimostra che, un intero $n > 1$ è primo se e solo se n non è divisibile per nessun primo $1 < p \leq \sqrt{n}$

Dato n, non divisibile per nessun primo $1 < p \leq \sqrt{n}$. Assumiamo che n sia non primo. Allora dovrebbe avere almeno due fattori primi contando più volte stessi fattori. chiamando p, q questi fattori sono per ipotesi $p, q > \sqrt{n} \implies pq > \implies pq \neq n$. Ciò implica che n deve essere per forza primo.
Dato p primo $D(p) = \{-p, -1, 1, p\}$sono i divisori di p. Nessuno dei suoi divisori è maggiore di 1 e minore della sua radice quadrata dunque nessun numero compreso in quell'intervallo potrà dividere p che sia primo o non primo.

3 Polinomi

Sia $\mathbb{Q}[x]$ l'insieme dei polinomi nella variabile x con coefficiente razionali. Sia $P_n[x]$ il sottoinsieme di $\mathbb{Q}[x]$ che consiste di tutti gli elementi che posssone essere scritti come

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

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) Oer 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)
Siano $f, g \in \mathbb{Q}[x]$. Allora diciamo che $f \mid g$, se esiste un polinomio $h \in \mathbb{Q}[x]$tale che $fh = g$
Per definire il minimo comune multiplo $mcm(f, g)$ di una coppia di elementi non nulli $f, g \in \mathbb{Q}[x]$, sia

$$S = \{h \in \mathbb{Q}[x] - \{0\} \text{ t.c. } f \mid h, \quad g \mid h\} \qquad 1.3$$

Allora S non è vuoto perchè il prodotto tra i due polinomi appartiene a $Q[x] - \{0\}$, 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 h_0 un altro polinomio monico in $S \cap P_d[x]$. Allora, poiche h e h_0 sono polinomi monici di grado d, $h - h_0$ è zero o un polinomio di grado $< d$. Se $h - h_0 = 0 \implies h = h_0$. Supponiamo il contrario, cioè che $h - h_0 \neq 0$. Allora

$$f \mid h \quad f \mid h_0 \quad g \mid h \quad g \mid g_0 \implies f \mid (h - h_0), \quad g \mid (h_0 - h)$$

Quindi $h - h_0$ è un elemento di S di grado strettamente inferiore rispetto a h e h_0, il che è una contraddzione.

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

Teorema (1.5)
Siano $f, g \in \mathbb{Q}[x]$ 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 $r(x) = 0 \lor (r(x) \neq 0 \land deg(r) < deg(g))$

Dimostrazione:
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 $r(x) = 0 \lor (r(x) \neq 0 \land deg(r) < deg(g))$
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 $deg(r) < d$ perchè 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 $f_0 = f - gq_{n+1-d}$. Allora $deg(f) < n + 1$ perchè abbiamo eliminato il termine di ordine più alto di f. Per l'ipotesi di induzione, esistono polinomi q, r tale che $f_0 = qg + r$ dove $r(x) = 0 \lor (r(x) \neq 0 \land deg(r) < deg(g))$. Quindi

$$f_0 = f - gq_{n+1-d} = qg + r \implies f = (q_{n+1-d} + q)g + r$$

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

Lemma: (1.8)

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

$$T = \{af + bg \in \mathbb{Q}[x] - 0 \text{ t.c. } a, b \in \mathbb{Q}[x]\}$$

T contiene un unico polinomio monico di grado minimo.

Dimostrazione:
T non è vuoto in quanto $f, g \in T$. Dunque per il principio di buon ordinamento deve esistere h con grado minimo siccome si usa la funzione $deg(h) = d$ dove $deg : \mathbb{Q}[x] \to \mathbb{N}$. Per vedere che h è unico, supponiamo che h_0, sia un altro polinomio monico di grado d minimo in T. Siccome h e h_0 sono polinomi monici dello stesso minimo grado, $h - h_0 = 0$ oppure $h - h_0$ ha un grado strettamente inferiore. Se $h - h_0 = 0$ allora $h = h_0$ che conferma l'unicità. SUpponiamo che $h - h_0 \neq 0$. Per definizione

$$h = af + bg, \quad h_0 = a_0 f + b_0 g \implies h - h_0 = (a - a_0)f + (b - b_0)g \in T$$

che contraddice la minimalità dei gradi di h e h_0

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 $h \mid f$ e $h \mid g$.

Dimostrazione:
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 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 $h \mid f$.

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

Per la minimalità del grado di h, dobbiamo avere $r = 0$ che implica $h \mid f$. Ragionamento identico per quanto riguarda g. Segue che $h \mid f \wedge h \mid g$

Definizione: (1.9)
L'unico polinomio monico h di grado minimo in T si chiama massimo comun divisore $mcd(f, g)$ di f e g.

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

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

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

Esempio: (1.11)

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

Quindi

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

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

$$mcd(x^2 - 2x + 1, -x + 1 = mcd(0, -x + 1) = x - 1$$

Esempio: (1.12)

$$f = 6x^4 + 2x^3 + 5x^2 + 3x + 2 \quad g = 2x^2 + 1$$

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

Quindi

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

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

$$mcd(2x^2 + 1, 2x + 1) = mcd(2x + 1, 3/2) = 1$$

3.0.1 Esercizi

Esercizio 1
Mostra che se $f \in \mathbb{Q}[x] - 0$ e $f(0) = 0$ allora $x \mid f(x)$. Più in generale dimostra che se r è un numero razionale tale che $f(r) = 0$ allora $(x - r) \mid 0$

Assumiamo per assurdo che r sia una radice di $f \in \mathbb{Q}[x]$ perciò $f(r) = 0$ ma che $(x - r) \nmid r$. Perciò possiamo scrivere per il teorema di divisione con resto.

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

Dove r è uno scalare in quanto non può essere zero per ipotesi e deve avere grado strettamente minore di $x - r$. Ora valutando di nuovo il polinomio f su r troviamo $0 = r$ che è assurdo in quanto $r > 0$ per ipotesi.

Esercizio 2
Siano $f, g \in \mathbb{Q}[x]$ mostra che se $h \mid f$ e $h \mid g$ allora $h \mid mcd(f, g)$ e che se $f \mid h$ e $g \mid h$ allora $mcm(f, g) \mid h$.

Abbiamo già dimostrato che in analogia con i numeri interi possiamo scrivere l'identità di bezout per i polinomi. Dati $f, g \in \mathbb{Q}[x]$ si individua d il minimo di

$$T = \{af + bg \in \mathbb{Q}[x] - 0 \text{ t.c. } a, b \in \mathbb{Q}[x]\}$$

il massimo comun divisore in quanto come già dimostrato divide sia f che g e chiamando $\mu = mcd(f, g)$ abbiamo $deg(d) \leq deg(\mu)$.

$$d = af + bg \implies d = \mu an + \mu am \implies \mu \mid d \implies deg(\mu) \leq deg(d)$$

Dunque siccome è unico l'elemento di grado minimo appartenente a T allora $d = \mu = mcd(f, g)$ per il principio di buon ordinamento

$$d = af + bg = ahm + bhn \implies h \mid d$$

che conferma la tesi.

Per definizione il minimo comune multiplo è l'unico e minimo elemento dell'insieme

$$S = \{s \in \mathbb{Q}[x] - \{0\} \text{ t.c. } f \mid s, \quad g \mid s\}$$

poniamo per assurdo che un multiplo h che divide f e g non divida l'mcm

$$h = fm = gn \wedge h = sx + r \implies r = h - sx$$

Ciò è assurdo perchè risulterebbe che esiste un r con $deg(r) < deg(s)$ che divide f e g. Ricordiamo s essere il polinomio monico unico multiplo di f e g e di grado minimo per il principio di buon ordinamento.

Esercizio 3
Mostra che l'algoritmo euclideo per il calcolo di $mcd(f, g)$ termina al massimo in $min(deg(f), deg(r) + 1)$ passi.

Senza perdità di generalità si inizia il procedimento con $mcd(a, b)$ dove $deg(a) \leq deg(b)$. Nel peggiore dei casi avremo $deg(r) = deg(b) - 1$. A ogni iterazione il grado del resto diminuirà di uno, fino a che non avremo uno scalare a $min(deg(a), deg(b))$ passi. Se siamo partiti con i polinomi invertiti allora si aggiunge un passo che è quello per invertirli all'inizio.

Esercizio 4
Ricordiamo che la prova per contrapposizione è semplicemente la dichiarazione.

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

Si dimostri la seguente affermazione.

Controllando la tabella di verità si trova una tautologia, questo vuol dire che le due proposizioni sono equivalenti. Posso dunque dimostrare.$(P \implies Q)$ dimostrando $(\neg Q) \implies (\neg P)$

3.1 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-costanti $g, h \in \mathbb{Q}[x]$ 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 $deg(f) = deg(g) + deg(h) > 1$ contraddizione.

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

Esempio: (2.4)
Se $f \in \mathbb{Q}[x] - \{0\}$ ha una radice razionale r allora f è riducibile perchè $(x - r) \mid f$

Esempio: (2.5)
Sia $f \in \mathbb{Q}[x]$ un polinomio di grado 2. Allora f è irriducibile se e solo 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 Pradici razionali. Così il contropositivo di $P \implies Q$ è $(\neg Q) \implies (\neg P)$, i.e. se f ha una radice razionale allora f è riducubile. Il contropositivo di $Q \implies P$ è $(\neg P) \implies (\neg Q)$, cioè se f è riducibile e di grado 2 allora f ha una radice razionale. Perchè f ha grado 2, f riducibile implica che $f = gh$ dove g e h hanno grado 1, e quindi f ha un radice razionale.

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

Dimostrazione:
Sia $m = mcd(f, g)$. Allora $m \mid f$ e quindi $f = mq$ per qualche $q \in \mathbb{Q}[x]$. Per definizione poichè f è irriducibile, segue che o m o q ha grado zero, cioè o $m = 1$ o $m = uf$ per qualche $u \in \mathbb{Q} - \{0\}$. Nel primo caso abbiamo $mcd(f, g) = 1$. Nel secondo caso abbiamo $m = mcd(f, g) = uf \mid g \implies f \mid g$.

Lemma: (2.7)
Sia $f \in \mathbb{Q}[x]$ irriducibile. Se $f \mid gh$ allora $f \mid g$ o $f \mid h$

Dimostrazione:
In base al lemma precedente, se f non divide g allora $mcd(f, g) = 1$. Pertanto, esistono $a, b \in \mathbb{Q}[x]$ tali che $1 = af + bg$ e quindi $h = haf + bgh$. Per ipotesi $f \mid gh$ e $f \mid afh$ che implica $f \mid h$.

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

3.1.1 Teorema di Fattorizzazione unica

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

$$f(x) = p_1(x) \cdots p_r(x), \quad f(x) = q_1(x) \cdots q_s(x)$$

sono due fattorizzazioni in un prodotto di irriducibili allora:

- $r = s$
- Esiste una permutazione σ di $\{1, ..., r\}$ e una collezioni di costanti non nulla tali che

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

  Per $j = 1, ..., r$

Dimostrazione:
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 $deg(g), deg(h) < n + 1$. Per l'ipotesi di induzione si ha che g e h possono essere scritti como prodotto di polinomi irriducibili. Supponiamo ora di avere due fattorizzazioni di f. Allora, dal momento che $p_1 \mid f$ e $f = q_1 \cdots q_r$ segue che $p_1 \mid q_j$ per qualche j. Dal momento che p_1 e q_j sono irriducibili, ne consegue che $q_j = c_1 p_1$ per qualche $c \in \mathbb{Q} - \{0\}$.Senza perdità di generalità (riordinando i fattori), possiamo assumere $j = 1$. Per completare la dimostrazione, ora induciamo sul numero totale di fattori $r + s$. Sia $P(n)$ l'affermazione che se un polinomio non costante f ha una coppia di fattorizzazione irriducibili tali che $r + s \leq n$ allora $r = s$ e la fattorizzazione è unica fino al riordinamento dei fattori e alla loro moltiplicazione per elementi non nulli di $\mathbb{Q}$. L'affermazione $P(1)$ è vera perchè non esistono polinomi di questo tipo, dato che ogni fattorizzazione contiene almeno un fattore. L'affermazione $P(2)$ è vera perchè in questo caso $r = s = 1$ e la fattorizzazione è $f = p_1 = q_1$ dove $q_1 = c_1 p_1$. Supponiamo che $P(1), ..., P(n)$ 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 di fattori è $(r - 1) + (s - 1) = r + s - 2 = n + 1 - 2 = n - 1$.In particolare, Poiche $P(n - 1)$ è vero ne consegue

- $r - 1 = s - 1$
- la fattorizzazione di g in fattori irriducibili è unica fino a riordinamento e moltiplicazioni per elementi non nulli appartenenti a $\mathbb{Q}$

Pertanto $r = s$ e la fattorizzazione di f è unica fino a riordino e moltiplicazione per elementi non nulli appartenenti a $\mathbb{Q}$.

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

Corollario: (2.10)

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

$$fg = mcm(f,g)mcd(f,g)$$

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

$$f = p_1^{\epsilon_1} \cdots p_n^{\epsilon_n}, \quad g = p_1^{\delta_1} \cdots p_n^{\delta_n}$$

dove si assume la possibilità che $\epsilon_i, \sigma_i = 0$ in quanto non è detto siano tutti fattori comuni.

$$mcm(f,g) = p_1^{max(\epsilon_1,\delta_1)} \cdots p_n^{max(\epsilon_n,\delta_n)}$$

$$mcd(f,g) = p_1^{min(\epsilon_1,\delta_1)} \cdots p_n^{min(\epsilon_n,\delta_n)}$$

Quindi

$$mcm(f,g)mcd(f,g) = p_1^{max(\epsilon_1,\delta_1)+min(\epsilon_1,\delta_1)} \cdots p_n^{max(\epsilon_n,\delta_n)+min(\epsilon_n,\delta_n)}$$

$$p_1^{\epsilon_1+\delta_1} \cdots p_n^{\epsilon_n+\delta_n} = fg$$

Esempio: (2.11)

$$f = x^2 - 3x + 2, \; g = x^2 - 2x + 1 \implies mcd(f,g) = (x+1)$$

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

3.1.2 Esercizi

Esercizio 5:
Dimostrare che se $f \in \mathbb{Q}[x]$ è irriducibile e $f \mid g_1 g_2 \cdots g_r$ allora $f \mid g_j$ per qualche g_j.

Supponiamo che f non divida $r-1$ fattori tranne g_j. Avendo ricavato

$$mcd(mcd(a_1, ..., a_{n-1}), a_n) = mcd(a_1, ..., a_n)$$

Scriviamo l'identità di bezout per $n-1$ fattori in quanto $mcd(f, g_i \neq g_j) = 1$. Senza perdità di generalità poniamo $g_j = g_r$.

$$fa_0 + g_1 a_1 + .. + g_{r-1} a_{r-1} = 1 \implies f\alpha + \beta g_1 \cdots g_{r-1} = 1$$

Questo passaggio si giustifica dicendo che siccome f è irriducubile possiamo dire che un prodotto di polinomi non potrà mai dividere f se tra quel prodotto non abbiamo f. Il massimo comun divisore resta dunque invariato.

$$a_r f\alpha + a_r \beta g_1 \cdots g_{r-1} = a_r$$

Per ipotesi $f \mid g_1 g_2 \cdots g_r$ dunque $f \mid a_r$.

Esercizio 6:
Sia $f \in \mathbb{Q}[x]$ di grado 3. Mostrare che f è irriducibile se e solo se f non ha radici razionali.

Se f non ha radici razionali $x - r$ con $r \in \mathbb{Q}$ non è mai fattore di f. Ma in questo modo eliminiamo tutti i fattori q con $deg(q) = 1$. Un polinomio f di grado 3 riducubile può essere sempre scritto come prodotto tra un polinomo di grado2 e uno di grado 1 ciò ci assicura che il polinomio f sia irriducibile.
Allo stesso modo poniamo per assurdo che f sia riducibile e non ha radici razionali. Senza perdità di generalità abbiamo $f = gh = (x-r)h = (x-r)g$. che mostra la radice razionale r perciò f deve essere irriducibile.

Esercizio 7
Costruire un polinomio riducibile $f \in \mathbb{Q}[x]$ di grado 4 senza radici razionali

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

Esercizio 8
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

Data la fattorizzazione $f = q_0 \cdots q_r$ al più del riordinamento dei fattori e moltiplicazione per scalare.

$$q_i = c_i x^{max} + \cdots + q_{i,0}$$

Per soddisfare il fatto che f sia monico dobbiamo avere $\prod_i c_i = 1$. Moltiplicando ciascun q_i per c_i^{-1} abbiamo una fattorizzazione di un polinomio monico f in fattori monici σ_i.

$$\sigma_0 \cdots \sigma_r = c_0^{-1} q_0 \cdots c_r^{-1} q_r = \prod_{i=0}^{r} c_i^{-1} (q_0 \cdots q_r)$$

$$\prod_{i=0}^{r} \frac{q_i}{c_i} = f$$

3.2 Teorema delle radici razionali

Enunciato:
Sia $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ l'insieme dei polinomi con coefficienti interi. Le radici razionali r di un polinomio non-costante $f \in \mathbb{Q}[x]$ tali che $f(0) = 0$ possono essere trovate come segue: Sia m il più piccolo intero positivo tale che $g = mf \in \mathbb{Z}[x]$. Allora r è un 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 $r = \frac{p}{q}$ dove $p \mid g_0$ e $q \mid g_n$ e $mcd(p, q) = 1$.

Dimostrazione:
Si supponga che p/q sia una radice di g con $mcd(p, q) = 1$. Allora

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

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

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

equivalente a

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

Per ipotesi $mcd(q, p) = 1$ segue che per il lemma di euclide $p \mid g_0$. D'altra parte, l'equazione può essere anche riscritta come

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

che allo stesso modo implica $q \mid g_n$.

Nota: (3.1) Se $f(0) = 0$ allora r è una radice $(x \mid f)$.Scrivi $f = x^n f$ con $h(0) \neq 0$ e applicare il metodo descritto nell'enunciato del teorema a $h(x)$

Esempio: (3.2)
Sia $r = p/q$ una radice razionale di $f = x^2 + 7x - 6$ con $mcd(p, q) = 1$. Allora $p \mid (-6)$ e $q \mid 1$. Quindi le possibili radici razionali di f sono $\pm 1, \pm 2, \pm 3, \pm 3, \pm 6$.
Infine si calcola $x^3 - 7x - 6 = (x + 1)(x + 2)(x - 3)$.

Proposizione (3.3)
Sia $f \in \mathbb{Z}[x]$ un polinomio non costante monico. Allora ogni radice razionale di f è un numero intero.

Dimostrazione: Scriviamo $f = x^n + f^{n-1}x^{n-1} + f_0$. Sia $r = p/q$ una radice razionale con $mcd(p, q) = 1$. Allora $p \mid f_0$ e $q \mid 1 \implies q = 1$. Quindi $r \in \mathbb{Z}$

Sia r una radice intera di un polinomio monico non costante $f \in mathbbZ[x]$ 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 ricerca delle radici intere.

Esempio: (3.4)
Sia $f = x^5 + 7x^2 - 60$. Sia r una radice intera di f. Allora r è contenuta nell' insieme.

$$R_0 = \{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm10, \pm12, \pm15, \pm20, \pm30, \pm60\}$$

Per essere sistematici, consideriamo le possibili radici in ordine crescente di valore assoluto. $f(1) = -52$: Quindi $(r - 1) \mid 52 = g_0$, e di conseguenza:

$$[(r - 1) \in \{\pm1, \pm2, \pm4, \pm13, \pm26, \pm52\}] \wedge [r \in R_0] \implies r \in R_1 = \{2, 3, 5, -12, -3, -1\}$$

$f(-1) = -54$: Quindi $(r + 1) \mid 54 = g_0$, e di conseguenza:

$$[(r + 1) \in \{\pm1, \pm2, \pm3, \pm6, \pm9, \pm18, \pm27, \pm54\}] \wedge [r \in R_1] \implies r \in R_2 = \{2, 5, -3\}$$

Si calcola che $f(2) = 0$, $f(-3) = -240$ e $f(5) = 3240$. Così,2 è la sola radice razionale di f.

3.2.1 Esercizi

Esercizio 9:
Sia

$$f = \frac{a_n}{b_n}x^n + \cdots + \frac{a_0}{b_0}$$

dove i coefficienti $\frac{a_i}{b_i} \in \mathbb{Q}$ sono frazioni a minimi termini, cioè tali che $a_i, b_i \in \mathbb{Z}$ e $mcd(a_i, b_i) = 1$. Trova il minimo intero tale che $mf \in \mathbb{Z}[x]$ in funzione di a_i, b_i.

Dati $c_i = \frac{ma_i}{b_i}$. Affinche i nuovi coefficienti appartengano a $\mathbb{Z}$ dobbiamo scrivere la nuova condizione $ma_i \mid b_i$. Ovviamente $m = mcm(b_1, ..., b_n)$ è una soluzione sempre ammissibile.

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

Possiamo innanzitutto trovare la radici razionali e trovare i polinomi $(x - r)$ irriducibili (in quanto di grado 1).

$$R_24 = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm24\}$$

$$f(1) = -28 = g'_0 \implies (r - 1) \in \{\pm1, \pm2, \pm4, \pm7, \pm14, \pm28\} \implies r \in \{2, 3, 8, -1, -3, -6\}$$

$$f(-1) = -36 = g''_0 \implies (r + 1) \in \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm9, \pm12, \pm18, \pm36\} \implies r \in \{2, 3, 8, -3\}$$

Calcoliamo $\{f(2) = -42, f(3) = -60, f(8) = 0, f(-3) = -132\}$. Dunque $x - 8$ divide $x^3 - 8x^2 + 3x - 24$. Possiamo dunque scrivere $q(x-8) = x^3-8x^2+3x-24$ dove q risulta essere x^2+3 con radici appartenti a $\mathbb{C}$ e dunque irriducibile.

4 Teoria dei Reticoli

4.1 Basi e Volumi

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

$$L = \{\lambda_1 b_1 + \cdots + \lambda_m b_m \text{ t.c. } \lambda_1, ..., \lambda_m \in \mathbb{Z}\}$$

Chiamiamo L un reticolo e B una base per L. Per semplicità, se non diversamente specificato, assumiamo $m = n$.
Nota: (2.1) A volte scriviamo $L(B)$ invece di L per chiarire il ruolo della base B.

Esempio: (2.2)
Sia $B = \{e_1, ..., e_n\}$ allora $L(B) = \mathbb{Z}^n$

Esempio: (2.3)
Sia $B = \{(1, 2), (1, 1)\}$. Allora anche in questo caso si ha $L(B) = \mathbb{Z}^2$

Esempio: (2.4)
Sia $n \geq 2$

$$L = \{(x_1, .., x_n\} \in \mathbb{Z}^n \text{ t.c. } 2 \mid (x_1 + \cdots + x_n\}$$

è un reticolo con base.

$$b_j = e_j - e_{j+1}, \quad j = 1, ..., n-1 \quad b_n = e_n + e_{n-1}$$

Ricordiamo che supponiamo il nostro sottoinsieme $B \subset \mathbb{R}^n$ di vettori linearmenti indipendenti abbia n elementi. Chiamiamo $L(B)$ il reticolo associato. Con un abuso di notazoine, possiamo chiamare B anche la matrice $n \times n$ di cui le colonne sono i vettori di B. Sia T un'altra matrice di rango massimo con valori interi. Allora il prodotto BT è la base di un nuovo reticolo $L(BT)$.
Per esempio il reticolo $\mathbb{Z}^n$ ha una base dati dai vettori elementari $\{e_1, .., e_n\}$, quindi la matrice corrispondente è la matrice identità $n \times n$, che denotiamo come Id_n. Quindi $Z^n = L(Id_n)$.
Se T una matrice, scriviamo $T(\mathbb{Z}^n)$ l'immagine di $\mathbb{Z}^n$ sotto T, cioè l'insieme di tutti gli elementi della forma $T(v)$, con $v \in \mathbb{Z}^n$ Se B è la base di un reticolo (e quindi anche una matrice di rango massimo), Allora $B(\mathbb{Z}^n)$ è il reticolo generato dalle colonne di B, quindi $L(B) = B(\mathbb{Z}^n) = B(L(Id_n))$

Esempio: (2.7)

$$B = (b1, b2), \quad T = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \implies BT = (b1 + 2b2, 3b2)$$

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

Teorema: (2.8) Sia T una matrice con solo valori interi. Allora T^{-1} esiste e ha solo valori interi se e solo se $det(T) = \pm 1$. In questo caso si dice che T è una matrice unimodulare.

Teorema: (2.9)
Sia T una matrice invertibile on valori interi e B una base di un reticolo $L = B(\mathbb{Z}^n)$. Allora $L(BT) \subseteq L(B)$

Dimostrazione:

$$L(BT) = BT(\mathbb{Z}^n) \subset B(\mathbb{Z}^n) = L(B)$$

Teorema: (2.10)
$L(B) = L(C)$ se e solo se esiste una matrice U unimodulare tale che $C = BU$

Dimostrazione:
Per il lemma, $C = BU \implies L(C) \subseteq L(C)$. Nello stesso modo, $C = BU$ e U unimodulare implica che $B = CU^{-1}$. Quindi $L(B) = L(CU^{-1}) \subseteq L(C) \implies L(B) = L(C)$.

Viceversa se $L(B) = L(C)$ allora $B = CT$ per qualche matrice T con valori interi. (ogni b deve essere una combinazione lineare intera di elementi di c. Allo stesso modo, abbiamo $C = BU$ per qualche altra matrice U a valori interi. Quindi $B = CT = BUT$ e, poichè B è invertibile, ne segue che $UT = Id$ e che T è unimodulare.

Data una base $B = (b1, ..., b_n)$ di L, il parallelepipedo fondamentale è

$$P(B) = \{x_1 b_1 + \cdots x_n b_n \text{ t.c. } x_1, ..., x_n \in \{0, 1\}$$

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

$$vol(P(C)) = |det(C)| = |det(BU)| = |det(B)det(U)| = |det(B)| = vol(P(B))$$

Definizione: (2.11)
$vol(L) = |det(B)|$ dove B è una qualsiasi base di L.

In particolare, due basi che danno i parallelpipedi fondamentali con volumi diversi descrivono reticoli diversi.

Esempio: (2.12)
$B = \{(1, -1), (1, 1)\}$ e $C = \{(2, 3), (1, 2)\}$ definiscono reticoli diversi. Hanno infatti volume diverso.

Esempio: (2.13)
$B = \{(1, -1), (1, 1)\}$ 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. Osservando che $|det(A)| = |det(C)|$ concludiamo che

$$det(A) \neq det(C) \implies L(B) \neq L(C)$$

Non è detto il contrario.

4.1.1 Esercizi

Esercizio 1
Verificare che $L(Id_n)) = \mathbb{Z}^n \neq L = \{(x_1, .., x_n\} \in \mathbb{Z}^n$ t.c. $2 \mid (x_1 + \cdots + x_n\}$

$$B = Id_n \implies |det(B)| = 1 \quad C = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ -1 & 1 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 1 \end{pmatrix} \implies |det(C)|1 =$$

I determinanti sono uguali, però si trova che il reticolo generato dalla Base C ha una proprietà che il reticolo Z_n non ha (la somma delle componenti dei vettore del reticolo è pari). Dunque $L(C) \subset L(B) = B(\mathbb{Z}_n) \neq L(C)$.

Dimostrazione:
Dato $c_i \in L(B)$ dove $B = \{b1, ..., b_n\} = |b_i|_1 = 2n$.

$$c_i = \lambda_1 b_1 + \cdots + \lambda_n b_n = \begin{pmatrix} \lambda_1 b_{1,1} + \cdots + \lambda_n b_{n,1} \\ . \\ . \\ . \\ \lambda_1 b_{1,n} + \cdots + \lambda_n b_{n,n} \end{pmatrix}$$

$$|c_i|_1 = \sum_{i=1}^{n} \lambda_i |b_i|_1$$

Siccome $|c_i|_1$ è somma di numeri pari anche esso è pari.

Esercizio 2
Verificare il teorema (2.8).

Prendiamo $T \in \mathbb{Z}^{n\times n}$ e $T^{-1} \in \mathbb{Z}^{n\times n}$ tale che $TT^{-1} = Id$.
Per il teorema di binet Cauchy possiamo scrivere dunque

$$det(TT^{-1}) = det(Id) \implies det(T)det(T^{1}) = 1$$

Dunque ricaviamo $det(T^{-1}) = \frac{1}{det(T)}$ che si conferma esistere ad apprtenere ai numeri interi (in quanto T^{-1} si è supposto avere solo elementi interi) se e solo se $det(T) = \pm 1$.

Esercizio 3
Verificare che le due matrici

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 3 & 2 \\ 3 & 2 & -1 \\ 2 & 1 & -1 \end{pmatrix}$$

Descrivono lo stesso reticolo in $\mathbb{R}^3$.

Osserviamo che deve esistere $AU = B$ affinchè abbiano lo stesso reticolo. Dobbiamo controllare che questa matrice U sia unimodulare $|det(A)| = |det(B)|$. Una volta controllato ciò dovremmo poter costruire una matrice che sia unimuodulare per cui valga $AC = B$.

$$det(A) = +3 = |det(A)| = 3 \text{ e } det(B) = +3 \implies |det(B)| = 3$$

i due determinanti sono uguali dunque non si esclude a priori che le due matrici generino reticoli diversi. Ora proviamo a costruire $U = A^{-1}B$.

$$A^{-1} = \frac{1}{3}cof(A)^T \text{ dove } cof(A) = \begin{pmatrix} 1 & 1 & -1 \\ -2 & 1 & 2 \\ 4 & -2 & -1 \end{pmatrix} \implies A^{-1} = \frac{1}{3}\begin{pmatrix} 1 & -2 & 4 \\ 1 & 1 & -2 \\ -1 & 2 & -1 \end{pmatrix}$$

$$A^{-1}B = \frac{1}{3}\begin{pmatrix} 6 & 3 & 0 \\ 3 & 3 & 3 \\ 0 & 0 & -3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$$

Il det è -1 e ha valori interi. Dunque A e B descrivono lo stesso reticolo.

Esercizio 4
Trova una base B in $\mathbb{Z}^2$ in cui la matrice corrispondente ha solo valori > 10 in valore assoluto.

Per il teorema (2.10) possiamo dire:

$$IdU = B \implies B = U \implies det(B) = \pm 1 \land B \in \mathbb{Z}^{2\times 2}$$

che implica.

$$b_{11}b_{22} - b_{12}b_{21} = \pm 1$$

Dunque basta che B sia unimodulare per far si che $B(\mathbb{Z}^n) = \mathbb{Z}^n$.
Un esempio può essere

$$B = \begin{pmatrix} 13 & 14 \\ 12 & 13 \end{pmatrix}$$

Esercizio 5
Siano $L = L(B)$ e $L' = L'(B')$ due reticoli con base B e B'. Supponi che $L \subseteq L'$. Dimostra che esiste una matrice di rango massimo T tale che $L = T(L')$. Deduci che $vol(L) \geq vol(L')$ e che l'uguaglianza vale se e solo se $L = L'$.

$L \subseteq L'$ allora possiamo dire che $B(\mathbb{Z}^n) \subseteq B'(\mathbb{Z}^n)$ e

$$\{v = (\lambda_1' b_{11}') + \cdots + \lambda_n' b_{1n}')t_1 + \cdots + (\lambda_1' b_{n1}') + \cdots + \lambda_n' b_{nn}')t_n) \text{ t.c. } \lambda' \in \mathbb{Z} \text{ e } v \in L(B)\}$$

Siccome il vettore dei coefficienti della combinazione lineare appartiene a un sottoinsieme di $\mathbb{Z}^n$ (in quanto non è detto che $B'(\mathbb{Z}^n) = \mathbb{Z}^n$). Ma $L = B(\mathbb{Z}^n)$ quindi

$$\{v = \lambda b_1 + \cdots + \lambda b_n \text{ t.c. } \lambda \in \mathbb{Z} \text{ e } v \in L(B)\} \implies B = B'T$$

Con T di rango massimo di modo che sia possibile che coincidano $L(B)$ e $L(C)$.
Ora per l'equivalenza volume-determinante scriviamo

$$vol(L) = |det(B'T)| \geq |det(B')| = vol(L')$$

Espressione che vale sempre siccome abbiamo supposto che T essendo di rango massimo non è mai uguale a 0. L'unico caso in cui varrebbe con l'uguale è quello in cui T è unimodulare. In questo caso per il teorema (2.10) $L = L'$.

4.2 Richiami sulle Norme

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: (3.1)
Per un numero reale $p \geq 1$, la p-norma di $x \in \mathbb{R}^n$ è definita da

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

Definiamo anche:

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

Proposizione: (3.2)
Per ogni $p \geq 1$ la p-norma è una norma nel senso di algebra lineare:

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

Esempio: (3.3)
Se $p = 2$ la p-norma è la distanza euclidea standard. Spesso scriviamo $|x|$ invece di $|x|_2$. In questo caso, la norma deriva dal prodotto scalare standard $< x, y >$ su $\mathbb{R}^n$ definito come

$$(x, y) = x_1 y_1 + \cdots + x_n y_n$$

Infatti, $|x| = \sqrt{(x, x)}$.

Esempio: (3.4)
Per $p = 1$ abbiamo $|(x_1, .., x_n)| = |x_1| + \cdots + |x_n|$

Teorema: (3.5)
Le norme $| * |_p$ e $| * |_q$ sono equivalenti se esistono costanti C e D tali che

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

per ogni $x \in \mathbb{R}^n$. Dunque possiamo cambiare norma in base al problema a patto che siano equivalenti.

4.3 SVP

Definizione: (3.6)
Il problema del vettore più breve (SVP_p) nella norma p è il seguente :

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

Teorema: (3.7)
SVP_∞ è $NP-$difficile.

Nota: (3.8) Non possiamo usare la relazione di equivalenza tra $|*|_p$ e $|*|_\infty$ per concludere che anche SVP_p è NP-difficile.

Per continuare ricordiamo che un insieme $S \subset \mathbb{R}_\ltimes$ si dice convesso se, dati due punti p e $q \in S$, il segmento che collega p e q è anch'esso contenuto in S.

Teorema: (3.9) *Blichfeldt*
Sia $L \subset \mathbb{R}^n$ un reticolo e $S \subseteq \mathbb{R}^n$ un insieme convesso tale che $vol(S) > vol(L)$. Allora esistono due punti distinti $p_1, p_2 \in S$ tali che $p_1 - p_2 \in L$.

Teorema: (3.10) *Minkowski*
Se $L \subset \mathbb{R}^n$ è un reticolo e S è un insieme convesso, simmetrico rispetto all'origine e con volume maggiore di $2^n det(L)$. Allora S contiene un punto non nullo di L.

Dimostrazione:
Sia $S' = (1/2)S$. Allora $vol(S) = 2^{-n} vol(S)$ e quindi $vol(S) > det(L)$. Per il teorema di Blichfeldt, esistono due punti distinti $p_1, p_2 \in S'$ tali che $p_1 - p_2 \in L$. Visto che $S' = (1/2)S$, ne segue che $2p_1, 2p_2 \in S$, 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

$$p_1 - p_2 = 1/2(2p_1 - 2p_2)$$

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

Il volume $V_n(r)$ della palla

$$B_n(r) = \{x = (x_1, ..., x_n) \in \mathbb{R}^n \text{ t.c. } |x| \leq r\}$$

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

$$V_{2n}(r) = \frac{\pi^n}{n!} r^{2n}, \quad V_{2n+1}(r) = \frac{2(n!)(4\pi)^n}{(2n+1)!} r^{2n+1}$$

Per semplificare la formula successivva scriviamo $V_n(r) = \gamma_n r^n$.

Corollario: (3.11)
Dato un reticolo $L \subset \mathbb{R}^n$, sia $\lambda_1(L)$ la lunghezza del vettore non nullo più corto in L rispetto alla norma euclidea $|*|$. Allora

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

Dimostrazione:

$$r > 2\left(\frac{vol(L)}{\gamma_n}\right)^{\frac{1}{n}} \implies V_n(r) = \gamma_n r^n > \gamma_n 2^n \left(\frac{vol(L)}{\gamma_n}\right) = 2^n vol(L)$$

Per il teorma di Minkowski, ogni sfera raggio r centrata nell'origine conterrà un vettore reticolare non nullo, e quindi il vettore più breve di L diverso da zero.

Nota: (3.12) La sfera di raggio r contiene l'ipercubo $\left[-\frac{r}{\sqrt{n}}, \frac{r}{\sqrt{n}}\right]$, da cui segue $\lambda_1(n) \leq \sqrt{n}\, vol(L)^{\frac{1}{n}}$

4.3.1 Esercizi

Esercizio 1:
Trova un vettore x_v diverso da zero di lunghezza minima rispetto alla norma euclidea nel reticolo descritto nell'esercizio 1 dello scorso capitolo.

Dalla divisibilità per 2 della somma dei componenti dei vettori reticolari possiamo accorgerci che la somma $|x_1| + \cdots + |x_n|$ delle componenti del vettore x_v deve essere 0. Notiamo che $n-1$ vettori di base (soddsfano questa condizione) e hanno norma euclidea $\sqrt{2}$. Si nota inoltre che è impossibile che esista un vettore la cui somma è divisibile per 2 e norma euclidea $< \sqrt{2}$, in quanto un vettore con un unico 1 non appartiene al reticolo.

4.4 Algoritmo di Gauss

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

4.4.1 Descrizione Algoritmo

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

- Se $|v_2| < |v_1|$ scambia $|v_1|$ e $|v_2|$;
- Sia $m = \lfloor (v_1, v_2)/|v_1|^2 \rceil$.
- Se $m = 0$ il risultato è la base $\{v_1, v_2\}$
- Se $m \neq 0$, sia $v_2^* = v_2 - mv_1$
- 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. As ogni passo si riduce la lunghezza dei vettori di base. Infatti, se assumiamo $(v_1, v_2) \geq 1/2$ abbiamo

$$\begin{aligned} |v_2^*|^2 < |v_2|^2 &\iff |v_2|^2 + m^2|v_1|^2 - 2m(v_1, v_2) < |v_2|^2 \\ &\iff m^2|v_1|^2 < 2m(v_1, v_2) \\ &\iff m < 2\frac{(v_1, v_2)}{|v_1|^2} \\ &\iff \left(m - \frac{(v_1, v_2)}{|v_1|^2}\right) < \frac{(v_1, v_2)}{|v_1|^2} \end{aligned}$$

Che vale poichè $m \leq (v_1, v_2)/|v_1|^2 + 1/2$.

Lemma: (4.1)
Sia $\{v_1, v_2\}$ il risultato dell'algoritmo di Gauss. Allora v_1 è un vettore più breve di L.

Dimostrazione:
Poichè l'algoritmo è terminato, sappiamo che:

$$|v_1| \leq |v_2|, \quad \frac{|(v_1, v_2)|}{|v_1|^2} \leq \frac{1}{2}$$

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

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

$$\geq c_1^2|v_1|^2 - |c_1c_2||v_1|^2 + c_2^2|v_2|^2$$
$$\geq (c_1^2 - |c_1c_2| + c_2^2)|v_1|^2$$

Gli ultimi due passaggi sono giustificati rispettivamente dalla seconda ipotesi e dalla prima ipotesi. Inoltre la quantità

$$c_1^2 - |c_1c_2| + c_2^2$$

è un intero. Pertanto è sufficiente è dimostrare che

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

$$c_1c_1 + c_2c_2 > c_1c_2$$

Senza perdità di generalità assumiamo $c_2 = max(c_1, c_2) \implies c_2c_2 > c_1c_2$ che verifica e dimostra il lemma.

Esempio: (4.5)

- $u = (2,3), v = (5,8), m = 3$
- $u = (-1,-1), v = (2,3), m = 2$
- $u = (0,1)v = (-1,-1), m = -1$
- $u = (0,1)v = (-1,0)m = 0$

Esempio: (4.6)

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

4.4.2 Costruzione di un Crittosistema

Come possiamo utilizzare un reticolo per costruire un crittosistema?
Gli ingredienti essenziali sono:

- Una base di vettori brevi per il reticolo. Questa è la chiave segreta
- Una base di vettori lunghi che descriva lo stesso reticolo, questa è la chiave pubblica.

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

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

dove n è un intero. Allora M è unimodulare $\iff x, y \in \mathbb{Z} \wedge det(M) = 1$. Questa si chiama equazione di Pell

$$x^2 - ny^2 = 1$$

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

Esempio: (4.9)
Per $n = 313$, $(x_1, y_1) = (321881120829134849, 1819380158564160)$.

Esempio: (4.10)
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 $B = (5,-3), (-3,5)$. Molitplicando 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:

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

Una bella caratteristica dell'equazione di Pell è che ha un numero infinito di soluzioni. Esse possono essere trovate utilizzando la relazione di ricorrenza di Brahmaguta:

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

Per spiegare questa relazione occorre introdurre il seguente lemma:

Lemma: (4.12)
Se A e B sono matrici 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 ha valori interi e $det(A^T) = det(A) = \pm 1$.

In particolare, siano

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

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

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

dove $det(AB) = det(A)det(B) = 1$ e $det(AB) = r^2 - ns^2 = (x^2 - ny^2)(u^2 - nv^2) = 1$.
Perciò le soluzioni x, y e u, v sono soluzioni per AB.Allo stesso modo r, s sono soluzioni per A e B in quanto

$$\begin{aligned} (ux + nvy)^2 - n(vx + uy)^2 &= u^2x^2 + n^2v^2y^2 + 2uxnvy - nv^2x^2 - nu^2y^2 - 2nvxuy \\ &\iff u^2x^2 + n^2v^2y^2 + -nv^2x^2 - nu^2y^2 \\ &\iff u^2(x^2 - ny^2) - nv^2(x^2 - ny^2) = 1 \end{aligned}$$

Dunque se (x, y) soluzione di A e (u, v) soluzione di B allora $(r = ux + nvy, s = vx + uy)$ è ancora soluzione di A e B per costruzione.

Teorema: (4.13)
Ogni matrice intera 2×2 di determinante 1 può essere scritta come prodotto finito delle matrici

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

Nota: La moltiplicazione tra matrici non è commutativa. La rappresentazione di una matrice come prodotto di S e T non è unica.

4.4.3 Esercizi

Esercizio 1:
Utilizza l'algoritmo di Gauss per trovare il vettore più corto del reticolo

$$\begin{pmatrix} 10 & 13 \\ 13 & 14 \end{pmatrix}$$

- $u = (10, 13), v = (13, 14), m = 1$
- $u = (3, 1), v = (10, 13), m = 4$
- $u = (3, 1), v = (-2, 9), m = 0$

Dunque $u = (3, 1)$ è il vettore più corto del reticolo.

Esercizio 2:
Trova almeno 5 soluzioni dell'equazione di Pell.

$$x^2 - 2y^2 = 1$$

Si nota che una soluzione possibile è $(x, y) = (7, 5)$. Ora basta usare le regole di ricorrenza di brahmaguta.

- $(x^2 + ny^2, 2xy) = (99, 70) = (r, s)$
- $(rx + nsy, sx + ry) = (1393, 985) = (r', s')$
- $(r'x + ns'y, s'x + r'y) = (19601, 13860) = (r'', s'')$
- $(r''x + ns''y, s''x + r''y) = (275807, 195025) = (r''', s''')$

5 Relazioni di equivalenza

5.1 Relazioni

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

- Traslazioni
- Rotazioni
- Riflessioni

Esempio: (1.1)
Dati due triangoli T_1 e T_2 sono congruenti se c'è un isometria che muove T_1 su T_2.

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

Esempio: (1.3)
Due Triangoli T_1 e T_2 sono simili se T_1 diventa congruente a T_2 dopo aver riscalato le distanze.

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)
Sia $S = \mathbb{Z}$ poniamo aRb se e solo se $a \leq b$. Allora R è una relazione.

Esempio: (1.6)
Sia S in 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 inseme finito $S = \{s_1, ..., s_n\}$ può essere rappresentata dalla matrice booleana $n \times n$:

$$M = (m_{ij}), \quad m_{ij} = \begin{cases} 1 & (s_i, s_j) \in R \\ 0 & (s_i, s_j) \notin R \end{cases}$$

Equivalentemente, una relazione R può essere rappresentata da un grafo diretto il cui insieme di vertici e l'insieme S con un arco orientato 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 orientato.

Definizione: (1.7)
Una relazione R 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: $(A \subseteq B \implies B \subseteq A)$.
A seconda della definizione, un grafo può avere o meno un 'self-loop' da un vertice allo stesso vertice. Nelle corrispondenze 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)

In tutti gli esempi appena visti, la relazione è riflessiva.

Esempio: (1.11)
Il caso più semplice di una relazione che non è riflessiva è di prendere un insieme 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)
Sia $S = \{2, 3, ...\}$ e aRb se e solo se a e b sono coprimi. Questo esempio è simmetrica perchè $mcd(a, b) = mcd(b, a)$ ma non è riflessivo perchè $mcd(a, a) = a > 1$.

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: $mcd(2, 3) = 1$ e $mcd(3, 4) = 1$ ma $mcd(2, 4) = 2$.

5.2 Relazioni di Equivalenza

Definizione: (1.14)
Una relazione R su un insieme S è una relazione di equivalenza se e solo se è riflessiva, simmetrica e transitiva.

Esempio: (1.15)
Congruenza, parallelismo e similarità (esempi (1.1), (1.2), (1.6)) sono relazioni di equivalenza.
Nota: (1.16) Relazioni di equivalenza sono di solito scritte come $a \sim b$.

Nota: (1.17) Un'altra classe importante di relazione sono le relazioni di ordine. Diciamo che una relazione è una relazione di ordine se è riflessiva, transitiva e antisimmetrica. Antisimmetrica significa che aRb e bRa allora $a = b$.
Le relazioni $\leq$ e $\subseteq$ date negli esempi (1.5) e (1.6) sono di ordine.

Nota: (1.18) Sia M una matrice quadrata booleana generta casualmente. In generale, la relazione R associata non è:

- Riflessiva se esiste almeno una voce $m_{ii} \neq 1$.
- Simmetrica se M non è simmetrica
- Transitiva se $(M^2)_{ac} \neq 0 \not\Longrightarrow M_{ac} \neq 0$

Per il resto del corso avremo sempre a che fare con relazioni di equivalenza.

Esempio: (1.19)
Sia S l'insieme di tutte le matrici $m \times n$. Diciamo che due matrici A e B sono equivalenti per righe se possiamo ottenere B da A attraverso una successione delle seguenti mossa:

- Scambiare due righe
- Moltiplicare una riga per uno scalare non nullo
- Combinare linearmente le righe

Allora $A \sim B$ se e solo se A è equivalente per righe 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).

5.3 Spazi Quoziente e Classi di Equivalenza

Definizione: (1.21)
Sia $\sim$ una relazione di equivalenza su S e $a \in S$. Allora l'insieme

$$[a] = \{b \in S \text{ t.c. } a \sim b\}$$

è chiamato 'classe di equivalenza di a'. Un elemento $s \in S$ tale che $s \sim a$ si chiama '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:
Se $a \sim b$ abbiamo che $[b]$ contiene tutti i b' tali che $b' \sim b$ ma siccome $\sim$ è una relazione di equivalenza allora $b \sim a \implies b' \sim a \implies a \sim b' \implies [b] \subseteq [a]$. Viceversa $[a]$ contiene tutti i a' tali che $a' \sim a$ ma siccome $\sim$ è una relazione di equivalenza allora $a' \sim b \implies b \sim a' \implies [a] \subseteq [b]$. Dunque $[a] = [b]$.
Per $a \nsim b$ invece supponiamo che esista un elemento comune s. Se $s \in [a]$ allora $a \sim s$. Se $s \in [b]$ allora $s \sim b$. Ma siccome $\sim$ è una relazione di equivalenza si ha $a \sim b$ che è assurdo.

Definizione: (1.23)
Sia $\sim$ una relazione di equivalenza su S. Allora $S/\sim$ è l'insieme di tutte le classi di equivalenza di S. L'insieme $S/\sim$ è chiamato lo spazio quoziente si S rispetto a $\sim$.

Può essere difficile a volta capire lo spazio quoziente. Un metodo per riuscire a capirlo è di provare a costruire una mappa $f : S \to T$ tale che

- $f(S) = T$
- $f(a) = f(b) \iff a \sim b$

Data una tale mappa f, possiamo definire una mappa $g : (S/\sim) \to T$ con la regola

$$g([s]) = f(s)$$

Per vedere che la mappa è ben definita, supponiamo $s' \sim s$. Allora $f(s) = f(s')$. In altre parole, la funzione, la mappa g dipende solo dalla classe di equivalenza $[s]$ e non dal particolare rappresentante s. Poichè f è suriettiva, lo è anche g. Infine, g è iniettiva perchè $g[s] = g[s']$ significa $f(s) = f(s')$ e quindi $s \sim s'$, ovvero $[s] = [s']$. Quindi in particolare se f rispetta le condizione date, la mappa risultante g sarà una bigezione.

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 canocnica per righe. Ricordiamo che un matrice si dice in forma canonica per righe se

- Tutte le righe con soli zero sono in fondo alla matrice
- Per ogni riga, il pivot (cioè il valore non nullo più a sinistra della riga) è 1 e si trova più a destra del pivot delle righe sopra.
- Una colonna in cui c'è un pivot ha tutti gli altri elementi = 0

Allora l'algoritmo di eliminzazione di Gauss-Jordan da una mappa $f : S \to T$ che è suriettiva. Inoltre due matrici $A = B$ in 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 una bigezione.

Esempio: (1.26)
Sia P l'insieme di tutte le permutazioni di $\{1, ..., n\}$. Allora, la relazione $\sim$ su $S = \mathbb{C}^n$ definita da $(z_1, ..., z_n) \sim (\omega_1, ..., \omega_n)$se e solo se esiste una permutazione $\sigma \in P$ tale che $z_j = \omega_{\sigma(j)}$ per $j = 1, ..., n$

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
$$f : S \to T, \quad f(z_1, ..., z_n) = (\lambda - z_1)(\lambda - z_2) \cdots (\lambda - z_n)$$
è suriettiva perchè un polinomio monico di grado n si fattorizza in un prodotto di questa forma per il teorema fondamentale dell'algebra. Similmente, il valore di $f(z_1, ..., z_n)$ è chiaramente invariante sotto permutazioni di $(z_1, ..., z_n)$. Infine poichè la fattrizzazione di un polinomio monico è unica senza contare il riordinamento, segue che $f(z) = f(\omega) \iff z \sim \omega$.

Esempio: (1.27)
Sia S l'insieme dei triangoli nel piano e sia $\sim$ la relazione di equivalenza data dalla congruenza. Si fissa una semiretta L nel piano con origine p. Sia $\Delta \in S$ un triangolo con lunghezze dei lati $\lambda_1 \leq \lambda_2 \leq \lambda_3$. Con un movimento rigido si può porre il lato più corto di Δ su L di modo che p coincida con uno dei vertici. Siano θ_1 e θ_2 gli angoli di Δ corrispondenti ai vertici di Δ su L. Poichè la riflessione rispetto a una linea perpendicolare a L è una congruenza, possiamo assumere che $\theta_1 \leq \theta_2$ senza perdere di generalità. Inoltre poichè il lato su L è il più corto θ_3 deve essere il più corto. Poichè la somme degli angoli è $\theta_1 + \theta_2 + \theta_3 = \pi$ dobbiamo avere $\pi - \theta_1 + \theta_2 \leq \theta_1$ ovvero $2\theta_1 + \theta_2 \geq \pi$.
Sia $T = \{(\theta_1, \theta_2, \lambda) \in [0, \pi] \times [0, \pi] \times [0, \infty] \text{ t.c. } \theta_1 \leq \theta_2, \quad \theta_1 + \theta_2 < \pi, \quad 2\theta_1 + \theta_2 \geq \pi\}$. 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 poichè $\theta_1 + \theta_2 < \pi$, dato un punto in T possiamo costruire un triangolo con queste proprietà. Scegliamo un semipiano H su un lato di L, e disegnamo 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. Quindi f induce una bigezione $S/\sim \cong T$.

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 $l \in S$ è equivalente a un'unica linea L che passa per l'origine $(0, 0)$. Sia C il cerchio unitario dato dall'equazione $y^2 + x^2 = 1$. Allora una linea L che passa per l'origine interseca C in due punti antipodali (x, y) e $(-x, -y)$. Sia C' il sottoinsieme costituito da i punti di C per cui $y \geq 0$. Allora a meno che L sia l'asse x, $L \cap C'$ è un singolo punto (x, y) con $y \geq 0$. 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 $f(l) = f(l')$ se e solo se l è parallela a l', ovvero $l \sim l'$.

Esempio: (1.29)
Consideriamo l'insieme degli interi $\mathbb{Z}$ e la relazione xRy se $4|(x - y)$. Questa è una relazione di equivalenza, e ci sono 4 classi di equivalenza:
$$\{..., -8, -4, 0, 4, 8, ...\}, \{..., -7, -3, 1, 5, 9, ...\}, \{..., -6, -2, 2, 6, ...\}, \{..., -9, -5, -1, 3, 7, 11, ...\}$$
Prendiamo $T = \{0, 1, 2, 3\}$. Allora la funzione che associa ad ogni numero il resto della divisione per 4 induce una bigezione: $S/\sim \to T$.
Un modo alternativo di descrivere relazioni di equivalenza è il seguente:

5.4 Partizioni

Definizione: (1.30)
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 $s \in A$
- $A.B \in \mathcal{P} \implies A = B \vee A \cap B = \emptyset$

In altre parole, un partizione di S è una decomposizione di S in una collezione di sottoinsiemi mutualmente disgiunti.

Esempio: (1.31)

Sia $\mathcal{P}$ una partizione dell'insieme S. Allora

$$a \sim b \iff \exists P \in \mathcal{P} \text{ t.c. } a, b \in P$$

è una relazione di equivalenza.

Dimostrazione:

- Riflessività: Per ogni $a \in S$ esiste sempre un insieme $P \in \mathcal{P}$ tale che $a \in P$. Dunque $a \sim a$
- Simmetria: se $a \sim b$ allora $\exists P \in \mathcal{P}$ t.c. $a, b \in P \implies b, a \in P \implies b \sim a$.
- Transitività: $a \sim b$ allora $\exists P \in \mathcal{P}$ t.c. $a, b \in P$. $b \sim c$ allora $\exists P' \in \mathcal{P}$ t.c. $b, c \in P'$. Ma siccome $P \cap P' = \{b\}$ allora $P = P' = \{a, b, c\} \implies a \sim c$.

Esempio: (1.32)
Sia $\sim$ una relazione di equivalenza su S. Allora

$$\mathcal{P} = \{|a| \text{ t.c. } a \in S\}$$

è una partizione di S.

Dimostrazione:
Si nota che in quanto $\sim$ è una relazione di equivalenza allora per ogni $a \in S$ allora $a \sim a$ dunque $a \in [a]$. Abbiamo già dimostrato la seconda proprietà fondamentale delle partizioni (1.22). Dunque la collezione di tutte le classi di equivalenza è un partizione $\mathcal{P}$.

Teorema: (1.35)
Si fissi un insieme S. Sia Π l'insieme di tutte le possibili partizioni di S e si denoti con ε l'insieme di tutte le possibili relazioni di equivalenza su S. Si denoti con $f : \Pi \to \varepsilon$ la mappa definita dall'esempio (1.31). Si denoti con $g : \varepsilon \to \Pi$ la mappa definita dall'esempio (1.32). Allora $f \circ g$ e $g \circ f$ sono le mappe identità su ε e Π rispettivamente. In altre parole, f e g sono bigezioni inverse.

Dimostrazione:

- $f \circ g = Id_\varepsilon$: Sia $\mathcal{P} = g(\sim)$ e $R = f(\mathcal{P})$. Dobbiamo dimostrare che $aRb \iff a \sim b$.
  Supponiamo che $a \sim b$. Allora per l'esempio (1.32) esiste $P \in \mathcal{P}$ tale che $a, b \in P$. Allora, per l'esempio (1.31), aRb. In altre parole $a \sim b \implies aRb$.
  Viceversa, sipponiamo che aRb. Allora per l'esempio (1.31) esiste $P \in \mathcal{P}$ tale che $a, b \in P$. Allora per l'esempio (1.32), $a \sim b$.
- $g \circ f = Id_\mathcal{P}$: Sia $R = f(\mathcal{P})$ e $\mathcal{P}' = g(R)$. Allora poichè $\mathcal{P}$ 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 $A = B$.
  Supponiamo che $s' \in A$. Allora per l'esempio (1.31), sRs'. Si ricava che per l'esempio (1.32) $s' \in B$. Dunque $A \subseteq B$.
  Supponiamo che $s' \in B$. Allora per l'esempio (1.32) , $s'Rs$ e quindi, per l'esempio (1.32), $s' \in A$. Dunque $B \subseteq A$.

Esempio: (1.36)
Sia L una retta in $\mathbb{R}^2$. Dati due punti $p, q \in \mathbb{R}^2$, diciamo che $p \sim_L q$ in $\mathbb{R}^2$ se la retta parallela a L passante per p passa anche per q. La relazione $\sim_L$ è una relazione di equivalenza.
Sia T una retta in $\mathbb{R}^2$ non parallela ad L. Allora la funzione che manda p nell'intersezione tra T e la retta parallela ad L passante per p definisce una bigezione: $T \cong \mathbb{R}^2/\sim_L$.

5.5 Esercizi

Esercizio 1:
Sia $f : X \to Y$ una funzione. Dimostrare che $a \sim b \iff f(a) = f(b)$ è una relazione di equivalenza.

- riflessività: $\forall a \in X f(a) = f(a) \implies a \sim a$ In quanto una funzione è ben definita per definizione

- simmetria: $a \sim b \implies f(a) = f(b) \implies f(b) = f(a) \implies b \sim a$
- Transitività: $a \sim b \implies f(a) = f(b)$ e $b \sim c \implies f(b) = f(c)$ Siccome = è una relazione di equivalenza allora $f(a) = f(c) \implies a \sim c$

Esercizio 2:
Sia $S = \{x_1, ..., x_n\}$. Considera le seguenti tre relaizoni sull'insieme dei sottoinsieme $\mathcal{P}(S)$ e determina se sono relazioni di equivalenza.

- $(A, B) \in R$ se A contiene un numero di elementi minore o uguale a B.
  $\forall A \in \mathcal{P}(S)$ si ha $\#A \leq \#A \implies (A, A) \in R \implies$ Riflessiva.
  $(A, B) \in R \implies \#A \leq \#B \implies \#B \geq \#A \not\Longrightarrow (B, A) \in R \implies$ Non simmetrica.
  $(A, B) \in R \implies \#A \leq \#B$ e $(B, C) \in R \implies \#B \leq \#C$ quindi $(A, C) \in R \implies$ Transitiva.
  Dunque non è una relazione di equivalenza.
- $(A, B) \in R$ se A e B hanno lo stesso numero di elementi.
  $\forall A \in \mathcal{P}(S)$ si ha $\#A = \#A \implies (A, A) \in R \implies$ Riflessiva.
  $(A, B) \in R \implies \#A = \#B \implies \#B = \#A \implies (B, A) \in R \implies$ Simmetrica.
  $(A, B) \in R \implies \#A = \#B$ e $(B, C) \in R \implies \#B = \#C$ quindi $(A, C) \in R \implies$ Transitiva.
  Dunque è una relazione di equivalenza
- $(A, B) \in R$ se l'intersezione $A \cap B = \emptyset$.
  $\forall A \mathcal{P}(S)$ si ha $A \cap A = A \implies$ non Riflessiva.
  $(A, B) \in R \implies A \cap B = \emptyset \implies B \cap A = \emptyset \implies (B, A) \in R \implies$ Simmetrica.
  $(A, B) \in R \implies A \cap B = \emptyset$ e $(B, C) \in R \implies B \cap C = \emptyset$ non è detto però che $A \cap C = \emptyset$, perciò non è transitiva.
  Dunque non è una relazione di equivalenza

Esercizio 3:
Sia $X = \{a, b, c\}$ un insieme con 3 elementi. Considera la relazioni di equivalenza su R su $\mathcal{P}(X)$ definita da $(A, B) \in R$ se solo se hanno lo stesso numero di elementi. Determina le classi di equivalenza di R.

$$[\#0] = \{\emptyset\}, \quad [\#1] = \{\{a\}, \{b\}, \{c\}\},$$

$$[\#2] = \{\{a, b\}, \{b, c\}, \{a, c\}\}, \quad [\#3] = \{X\}$$

Esercizio 4:
Verifica che la relazione R, definita $(a, b)R(c, d)$ se solo se $ad = bc$ definisce una relazione di equivalenza sulle coppie di numeri interi non nulli. Cosa c'entra questa relazione con le frazioni?

- riflessività: $\forall (a, b) \in \mathbb{Z}^2 ab = ba \implies (a, b)R(a, b)$ In quanto il prodotto è commutativo su $\mathbb{Z}$.
- simmetria: $(a, b)R(c, d) \implies ad = bc \implies bc = ad \implies cb = da \implies (c, d)R(a, b)$
- Transitività: $(a, b)R(c, d) \implies ad = bc$ e $(c, d)R(e, f) \implies cf = de \implies \frac{adf}{b} = de \implies af = be$
  Dunque $(a, b)R(e, f)$ ma a patto che $d \neq 0$ e $b \neq 0$. Vale anche $cf = \frac{bce}{a} \implies fa = be \implies af = be$ con $c \neq 0$ e $a \neq 0$. In conclusione $f \neq 0$ e $e \neq 0$.

Se trattassimo le frazioni come vettori $\mathbb{Z}^2$ senza contare l'ordine di numeratore e denominatore allora vale la seguente relazione di equivalenza. Ovviamente con un denominatore a zero viene meno la transitività.

Esercizio 5:
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 solo se $A = MBM^{-1}$ per qualche matrice ortogonale M definisce una relazione di equivalenza su S. Dare una descrizione di $S/\sim$.

- riflessività: $\forall A \in S$ si ha $A = IdAId^{-1} \implies A \sim A$
- simmetria: $A \sim B \implies A = MBM^T \implies B = M^TAM \implies B = M_1AM_1^{-1} \implies B \sim A$ siccome M^T è sempre ortogonale. Infatti dato M ortogonale allora $MM^T = M^TM = Id$. Dato M^T abbiamo $M^TM = Id$.

- Transitività: $A \sim B \implies A = MBM^T$ e $B \sim C \implies B = M_1CM_1^T$ dunque $A = MM_1CM_1^TM^T \implies A \sim C$ siccome prodotto di matrici ortogonali è ortogonale. Infatti dato M e M_1 ortogonali vale $MM^T = M^TM = Id$ e $M_1M_1^T = M_1^TM_1 = Id$. Dunque per (MM_1) abbiamo $MM_1(MM_1)^T = MM_1M_1^TM^T = MM^T = Id$.

Dato un certo endomorfismo di V descirtto da una matrice A simmetrica, l'algoritmo di Gran-schmidt riesce sempre a trovare una base ortonormale M. Per il teorema spettrale questo spazio vettoriale ha una base ortonormale composta dagli autovettori di A. Se A è simile a B allora le basi di autovettori di A e B sono le stesse perciò il processo di ortogonalizzazione di gran schmidt restituisce la stessa base M. La collezione di insiemi di matrici per i quali ho differenti basi ortonormali M_i è lo spazio quoziente $S/\sim$.

Esercizio 6:
Dare una descrizione geometrica dell'insieme delle classi di equivalenza di linee in $\mathbb{R}^3$ con la relazione di equivalenza data dalle traslazioni.

Ogni $L \subset \mathbb{R}^3$ è parallela a una sola linea passante per l'origine. A questo punto prendiamo in considerazione la sfera unitaria $C : x^2 + y^2 + z^2 = 1$ e prendiamone in considerazione i punti con $z \geq 0$. Esistono infinite rette $\in U$ con $U = \{(x, y, 0)$ t.c. $x, y \in \mathbb{R}\}$ la cui intersezione con C da luogo a più di un punto. Priviamo perciò C dei punti appartenenti a $U' = \{(x, y, 0)$ t.c. $x^2+y^2 = 1 \wedge y <= 0\} - \{(1, 0)\}$ e chiamiamo l'insieme risultante T. Per costruzione ogni linea passante per l'origine interseca T in un solo punto. Ogni classe di equivalenza sarà rappresentata da una sola linea L (in quanto disgiunte per definizione) passante per l'origine e per costruzione da un solo punto $p \in T$. Abbiamo perciò costruito una bigezione $g : S/\sim \to T$ in quanto $f : S \to T$ restituisce $f(l) = f(l')$ solo quando sono parallele $l' \sim l$.

Esercizio 7:
Quali di queste matrici Booleane rappresentano una relazione di equivalenza su un insieme di tre elementi? E quali definiscono una relazione d'ordine?

$$R_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad R_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad R_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

La prima relazione R_1 è riflessiva in quanto tutti gli $r_{ii} \neq 0$, è simmetrica in quanto $R^T = R$ ed è transitiva in quanto:

$$R^2 = \begin{pmatrix} 2 & 2 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Dunque R_1 è una relazione di equivalenza.
La seconda relazione R_2 non è riflessiva in quanto tutti esistono $r_{ii} \neq 1$. Siccome sia le relazioni di ordine che di equivalenza devono rispettare la riflessività segue che R_2 non nè di ordine nè di equivalenza.
La terza relazione R_3 è riflessiva in quanto tutti gli $r_{ii} \neq 1$, è antisimmetrica in quanto l'unica parte simmetrica è la diagonale ed è transitiva in quanto:

$$R^2 = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

Dunque R_3 è una relazione di ordine.

6 Spazi Vettoriali Quoziente

6.1 Costruzioni di 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 sempplicemente 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: $x \in V \implies x - x \in U \implies x \sim x$
- 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

  $$x - z = (x - y) + (y - z) \in U$$

  poichè $x \sim y \implies x - y \in U$ e $y \sim z \implies y - z \in U$. Allora $x \sim z$.

Esempio: (2.2)
Sia $V = \mathbb{R}^2$ e $U = \{(X, 2x) \text{ t.c. } x \in \mathbb{R}\}$. Allora le classi di equivalenza in V/U sono precisamente le rette parellele a U, cioè le rette con pendenza 2.

Lemma: (2.3)
Sia U un sottospazio di V. Allora V/U è uno spazio vettoriale rispetto alle operazioni:

- $c[u] = [cu]$
- $[u] + [u'] = [u + u']$

Dimostrazione:
Da fare

6.2 Isomorfismi e Spazi Vettoriali Quozienti

Proposizione: (2.4) Sia $f : V \to W$ una mappa lineare. Supponiamo che f sia suriettiva e che $U = ker(f) = \{x \in V \text{ t.c. } f(x) = 0\}$. Allora f induce un isomorfismo lineare $f_0 : V/U \cong W$.

Dimostrazione:

La prima cosa da dimostrare è che f_0 è ben definita. Osserviamo che se $v \sim v'$ allora $v - v' \in U$, quindi $f(v) = f(v' + v - v') = f(v') + 0$, quindi f non cambia sulle classi di equivalenza. Possiamo perciò definire $f_0(v) = f([v])$. Poichè f è suriettiva, lo è anche f_0. Inoltre f_0 è iniettiva. Infatti, se $f_0([v]) = 0$ allora $f(v) = 0$ e quindi $v \in U$. Se segue che $v \sim 0$, cioè $[v] = 0$. Rimane da dimostrare che f_0 è lineare. Questo segue dal lemma (2.3).

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 $u = u + w$ 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: (2.5)
Se $V = U \oplus W$ allora V/U è isomorfo a W attraverso la mappa

$$f([v]) = w, \quad v = u + w, \quad u \in U, \quad w \in W$$

Dimostrazione: Consideriamo la mappa lineare $g : V \to W$ definita da $f(v) = w$, dove $v = u + w$. Possiamo verificare che f è sia iniettiva che suriettiva. Inoltre abbiamo che $ker(g) = U$. Allora dalla proposizione (2.4) otteniamo un isomorfismo lineare $g_0 : V/U \to W$ definito da $g_0([v]) = w$. Otteniamo quindi il risultato con $f = g_0$.

Esempio: (2.6)
Sia $\mathbb{Q}[x]$ lo spazio vettoriale dei polinomi a coefficienti razionali. Sia $P_0 \subset \mathbb{Q}[x]$ il sottospazio dei polinomi costanti. Allora le classi di equivalenza in $\mathbb{Q}[x]/P_0$ sono date da polinomi che sono uguali tranne che per il termine noto.

6.3 Prodotti Diretti e Proiezioni

Un metodo standard per trovare una decomposizione come somma diretta $V = U \oplus W$ è attraverso operatori di proiezione:

Definizione: (2.7)
Un endomorfismo $\pi : V \to V$ è chiamato proiezione se $\pi^2 = \pi$. Se U è un sottospazio di V allora una proiezione su U è un operatore proiezione tale che $\pi(V) = U$.

Ricordiamo che dati due sottospazi U e W tali che $V = U \oplus W$ con la mappa π che proietta un vettore v sul sottospazio U. Allora $(Id - \pi)$ è una mappa che proietta v su W.

Lemma: (2.8)
Sia $\pi : V \to V$ una proiezione. Sia $U = \pi(V)$ e $W = ker(\pi)$. Allora, $V = U \oplus W$.

Dimostrazione:
Sia v in V. Allora $v = \pi(v) + (Id - \pi)(v)$ dove $\pi(v)$ e $(Id - \pi)(v)$. Infatti, $\pi(Id - \pi(v)) = \pi(v) - \pi^2(v) = 0$. 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 $t \in W \implies \pi(t) = 0$. Allora

$$0 = \pi(t) = \pi^2(v) = \pi(v) = t$$

e quindi $U \cap W = \{0\}$.

Nota: (2.9) In questo caso, possiamo descrivere W come l'immagine di $Id - \pi$, dove $Id : V \to V$ è la mappa identità. Infatti se $w \in ker(\pi)$, abbiamo che $w = (Id - \pi)(v)$.

Esempio: (2.10)

Sia $\mathbb{Q}[x]$ lo spazio vettoriale dei polinomi a coefficienti razionali. Allora $\mathbb{Q}[x] = P_0 \oplus P_{>0}$ è il sottospazio dei polinomi costanti P_0 e $P_{>0}$ è il sottospazio dei polinomi con termine noto 0. In questo caso la proiezione su P_0 è data da $\pi(f) = f_0$, dove f_0 è il termine noto di f.

Sia $(*,*)$ un prodotto scalare definito su uno spazio vettoriale reale V e sia U un sottospazio di V. Allora

$$U^{\perp} = \{v \in V \text{ t.c. } (u,v) = 0 \quad \forall u \in U$$

è chiamato il complemento ortogonale di U. Continuando, ricordiamo che per il processo di Gran-schmidt, se U ha dimensione finita, possiamo costruire una base ortonormale $B = \{u_1, .., u_j\}$ tale che $(u_i, u_j) = \delta_{ij}$.

Proposizione: (2.11)
Sia $(*,*)$ un prodotto scalare su uno spazio vettoriale reale V. Sia U un sottospazio di dimensione finita con base ortonormale $B = \{u_1, ..., u_n\}$. Allora

$$\pi(v) = \sum_{j=1}^{n} (v, u_j) u_j$$

è una proiezione su U.

Dimostrazione:

- $\pi(V) = U$ Per definizione, $v \in V \implies \pi(v)$ è una combianzione lineare della base b, e quindi $\pi(V) \subseteq U$.
  Viceversa, poichè B è una base ortonormale di U

  $$\pi(u_k) = \sum_{j=1}^{n} (u_k, u_j) u_j$$

  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, siccome B è base ortonormale di U abbiamo

  $$\pi^2(v) - \pi(v) = \pi\left(\sum_{j=1}^{n} c_j u_j\right) - \sum_{j=1}^{n} c_j u_j$$

  $$\sum_{j=1}^{n} c_j \pi(u_j) - \sum_{j=1}^{n} c_j u_j = \sum_{j=1}^{n} c_j u_j - \sum_{j=1}^{n} c_j u_j = 0$$

Corollario: (2.12)
Sia V uno spazio vettoriale con un prodotto scalare $(*,*)$ e sia U un sottospazio di dimensione finita. Allora $V = U \oplus U^{\perp}$.

Dimostrazione: Sia π la proiezione data nel Lemma (2.11). Un elemento $v \in V$ è in $ker(\pi)$ se e solo se $(u,v) = 0$ per ogni $u \in U$. quindi $ker(\pi) = U^{\perp}$. Il risultato ora segue dal lemma (2.8).

6.4 Esercizi

Esercizio 1:
Consideriamo il sottospazio

$$U = \{(x, y, 0) \text{ t.c. } x, y \in \mathbb{R}\} \subseteq \mathbb{R}^3$$

Scrivere esplicitamente la matrice di proiezione ortogonale $\pi : \mathbb{R}^3 \to \mathbb{R}^3$ corrispondente a U e calcolare $\mathbb{R}^3/U$.

Innanzitutto individuiamo il sottospazio ortogonale $U^{\perp} = \{(0, 0, z) \text{ t.c. } z \in \mathbb{R}\}$. in questo modo proiettondo su $U^{\perp}$ abbiamo $ker(\pi) = U$. E siccome la proiezione è una mappa lineare possiamo dire:

$$\pi(w) - \pi(v) = 0 \iff u \sim v$$

$$w - v \in U$$

Ricaviamo lo spazio quoziente $\mathbb{R}^3/U$ come tutti i piani affini al sottospazio U. La matrice di proiezione su $U^{\perp}$ risulta essere:

$$P = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Esercizio 2:
Consideriamo il sottospazio

$$U = \{(x, y, z) \text{ t.c. } x = y = z \in \mathbb{R}\} \subseteq \mathbb{R}^3$$

Scrivere esplicitamente la matrice di proiezione ortogonale $\pi : \mathbb{R}^3 \to \mathbb{R}^3$ corrispondente a U e calcolare $\mathbb{R}^3/U$.

Ancora una volta proiettiamo sul sottospazio ortogonale W con Base $B = \{(1, -1, 0)^T(1, 0, -1)^T\}$ composta da due vettori linearmente indipendenti e_1, e_2. Dato $v \in \mathbb{R}^3$ e $p = Ex$ proiezione sul piano W avente base $E = \{e_1, e_2\}$ possiamo calcolare la proiezione su W come $Id - \pi_U$ dove π_U è la proiezione su U. Dato $e = (1, 1, 1)^T$ il vettore di base di U allora:

$$e^T(v - ex) = 0 \wedge p = ex \implies x = \frac{e^T v}{e^T e}$$

$$p = \frac{ee^T}{e^T e} v \implies P_U = \frac{1}{6}\begin{pmatrix} 1 & 1 & -2 \\ 1 & 1 & -2 \\ -2 & -2 & 4 \end{pmatrix}$$

$$P_W = Id - P_U$$

La mappa P_W descrive una relazione di equivalenza per cui si costruisce lo spazio quoziente $\mathbb{R}^3/U$.

$$\pi(w) - \pi(v) = 0 \iff u \sim v$$

$$ker(\pi) = U \implies w - v \in U$$

Identifichiamo lo spazio quoziente $\mathbb{R}^3/U$ come tutti le rette parallele ad U.

7 Aritmetica modulare

7.1 Congruenze e operazioni mod n

Si fissi un intero $n > 1$. Siano a, b interi. Allora, diciamo che $a \equiv b \bmod n$ se e solo se n divide $a - b$.

Lemma: (1.1)
$\equiv$ (mod n) è una relazione di equivalenza su $\mathbb{Z}$.

Dimostrazione

- Riflessività: $a \equiv a \bmod n$ perchè $a - a = 0$ e $n \mid 0$.
- Simmetria: $a \equiv b \bmod n \implies n \mid (a - b) \implies n \mid b - a \implies b \equiv a \bmod n$
- Transitività: $a \equiv b \bmod n \implies n \mid a - b$. Allo stesso modo $b \equiv c \bmod n \implies n \mid b - c$. Siccome $a - c = (a - b) + (b - c)$ allora $n \mid a - c \implies a \equiv c \bmod n$.

Supponiamo adesso che $a, b \in \{0, 1, ..., n - 1\}$ e $a \equiv b \bmod n$. Scambiando a e b se necessario assumiamo che $a \geq b$. Allora

$$a \equiv b \bmod n \implies n \mid (a - b) \in \{0, ..., n - 1\}$$

e quindi $a - b = 0$, ovvero $a = b$. Sia

$$T = \{[0], ..., [n - 1]\}$$

Per il teorema della divisione, dato $a \in \mathbb{Z}$ esiste un' unica coppia di interi tali che

$$a = qn + r, \quad 0 \leq r < n$$

Definiamo $f : \mathbb{Z} \to T$ tramite $f(a) = [a]$. Allora

- $\mathbb{Z} = T$
- $f(a) = f(b) \iff a \equiv b \mod n$

La proposizione $f(\mathbb{Z}) = T$ è vera perchè $j \in \{0, ..., n - 1\} \implies f(j) = [j]$. Supponiamo adesso che $f(a) = f(b) = [r]$. Allora $a = nq + r$ e $b = nq' + r$ per interi q e q'. Quindi

$$a - b = n(q - q') \implies a \equiv b \bmod n$$

Viceversa se $a \equiv b \bmod n \implies n \mid (a - b)$ e quindi c'è un intero c tale che $a - b = nc$. Sia $a = nq + r$ con $0 \leq r < n$. Allora

$$a = a - b + b = nc + nq + r = n(c + q) + r$$

e quindi $f(a) = f(b)$. Insomme abbiamo dimostrato che:

Lemma: (1.3)
Sia $\mathbb{Z}_n$ lo spazio quoziente di Z rispetto a ($\equiv$ mod n . Sia T l'insieme definito precedentemente allora $f : \mathbb{Z} \to T$ definita da $f(a) = [a]$ definisce una bigezione da $\mathbb{Z}_\ltimes$ a T.

Adesso definiamo addizione e moltiplicazione su $\mathbb{Z}_n$ usando T.

Definizione (1.4)
Sia $[a], [b] \in T$. Allora

- $[a + b] = [a] + [b]$
- $[ab] = [a][b]$

Addizioni mod n

- la addizione mod n è una funzione. Infatti fissato un intero $n > 0$ abbiamo una funzione:

$$+_n : \mathbb{Z} \to \{0, 1, 2, ..., n - 1\}$$

Essa è definita tramite l'algoritmo della divisione $\text{mod}_n(a) = r$ dove r è unico ed apparteine a $\{0, 1, 2, ..., n - 1\}$ tale che $a = n \cdot q + r$ per qualche $q \in \mathbb{Z}$

- Funziona solo se viene rispettata la seguente proprietà
Fissato n un intero positivo > 1 e dati $a, b \in \mathbb{Z}$ si ha

$$a \text{ mod } n = a' \text{ e } b \text{ mod } n = b'$$

$$\implies (a + b) \text{ mod } n = (a' + b') \text{ mod } n$$

Dimostrazione
Per il teorema di divsione col resto.

$$a = n \cdot q_1 + a' \text{ e } b = n \cdot q_2 + b'$$

$$\text{con } 0 \leq a' \leq n - 1 \text{ e } 0 \leq b' \leq n - 1$$

$$(a + b) - (a' + b')$$

$$\iff n \cdot q_1 + a' + n \cdot q_2 + b' - (a' + b')$$

$$\implies n \mid n \cdot (q_1 + q_2)$$

$$\therefore (a + b) \equiv (a' + b') \text{ mod } n$$

Moltiplicazioni mod n

- la moltiplicazione mod n è una funzione. Infatti fissato un intero $n > 0$ abbiamo una funzione:

$$\cdot_n : \mathbb{Z} \to \{0, 1, 2, ..., n - 1\}$$

Essa è definita tramite l'algoritmo della divisione $\text{mod}_n(a) = r$ dove r è unico ed apparteine a $\{0, 1, 2, ..., n - 1\}$ tale che $a = n \cdot q + r$ per qualche $q \in \mathbb{Z}$

- Funziona solo se viene rispettata la seguente proprietà
Fissato n un intero positivo > 1 e dati $a, b \in \mathbb{Z}$ si ha

$$a \text{ mod } n = a' \text{ e } b \text{ mod } n = b'$$

$$\implies (a \cdot b) \text{ mod } n = (a' \cdot b') \text{ mod } n$$

Dimostrazione
Per il teorema di divsione col resto.

$$a = n \cdot q_1 + a' \text{ e } b = n \cdot q_2 + b'$$

$$\text{con } 0 \leq a' \leq n - 1 \text{ e } 0 \leq b' \leq n - 1$$

$$(a \cdot b) - (a' \cdot b')$$

$$\iff (n \cdot q_1 + a') \cdot (n \cdot q_2 + b') - (a' \cdot b')$$

$$n \cdot (n \cdot q_1 \cdot q_2 + q_1 \cdot b' + a' \cdot q_2) + (a' \cdot b') - (a' \cdot b')$$

$$\therefore (a \cdot b) \equiv (a' \cdot b') \text{ mod } n$$

Nota: (1.5) Dati $a, b \in \{0, 1, ..., n - 1\}, a + b$ o ab potrebbero essere maggiori di n. In questo caso, dobbiamo scrivere $a + b = qn + r$ o $ab = q'n + r'$ dove $0 \leq r < n$ e definiamo $[a + b] = [r]$ o $[ab] = [r']$

Esempio: (1.10)
Sia n un intero. Allora n è divisibile per 4 se e solo se le due ultime due cifre in base 10 sono divisibili per 4. Per vedere questo, nostiamo che $4 \mid 100$. Quindi

$$n = (a_m 10^m + \cdots + a_2 10^2) + a_1 10 + a_0$$

da cui si vede che $n \mid a_1 10 + a_0$ mod 4.

7.2 Residui quadratici

Definizione: (1.11)
Un numero intero m si dice residuo quadratico mod n se l'equazione $x^2 \equiv mmodn$ ha una soluzione con x intero, ovvero se esiste un intero tale che $x^2 \equiv m \pmod{n}$.

Esempio: (1.12) Calcoliamo tutti i quadrati mod 5.

$$\begin{array}{c|ccccc} a & 0 & 1 & 2 & 3 & 4 \\ a^2 & 0 & 1 & 4 & 4 & 1 \end{array}$$

Quindi a è un residuo quadratico se solo se $a \equiv 0, 1, 4 \text{mod } n$.

Esempio: (1.13) Osserviamo che $p = 2$ è l'unico numero primo pari. Tutti gli altri numeri primi sono $\equiv 1 \bmod 4$ oppure $\equiv 3 \bmod 4$.

Teorema: (1.14)
Siano p e q distinti numeri primi e dispari.

- Se $p \equiv 1 \bmod 4$ oppure $q = \equiv 1 \bmod 4$ allora $x^2 \equiv p \bmod q$ ha una soluzione se e solo se $x^2 \equiv q \bmod p$ ha una soluzione.
- Se $p \equiv 3 \bmod 4$ e $q = \equiv 3 \bmod 4$ allora $x^2 \equiv p \bmod q$ ha una soluzione se e solo se $x^2 \equiv -q \bmod p$ ha una soluzione.

Esempio: (1.15)
$x^2 \equiv p \bmod q$, $y^2 \equiv q \bmod p$.

- $(p, q) = (3, 13) : 4^2 = 16 \equiv 3 \bmod 13$, $1^2 = 1 \equiv 13 \bmod 3$.
- $(p, q) = (5, 29) : 11^2 = 121 \equiv 5 \bmod 29$, $2^2 = 4 \equiv 29 \bmod 5$.
- $(p, q) = (7, 29) : 6^2 = 36 \equiv 7 \bmod 29$, $1^2 = 1 \equiv 29 \bmod 7$.

Esempio: (1.16)
Abbiamo visto che $x^2 \equiv 3 \bmod 5$ non ha soluzioni. Il teorema implica che $x^2 \equiv 5 \equiv 2 \bmod 3$ non ha soluzioni.

Esempio: (1.15)
$x^2 \equiv p \bmod q$, $y^2 \equiv -q \bmod p$.

- $(p, q) = (3, 11) : 4^2 = 16 \equiv 3 \bmod 13$, $1^2 = 1 \equiv -11 \equiv 1 \bmod 3$.
- $(p, q) = (7, 19) : 8^2 = 64 \equiv 7 \bmod 19$, $3^2 = 9 \equiv -19 \bmod 7$.
- $(p, q) = (11, 19) : 7^2 = 49 \equiv 11 \bmod 19$, $5^2 = 25 \equiv -19 \bmod 11$.
- $(p, q) = (3, 23) : 7^2 = 49 \equiv 3 \bmod 23$, $1^2 = 1 \equiv -23 \bmod 3$.

Proposizione: (1.18)
La congruenza $x^2 \equiv -1 \bmod p$ ha soluzione se e solo se p è congruente a 1 mod 4.

Esempio: (1.19)

- $(p, q) = (13, 29) : 10^2 = 100 \equiv 13 \bmod 29$, $4^2 = 8 \equiv 3 \text{mod } 13$
- $(p, q) = (23, 29) : 9^2 = 81 \equiv 23 \bmod 29$, $11^2 = 121 \equiv 6 \text{mod } 23$
- $(p, q) = (3, 37) : 15^2 = 225 \equiv 3 \bmod 37$, $1^2 = 1 \equiv 37 \text{mod } 3$

Esempio: (1.20)

- $(p, q) = (7, 31) : 10^2 = 100 \equiv 7 \bmod 31$, $2^2 = 4 \equiv -31 \text{mod } 7$
- $(p, q) = (19, 31) : 9^2 = 81 \equiv 19 \bmod 31$, $8^2 = 64 \equiv -31 \text{mod } 19$
- $(p, q) = (11, 43) : 21^2 = 11 \equiv 11 \bmod 43$, $1^2 = 1 \equiv -43 \text{mod } 11$

7.3 Sistemi di equazioni lineari modulari

Possiamo anche considerare sistemi lineare $(A|b)$ usando l'aritmetica modulare modulo n. Per la regola di cramer ci aspetteremmo $Ax \equiv b \bmod n$ ha una soluzione se possiamo risolvere l'equazione $[\delta][det(A)] \equiv 1 \bmod n$, purchè A sia quadrata.

Esempio: (1.21)
Sia

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}$$

allora, $det(A) = 2$ e

$$A^{-1} = \frac{1}{2}\begin{pmatrix} 3 & -1 \\ -1 & 1 \end{pmatrix}$$

Sia $n = 5$. Poichè $[3][2] \equiv [1] \bmod 5$ ne segue che

$$A^{-1} \bmod 5 = [3]\begin{pmatrix} [3] & [-1] \\ [-1] & [-1] \end{pmatrix} = \begin{pmatrix} [4] & [2] \\ [2] & [3] \end{pmatrix}$$

D'altra parte, per $n = 4$, non c'è una soluzione di $[2][c] \equiv [1] \bmod 4$, quindi proviamo con il metodo di riduzione per righe.

$$(A|b) = \begin{pmatrix} [1] & [1] & | & [b_1] \\ [0] & [2] & | & [b_2 - b_1] \end{pmatrix}$$

Allora, se x è il vettore colonna corrispondente a (x_1, x_2) dobbiamo poter risolvere $2[x_2] \equiv [b_1 - b_2] \bmod 5$ per essere in grado di risolvere $Ax \equiv b \bmod 4$. Per esempio, se (b_1, b_2) allora $Ax = b$ non ha una soluzione $\bmod 4$.

7.4 Esercizi

Esercizio 1
Dimostrare che un intero n è divisibile per 9 se solo se la somma della sue cifre è divisibile per 9.

Scriviamo un qualsiasi numero n in base 10.

$$n = a_m 10^m + \cdots + a_0 \implies a_m(9+1)^m + \cdots + a_0$$

Scriviamo il binomio di newton $\sum_{k=0}^{m} \binom{m}{k} 9^k 1^{m-k} = b_m$ dunque

$$a_m b_m + \cdots + a_0$$

Notiamo che tutti i termini della sommatoria sono divisibili per 9 tranne il termine con $k = 0$. Allora ogni $a_m b_m = \sum_{k=1}^{m} \binom{m}{k} 9^k 1^{m-k} a_m + a_m \implies a_m b_m = 9k_m + a_m$. Se dividessimo per 9 avremmo come resto la somma delle singole cifre che ci porta alla condizione

$$[a_m + \cdots + a_0] \equiv 0 \bmod n$$

Esercizio 2
Siano a, b due numeri interi. Dimostrare che $10a + b$ è divisibile per 7 se e solo se $a - 2b$ è divisibile per 7.

$$10a + b \equiv 0 \bmod 7 \equiv [3]a + [1]b \equiv 0 \bmod 7$$

Divido entrambi i lati per l'inverso moltiplicativo $\mod 5$ di [3] ovvero [5].

$$a + [5]b \equiv 0 \equiv a + [-2]b \bmod 7$$

Siccome $-2 \in [5]$. Abbiamo già dimostrato che $\equiv$ è una relazione di equivalenza, allora possiamo percorrere il percorso al contrario per il viceversa.

Esercizio 3
Sia

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

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.

La condizione è equivalente all' esistenza di inverso moltiplicativo. Ricordandoci delle equazione diofantee possiamo dire che se sono coprimi allora esiste una soluzione. Si ricava che il primo numero primo a essere corpimo con 360 è 7.

$$\begin{pmatrix} [2] & [0] & [6] \\ [2] & [5] & [1] \\ [4] & [3] & [1] \end{pmatrix}^{-1} = [2]^{-1} \begin{pmatrix} [2] & [2] & [0] \\ [4] & [6] & [1] \\ [5] & [3] & [3] \end{pmatrix} = [4] \begin{pmatrix} [2] & [2] & [0] \\ [4] & [6] & [1] \\ [5] & [3] & [3] \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} [1] & [1] & [0] \\ [2] & [3] & [4] \\ [6] & [5] & [5] \end{pmatrix}$$

Esercizio 4
Calcola l'insieme dei residui quadratici modulo 7.

Calcoliamo tutti i quadrati mod 7.

$$\begin{array}{c|ccccccc} a & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ a^2 & 0 & 1 & 4 & 2 & 2 & 4 & 1 \end{array}$$

Quindi a è un residuo quadratico se solo se $a \equiv 0, 1, 2, 4 \bmod 7$.

8 Introduzione ad Anelli e Domini

8.1 Anelli commutativi con identità e Domini integrali

Definizione: (1.1)
Un anello commuatativo con identità è un insieme R con due mappe $+ : R \times R \to R$ e $* : R \times R \to R$ che soddisfano le seguenti proprietà.

- chiusura per $+$ e $*$
- associatività per $+$ e $*$
- commutatuvità per $+$ e $*$
- elementi identità 0 per $+$ e 1 per $*$
- inverso additivo (non è necessaria l'esistenza dell' inverso moltiplicativo)
- distributività

Esempio: (1.2)
Sia R un' anello commutativo con identità. Allora, possiamo definire l'anello polinomiale $R[x]$ come l'insieme di elementi della forma

$$f(x) = a_n x^n + \cdots + a_0, \quad a_n, ..., a_0 \in R$$

rispetto alle regole usuali per addizione e moltiplicazione tra polinomi. Un polinomio $f \in R[x]$ definisce una funzione $ev(f) : R \to R$ 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 esemepio 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: (1.3)
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:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1) * (r_2, s_2) = (r_1 r_2, s_1 s_2)$$

L'elemento identità per l'addizione è $(0_R, 0_S)$ l'elemento identità per la moltiplicazione è $(1_R, 1_S)$.

Esempio: (1.4)
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

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad f([x]_{mn}) = ([x]_m, [x]_n)$$

è una mappa ben definita tale che

$$f([x + y]_{mn}) = f([x]_{mn}) + f([y]_{mn}), \quad f([x]_{mn}[y]_{mn}) = f([x]_{mn}) * f([y]_{mn})$$

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 $y' = y + \beta mn$.

Una grande differenza tra Z e Z_n è la seguente: 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 $\mathbb{Z}_n$.

Definizione: (1.5)
Un dominio integrale è un anello commutativo con identità con la seguente proprietà:

$$a * b = 0 \implies a = 0 \lor b = 0$$

Esempio: (1.6)
$\mathbb{Q}[x]$ è un dominio integrale rispetto alle operazioni usuali di addizione e moltiplicazione polinomiale. Se R e S sono anelli commutativi con identità, allora $R \times S$ non è mai un dominio integrale perchè $(1_R, 0_S) * (0_R, 1_S) = (0_R, 0_S)$.

Strettamente correlata con le proprietà di essere un dominio integrale è l'esistenza di inversi moltiplicativi.

Definizione (1.7)
Sia $(R, +, *)$ un anello commutativo con identità. Allora un elemento non nullo u di 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: (1.8)
$[a] \in \mathbb{Z}_n$ è un unità se e solo se $mcd(a, n) = 1$.

Dimostrazione:
Supponiamo che $[a][b] = [1]$ in $\mathbb{Z}_n$. Allora esiste un numero intero c tale che $ab = 1+cn$, il che implica che $ab + (-c)n = 1$ dunque $mcd(a, n) = 1$. Viceversa, se $mcd(a, n) = 1$, allora esistono interi b e c tali che $ab + cn = 1$ e quindi $[a][b] = [1]$ in $\mathbb{Z}_n$.

Nota Importante: Se in un anello commutativo nonzero con identità esiste sempre l'inverso moltiplicativo allora questo è un dominio integrale. D'altra parte in un dominio integrale non deve esistere sempre l'inverso moltiplicativo.

Corollario: (1.9)
Sia p un numero primo. Allora, ogni elemento non nullo in $\mathbb{Z}_p$ è un unità.

Dimostrazione:
Se $a \in \{1, ..., p-1\}$ è primo allora $mcd(a, p) = 1$.

8.2 Funzione ϕ di Eulero

Definizione: (1.10)
La funzione $\phi : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ sugli interi positivi, definita da $\phi(1) = 1$ mentre $\phi(n) =$ al numero di unità presenti in $\mathbb{Z}_n$, si chiama funzione ϕ di Eulero.

Esempio: (1.11)
Calcoliamo i primi 6 valori della funzione ϕ di Eulero.

n	1	2	2	3	4	5
$U(n)$	$-$	$\{[1]\}$	$\{[1],[2]\}$	$\{[1],[3]\}$	$\{[1],[2],[3],[4]\}$	$\{[1],[5]\}$
$\phi(n)$	1	1	2	2	4	2

Esempio: (1.12)
Se p è un numero primo allora $\phi(p) = p - 1$ per il corollario (1.9). Più generalemente, 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 $mcd(a, p^r) = 1$ a meno che a non sia un multiplo di p. Il numero di tali multipli in $\{0, ..., p^r - 1\}$ è $p^r - 1$.

Lemma: (1.13)
Siano A e B insiemi finiti della stessa caridnalità. Allora la seguenti affermazioni 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 iniettiva allora $|f(A)| = |A|$. Allora $|f(A)| = |A| = |B|$ e quindi f è sureittiva. Similmente, per mostrare che se $f : A \to B$ è suriettiva allora $f : A \to B$ è iniettiva, consideriamo il constrapposto: 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 di cardinalità per renderli rigorosi.

Supponiamo adesso che $mcd(m, n) = 1$ dove $m, n > 1$. Allora dati interi a e b esiste un intero c tale che.

$$c \equiv a \bmod m\,, \quad c \equiv b \bmod n$$

Ricordiamo a questo punto per per il teorema di Bezout, esistono interi u, v tali che:

$$mu + nv = mcd(m.n) = 1$$

Sia $c = anv + bmu$. Allora

$$c = a(1 - mu) + bmu = a + mu(b - a) \equiv a \bmod m$$

$$c = anv + b(1 - nv) = nv(a - b) + b \equiv b \bmod n$$

Corollario: (1.14 | Teorema cinese del Resto)
Supponiamo che m, n siano intero > 1 tali che $mcd(m, n) = 1$. Allora la mappa $f([x]_{mn}) = ([x]_m, [x]_n)$ da $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ considerata precedentemente è una bigezione.

Dimostrazione:
La suriettività di f segue dall' esistenza dell'intero c visto prima (Th. Cinese Del Resto). Poichè $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ sono finiti e hanno la stessa cardinalità allora f è anche iniettiva per il lemma (1.13). Dunque f è una bigezione.

Proposizione: (1.15)
Supponiamo che m, n sono interi > 1 tali che $mcd(m, n) = 1$. 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 funzione $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ vista precedentemente si restringe a una bigezione da C a $A \times B$. In particolare, abbiamo $\phi(mn) = |C| = |A||B| = \phi(m)\phi(n)$.

Dimostrazione:
Per definizione $f^{-1}(A \times B) = \{[x] \in \mathbb{Z}_{mn}$ t.c.$f(x) \in A \times B$. Inoltre, poichè $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ 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

$$[c]_{mn} = f^{-1}([a]_m, [b]_n), \quad [c']_{mn} = f^{-1}([a]_m^{-1}, [b]_n^{-1})$$

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, poichè $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ 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 $mcd(c, mn) = 1$ e quindi per il teorema di Bezout, esistono interi μ e ν tali che $c\mu + (mn)\nu = 1$. Allora,

$$c\mu + m(n \ni) = 1 \implies mcd(c, m) = 1, \quad c\mu + n(m \ni) = 1 \implies mcd(c, n) = 1$$

e quindi $[c]_m$ è una unità di $\mathbb{Z}_m$ e $[c]_n$ è una unità di $\mathbb{Z}_n$. Come tali, $[c]_{mn} \in f^{-1}(A \times B)$.

Teorema: (1.16)

Sia n un intero positivo. Allora

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

Dimostrazione:
Consideriamo gli insiemi $S_d = \{m \in \mathbb{Z} \text{ t.c. } 1 \leq m < n, \quad mcd(m,n) = d\}$ ma $mcd(m,n) = d \implies mcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.Siccome poi ne vorremo trovare la cardinalità riscriviamo l'insieme nel seguente modo

$$S_d = \left\{k \in \mathbb{Z} \text{ t.c. } 1 \leq k \leq \frac{n}{d}, \ \ mcd\left(k, \frac{n}{d}\right) = 1\right\}$$

In questo modo stiamo contando fino n/d invece di contare fino a n e poi dividere per d. Ora si deve dimostrare che le classi S_d sono una partizione $\mathcal{P}$ dell'insieme $N = \{1, ..., n\}$. Qualsiasi $l \in N$ appartiene alla classe $S_{mcd(l,n)}$. Si trattano inoltre di insiemi disgiunti $\cap_i S_{d_i} = \emptyset$ in quanto, se si supponesse per assurdo che esistesse un elemento, avremmo $m' \in S_d \wedge m' \in S_{d'} \implies mcd(m', n) = d \wedge mcd(m', n) = d$. Siccome il massimo comun divisore è ben definito per definizione allora le classi S_d formano una partizione $\mathcal{P}$. La cardinalità di N può essere trovata anche sommando la cardinalità delle singole classi (perchè sono disgiunte).

$$\#S_d = \phi(n/d) \implies \sum_{d|n} \phi(n/d) = \#N$$

A questo punto $d \mid n \implies n = de \implies d = \frac{n}{e}$ per un qualche $e \mid n$. Dunque vuol dire che l'insieme dei divisori di n è lo stesso dell' insieme $\{\frac{n}{d} \text{ t.c. } d \mid n\}$. Sostituiamo nella funzione di eulero:

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

Proposizione: (1.17)
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

$$\begin{aligned} \phi(n) &= \phi(p_1^{r_1}) \cdots \phi(p_k^{r_k}) \\ &= p_1^{r_1}\left(1 - \frac{1}{p_1}\right) p_2^{r_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{r_k}\left(1 - \frac{1}{p_k}\right) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \end{aligned}$$

Il prossimo risultato è una generalizzazione del piccolo teorema di fermat.

8.3 Teorema di Eulero

Enunciato: (1.17)
Siano a e n due interi positivi con $n > 1$. Se $mcd(a,n) = 1$ allora $a^{\phi(n)} \equiv 1 \mod n$.

Dimostrazione:
Prima, notiamo che se R è un anello commutatuvo con identità, allora il prodotto di due unità di R è ancora un 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 il prodotto di tutte le unità

$$u = \prod_{s \in S} s$$

è una unità di R.
Sia $v \in S$. Allora la mappa $f : S \to S$ definita da $f(s) = us$ è iniettiva:

$$f(s) = f(s') \implies vs = vs' \implies v^{-1}vs = v^{-1}vs' \implies s = s'$$

Poichè S è finito, ne segue che f induce una bigezione da S a S. Perciò

$$u = \prod_{s\in S} s = \prod_{s\in S} f(s) = \prod_{s\in S} vs = v^{\phi(n)}u$$

e quindi $v^{\phi(n)} = 1$ perchè u è un unità. Per finire la dimostrazione, notiamo che $mcd(a, n) = 1$ implica che $[a] \in R$ è una unità. Ponendo $v = [a]$ ne segue che $[a]^{\phi(n)} = [1]$ in R ovvero $a^{\phi(n)} \equiv 1 \mod n$.

Corollario: (1.18)
Sia n un intero libero da quadrati, cioè n non è divisibile per nessun quadrato maggiore di 1. Allora se $b \equiv 1 \mod \phi(n)$ abbiamo $a^b \equiv a \mod n$ per ogni a.

Dimostrazione:
Se n è libero da quadrati, vuol dire che quando scriviamo la fattorizzazione in primi $n = p_1^{k_1} \cdots p_r^{k_r}$, tutti gli esponenti sono uguali a 1, cioè è un prodotto di primi distinti. Ora $a^b \equiv a \mod n$ se e solo se $a^b \equiv a \mod p_i$ per ogni i.(Per il Th. Cinese del Resto)
Se $a \equiv 0 \mod p_i$ questo è ovvio. Se $a \not\equiv p_i$, visto che $\phi(p_i) \mid \phi(n)$, otteniamo che b è $\equiv 1 \mod n$. Segue dal piccolo teorema di fermat che $a^b \equiv a \mod p_i$.

8.4 Esercizi

Esercizio 1
Usare il teorema di Eulero per dimostrare che $3^{102} \equiv 9 \mod 10$.

Si nota che $mcd(3, 10) = 1$ e che $\phi(10) = 5$ dunque.

$$[3^{102}] = [3^2][3^{100}] = [9] \quad \text{in } R = \mathbb{Z}_{10}$$

Notiamo che $mcd(9, 10) = 1$ dunque esiste l'inverso moltiplicativo e perciò moltiplichiamo entrambi i lati per $[9]^{-1}$.

$$[9]^{-1}[9][3^{100}] = [9][9]^{-1} \quad \text{in } R = \mathbb{Z}_{10}$$
$$[3^{100}] = [(3^{20})^5] = [1] \quad \text{in } R = \mathbb{Z}_{10}$$

A questo punto poniamo $a = 3^{20}$, per il teorema di eulero questa equazione è sempre vera.

Esercizio 2
Dimostrare che se R e S sono anelli commuatativi con identità allora anche $R\times S$ è un anello commutativo con identità rispetto ad addizione e moltiplicazione.

Definiamo $(R \times S, +, *)$ dove $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ e $(r_1, s_1) * (r_2, s_2) = (r_1 * r_2, s_1 * s_2)$.

- Chiusura: Siccome $(R, +, *)$ è un anello allora è chiuso rispetto alle due mappe. Segue che $r_1 + r_2 \in R$ e $r_1 * r_2 \in R$. Si fa la stessa osservazione per $(S, +, *)$. Dunque $(r_1 * r_2, s_1 * s_2) \in R \times S$ e$(r_1 + r_2, s_1 + s_2) \in R \times S$. Ricaviamo che $R \times S$ è chiuso sotto queste due operazioni.

- Associatività: Controlliamo se $[(r_1, s_1) + (r_2, s_2)] + (r_3, s_3)$è uguale a $(r_1, s_1) + [(r_2, s_2) + (r_3, s_3)]$. Siccome R e S sono anelli possiamo scrivere.

$$((r_1 + r_2) + r_3, (s_1 + s_2) + s_3) = (r_1 + (r_2 + r_3), s_1 + (s_2 + s_3) = (r_1, r_2) + [(s_1, s_2) + (r_3, s_3)]$$

Analogamente per la seconda mappa.

- Commutatività: Controlliamo se $(r_1, s_1) + (r_2, s_2)$ è uguale a $(r_2, s_2) + (r_1, s_1)$. Siccome R e S sono anelli commutativi allora:

$$(r_1 + r_2, s_1 + s_2) = (r_2 + r_1, s_2 + s_1) = (r_2, s_2) + (r_1, s_1)$$

  Analogamente per la seconda mappa.

- Elementi identità Si trova che $(0_R, 0_S)$ è l'elemento identità per $R \times S$ in quanto R e S sono anelli da cui si ricava.

$$(r_1 + 0_R, s_1 + 0_S) = (r_1, s_1) = (0_R + r_1, 0_S + s_1)$$

  Per la seconda mappa $(1_R, 1_S)$ risulta essere l'elemento identità per lo stesso motivo.

$$(r_1 * 0_R, s_1 * 0_S) = (r_1, s_1) = (0_R * r_1, 0_S * s_1)$$

- Esistenza di Inversi: Per la prima mappa esiste sempre l'inverso (comunemente chiamato inverso additivo) in quanto:

$$(r_1, s_1) + (-r_1, -s_1) = (r_1 + (-r_1), s_1 + (-s_1)) = (0_R, 0_S$$

  Per la seconda mappa non è detto che esista $r_1^{-1} \in R$ e $s_1^{-1} \in S$. Dunque (r_1^{-1}, s_1^{-1}) non è detto appartenga a $R \times S$.

- Distributività:

$$(r_1, s_1) * [(r_2, s_2) + (r_3, s_3)] = (r_1 * (r_2 + r_3), s_1 * (s_2 + s_3)$$

$$(r_1 * (r_2 + r_3), s_1 * (s_2 + s_3) = (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3) = (r_1 r_2, s_1, s_2) + (r_1 r_3, s_1 s_3)$$

$$(r_1 r_2, s_1, s_2) + (r_1 r_3, s_1 s_3) = (r_1, s_1) * (r_2, s_2) + (r_1, s_1) * (r_3, s_3)$$

Esercizio 3
Dimostrare che se R è un Dominio Integrale allora $R[x]$ è un Dominio integrale.

Definiamo gli elementi di $R[x]$ come

$$f(x) = a_n x^n + \cdots + a_0, \quad a_n, ..., a_0 \in R$$

Dove gli $a_n, ..., a_0$ possono essere 0_R e 1_R. Verifichiamo innanzitutto che si tratta di un anello.

- Chiusura: Dati due polinomi f, g in $R[x]$ prendiamo, senza perdere di generalità, il polinomio di grado f tale che $deg(f) \geq deg(g)$

$$f + g = (a_r + a'_r)x^n + \cdots + (a_0 + a'_0$$

  Siccome R è un anello (chiuso) allora si ricava che $f + g \in R[x]$.
  Per la seconda mappa invece prendiamo i due insiemi $R_f = \{a_n, ..., a_0\} \subseteq R$ e $R_g = \{a'_n, ..., a'_0\} \subseteq R$.Tutti gli elementi in $R_f \times R_g$ verranno moltiplicati senza contare l'ordine dei fattori. per la proprietà distributiva possiamo associare rispetto a x^r. In questo modo avremo

$$f + g = (a''_{2n})x^{2n} + \cdots + (a''_0)$$

  Dove gli a'' appartengono a R (le due mappe sono chiuse su R).

- Associatività: Controlliamo se $(f + g) + h = f + (g + h)$. Siccome R è un dominio integrale possiamo scrivere:

$$(f + g) + h = ((a_n + a'n) + a''n)x^n + \cdots + ((a_0 + a'_0) + a''_0), \quad a_n/a'_n/a''_n, ..., a_0/a'_0/a''_0 \in R$$

$$((a_n + a'n) + a''n)x^n + \cdots + ((a_0 + a'_0) + a''_0) = (a_n + (a'n + a''n))x^n + \cdots + (a_0 + (a'_0 + a''_0)$$

$$(a_n + (a'n + a''n))x^n + \cdots + (a_0 + (a'_0 + a''_0) = f + (g + h)$$

  Per la distriubutività dell' anello R si dimostra che $(f * g) * h = f * (g * h)$ in quanto quando si moltiplicano i fattori in $R_g \times R_f \times R_h$ l'ordine non conta.

- Commutatività: Controlliamo se $f+g=g+f$. Siccome R è un dominio integrale possiamo scrivere:

$$f+g=(a_n+a'n)x^n+\cdots+(a_0+a_0'),\quad a_n/a_n',...,a_0/a_0' \in R$$

$$(a_n+a'n)x^n+\cdots+(a_0+a_0')=(a_n'+a_n)x^n+\cdots+(a_0'+a_0)=g+f$$

Per la seconda mappa un'altra volta l'ordine dei fattori in $R_f \times R_g$ è invariante dunque $f*g=g*f$,per la proprietà distributiva.

- Elementi identità: Il polinomio avente solo coefficienti $a_i=0_R$ è l'elemento identità per $+$.

$$f+0_{R[x]}=(a_n+0_R)x^n+\cdots+(a_0+0_R)=(0_R+a_n)x^n+\cdots+(0_R+a_0)=a_nx^n+\cdots a_0=f$$

Il polinomio avente il coefficiente $a_0'=1_R$ e tutti gli altri coefficienti $a_{i>0}'=0_R$.

$$f*1_{R[x]}=\left(\sum_{i=0}^{n}a_n*a_i'\right)x^n+\cdots+\left(\sum_{i=0}^{n}a_0*a_i'\right)=(a_n*1_R)x^n+\cdots\cdot+(a_0*1_R)$$

$$(1_R*a_n)x^n+\cdots\cdot+(1_R*a_n)=a_nx^n+\cdots+a_0=f$$

- Esistenza di Inversi: Per la prima mappa esiste sempre l'inverso (comunemente chiamato inverso additivo) in quanto:

$$f+(-f)=(a_n+(-a_n)x^n+\cdots+(a_0+-a_0)=0_{R[X]}$$

e $-f$ appartiene a $R[x]$ perchè $-a_[i]$ appartiene a R. Per la seconda mappa ricaviamo

$$f*f^{-1}=\left(\sum_{i=0}^{n}a_n*a_i^{-1}\right)x^{2n}+\cdots+\left(\sum_{i=0}^{n}a_0*a_i^{-1}\right)$$

Il termine costante del polinomio deve essere 1_R

$$\sum_{i=0}^{n}a_0*a_i^{-1}=a_0\left(\sum_{i=0}^{n}a_i^{-1}\right)=1_R$$

Dunque deve esistere $\sum_{i=0}^{n}a_i^{-1}$ inverso moltiplicativo di a_0 e essere 0_R per annullare gli altri fattori. Ciò è impossibile.

- Distributività:

$$f*(g+h)=\left(\sum_{i=0}^{n}a_n*(a_i'+a_i'')\right)x^n+\cdots+\left(\sum_{i=0}^{n}a_0*(a_i'+a_i'')\right)$$

$$=\left(\sum_{i=0}^{n}a_n*a'i\right)x^n+\cdots+\left(\sum_{i=0}^{n}a_0*a'i\right)+\left(\sum_{i=0}^{n}a_n*a''i\right)x^n+\cdots+\left(\sum_{i=0}^{n}a_0*a''i\right)=f*g+f*h$$

- Dominio Integrale: Per verificare l'ulitmo proprietà dobbiamo dimostrare che $f*g=0_R[x] \iff f=0_{R_[x]}\vee g=0_{R[x]}$. Innanzitutto scriviamo $f*g$

$$\left(\sum_{i=0}^{n}a_na_i'\right)x^n+\cdots+\left(\sum_{i=0}^{n}a_0*a_i'\right)$$

Affinchè sia $0_{R[x]}$ ogni termine deve essere $=0$. Affinchè ogni termine sia 0_R allora $a_i=0_R\vee a_i'=0_R \implies f=0_{R_[x]}\vee g=0_{R[x]}$. Viceversa se $f=0_{R_[x]}\vee g=0_{R[x]}$ è facile verificare $f*g=0_R[x]$ (calcolare brutalmente).

Esercizio 4
Dimostrare che se R è un dominio integrale con un numero finito di elementi e $a \in R - 0 = R^*$, allora $f : R^* \to R^*, \quad f(x) = ax$ è suriettiva.

Siccome la mappa f ha come dominio e codominio lo stesso insieme finito R allora per il lemma (1.15) possiamo dimostrare la suriettività dimostrandone l'iniettività.

$$f(s) = f(s') \iff as = as' \iff as - as' = 0 \iff a(s - s') = 0$$

Quindi R è un dominio integrale $a(s - s') = 0 \iff a = 0 \lor (s - s') = 0$. Siccome $a \in R^*$ allora non può essere 0. Dunque $s - s' = 0 \iff s = s'$. La manipolazione fatta sopra si fa su R non su R^* in quanto R^* non è un dominio integrale.

Esercizio 5:
Quali sono i numeri che se divisi per 6 danno resto 5, se divisi per 5 danno resto 4, se divisi per 3 danno resto 2 e se divisi per 2 danno resto 1.

Modelliamo questo sistema di congruenze e poi vediamo se possiamo applicare il teorema cinese del resto.

$$\begin{cases} x \equiv 5 \bmod 6 \\ x \equiv 4 \bmod 5 \\ x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 2 \end{cases}.$$

Si nota subito che le ultime due congruenze sono modulo 2 e 3 e entrambi non sono coprimi a 6. Dunque o il sistema è irrisolvibile o sono coerenti con la prima congruenza. Si verifica facilmente che una soluzione qualsiasi della prima congruenza risolve sempre entrambe le ultime due congruenze. Risolviamo dunque il sistema limitandoci alle prime due equzioni. Il modus-operandi è il solito: Si individua $c = anv + bmu$ che soddisfa entrambe le congruenze. Si nota che esistono infinite soluzioni del tipo $[c]_{mn}$ in quanto:

$$a(1 - mu) + bmu + kmn = a - mu(b - a) + kmn \equiv a \bmod m$$

$$anv + b(1 - nv) + kmn = b - nv(a - b) + kmn \equiv b \bmod n$$

Dunque per 6 e 5 troviamo $6u + 5v = 1$. Applicando euclide esteso troviamo u e v.

$$mcd(1 \cdot 5 + 1, 5|u, v) = mcd(1, 5|u, u + v) = mcd(5, 1|u + v, u)$$

$$mcd(5 \cdot 1, 1|u + v, u) = mcd(0, 5|u + v, 6u + 5v) = mcd(5, 0|6u + 5v, u + v$$

$$c(-1, 1) \implies c(-6 + 5) = 1 \implies c = -1 \implies (1, -1)$$

Dunque abbiamo trovato $c = (5)(5)(-1) + (4)(6)(1) = [-1]_{30}$.

Esercizio 6:
Trova le soluzioni di $x \equiv 5 \bmod 7$ e $x \equiv 3 \bmod 13$.

Con $a = 5$, $m = 7$, $b = 3$, $n = 13$. Applichiamo euclide esteso per trovare u e v che risolvono l'identità di bezout $7u + 13v = 1$.

$$mcd(7, 13|u, v) = mcd(13, 7|v, u) = mcd(7 \cdot 1 + 6|v, u) = mcd(6, 7|v, u + v)$$

$$mcd(7, 6|u + v, v) = mcd(6 \cdot 1 + 1, 6|u + v, v) = mcd(1, 6|u + v, u + 2v)$$

$$mcd(6, 1|u + 2v, u + v) = mcd(6 \cdot 1, 1|u + 2v, u + v) = mcd(0, 1|u + 2v, 7u + 13v)$$

$$mcd(1, 0|7u + 13v, u + 2v)$$

$$c(-2, 1) \implies c(-14 + 13) = 1 \implies c = -1 \implies (u, v) = (2, -1)$$

Perciò $c = anv + bmu = (5)(13)(-1) + (3)(7)(2) = -23 + k91$.

9 Teoria dei Gruppi

9.1 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: $(a * b) * c = a * (b * c)$.
- Identità: Esiste $e \in G$ tale che $e * a = a = a * e$ 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 $a, b \in G$. Ora vediamo di dimostrare altre proprietà importanti.

Proprietà: (1.1.a)
$ab = cb \implies a = c$.

Dato $ab = cb$ esiste per la definizione di gruppo $a^{-1} \in G$. Dunque possiamo scrivere $abb^{-1} = cbb^{-1} \implies ae = ce \implies a = c$. Segue che se il gruppo è abeliano cancellazione a sinistra e a destra sono equivalenti. Tutto ciò funziona per il fatto che $f(x) = xb^{-1}$ è ben definita.(Esercizio 1 - Relazioni di Equivalenza).

Proprietà:(1.1.b)
La commutatività del fattore identità non è un assioma bensì un corollario.

Partiamo dimostrando $aa^{-1} = e \implies a^{-1}a = e$.

$$e = a^{-1}(a^{-1})^{-1} = (a^{-1}e)(a^{-1})^{-1} = (a^{-1}aa^{-1})(a^{-1})^{-1}$$

$$a^{-1}a(a^{-1}(a^{-1})^{-1}) = a^{-1}ae = a^{-1}a$$

Ora dimostramo che $a = ea$

$$ae = a(a^{-1}a) = (aa^{-1})a = ea$$

Proprietà: (1.1.c)
L'elemento Idenitità è unico.

Poniamo per assurdo esistano due elementi identità e_1 e e_2. $e_2e_1 = e_2$ in quanto e_1 è elemento identità. Allo stesso modo $e_2e_1 = e_1$ in quanto e_2 è elemento identità. Ricaviamo $e_1 = e_2$

Proprietà: (1.1.d)
L'inverso a^{-1} è unico.

Supponiamo esistano due inversi a_1^{-1}, a_2^{-1} di $a \in G$. Dunque $aa_1^{-1} = e = aa_2^{-1} \implies aa_1^{-1} = aa_2^{-1}$. Per la legge di cancellazione (1.1.a) abbiamo $aa_1^{-1} = aa_2^{-1} \implies a_1^{-1} = a_2^{-1}$.

Proprietà: (1.1.e)
$(a^{-1})^{-1} = a$.

$a^{-1}(a^{-1})^{-1} = e = aa^{-1} = a^{-1}a$ e per la legge di cancellazione abbiamo $a^{-1}(a^{-1})^{-1} = a^{-1}a \implies (a^{-1})^{-1} = a$.

Proprietà: (1.1.f)
a^{-n} può essere visto in due modi. (i)$a^{-1} * ... * a^{-1}$ ovvero l'inverso di a alla n. (ii)$(a * ... * a)^{-1}$ ovvero l'inverso di a^n.

Per la proprietà Sock-Shoes basta distribuire l'inverso e otterremo la stessa cosa. Ne possiamo dare una dimostrazione usando le proprietà viste precedentemente:

$$(ab)^{-1} = (b^{-1}a^{-1}) \text{ è equivalente a } (ab)(b^{-1}a^{-1}) = e$$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

Proprietà: (1.1.g)
$e^{-1} = e$.

$e^{-1}e = e$ siccome e^{-1} è l'inverso di e, e tutta via è l'elemento identità dunque $e^{-1}e = e^{-1}$, perciò $e^{-1} = e$.

Esempio: (1.2)
$(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$ sono gruppi abeliani con l'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 un spazio vettoriale. Allora, $(V, +)$ è un gruppo abeliano con un elemento identità $0 \in V$. L'inverso di $v \in V$ è $-v$.

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}.

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 tra 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 di matrici Unimodulari di tipo $n \times n$ è un gruppo rispetto alla moltiplicazione tra matrici. L'elementi identità è la matrice identità $n \times n$. L'inverso di A e 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 delle matrici diagonali in $GL_n(K)$ per $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ è un gruppo rispetto alla moltiplicazione tra matrici.

Esempio: (1.8)
Sia S un insieme. Allora, l'insieme G di tutte le bigezioni $f : S \to S$ è un gruppo rispetto alla composizione $(f \circ g)(s) = f(g(s))$. 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 S_n e chiamato il gruppo simmetrico (o di permutazioni) su n lettere.

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 chiuso rispetto alla moltiplicazione perchè

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

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 base.

Esempio: (1.12)
Sia M l'insieme di tutte le matrici 2×2. Allora M è chiuso rispetto alla moltiplicazione di matrici e contiene la matrice identità. Inoltre la moltiplicazione di matrici è associativa. Tuttavia M non è un gruppo perchè non è detto che M sia non singolare.

Esempio: (1.13)
Il gruppo circolare $S^1 = \{z \in \mathbb{C} \text{ t.c. } |z| = 1\}$ è il gruppo moltiplicativo dei numeri complessi di norma 1. Possiamo pensare a S^1 come al gruppo degli angoli. Infatti ofni numero di norma 1 si può scrivere come $e^{i\pi\theta}$ con $\theta \in \mathbb{R}$. La moltiplicazione $e^{i\pi\theta}e^{i\pi\theta'} = e^{i\pi(\theta+\theta')}$ è data quindi dalla somma degli angoli. Ricordiamo che due numeri $\theta, \theta' \in \mathbb{R}$ identificano lo stesso angolo se $\theta - \theta' = 2kn$ con $k \in \mathbb{Z}$.

Esempio: (1.14)
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 di convoluzione.

$$(f * g)(t) = \int_{-\infty}^{+\infty} f(s)g(t-\tau)d\tau$$

definisce un operazione binaria su S che è associativa per il teorema di Fubini. Tramite un cambio di variabile $r = \tau - t$ si nota che $(f * g)(t) = (g * f)(t)$. Ricordiamo che la delta di dirac è l'elemento identità per il prodotto di convoluzione.

$$(g * \delta)(t) = \int_{-\infty}^{+\infty} f(s)\delta(t-\tau)d\tau = fs$$

Ma δ non è liscia dunque $\delta \notin S$, ricaviamo che $(S, *)$ non è un gruppo.

Esempio: (1.15)
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 classiche.

$*$	C	F	S
C	C	F	C
F	F	F	S
S	C	S	S

Questa tabella descrive interamente come l'operazione binaria interagisce con l' insieme T. In questo caso si nota che l'operazione è commutativa su T (in quanto la tabella è simmetrica). $*$ non è tuttavia associativa, dunque $(T, *)$ non è un gruppo.

9.2 Sottogruppi

Un sottogruppo è l'analogo di un sottospazio.

Definizione: (2.1)
Un Sottoinsieme H di un gruppo G è un sottogruppo se solo se.

- H contiene l'elemento identità in 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 $(V, +)$ poichè contiene sempre l'elemento identità $0 \in U$, è chiuso rispetto a + e contiene l'inverso $-u$ di ognielemento $u \in U$. In contrasto se $b \in V - U$. Allora il traslato

$$b + U = \{b + u \text{ t.c. } u \in U\}$$

non è un sottospazio perchè non contiene lo 0 in quanto se supponessimo per assurdo il contrario avremmo:
$$u \in U, \quad b + u = 0 \implies b = -u \implies b \in U$$
Il che è assurdo siccome $b \in V - U$.

Esempio: (2.4))
Sia n un intero positivo allora
$$n\mathbb{Z} = \{nx \text{ t.c. } x \in \mathbb{Z}\}$$
è un sottogruppo di $(\mathbb{Z}, +)$.

Esempio: (2.5)
Se G è un gruppo e $g \in G$, allora
$$\langle g \rangle = \{g^n \text{ t.c. } n \in \mathbb{Z}\}$$
è un sottogruppo di G.

Esempio: (2.6)
Le matrici unimodulari (1.6) e le matrici diagonali (1.7) sono sottogruppi del gruppo di matrici $GL_n(K)$(1.5). Il sottoinsieme $SL_n(K)$ di $GL_n(K)$ costituito dalle matrici di determinante 1 è un sottogruppo di $SL_n(\mathbb{Z})$ di matrici $n \times n$ con determinante 1 con elementi interi è un sottogruppo del gruppo di matrici unimodulari.

Lemma: (2.7)
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:
Poichè 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. Poichè H è chiuso rispetto al prodotto e inversi $a, b \in H \implies ab^{-1} \in H$.

Lemma: (2.8)
Sia H un sottogruppo di $(G, *)$. Allora H è un gruppo rispetto alla restrizione di $*$ ad H.

Dimostrazione:
Da fare:

Lemma: (2.9)
Siano H e K sottogruppi di G. Allora $H \cap K$ è un sottogruppo di G.

Lemma: (2.10)
L'unione di due sottogruppi H e K di G è un sottogruppo se e solo se $H \subseteq K$ o $K \subseteq H$.

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 $H \cap K$ è H o K, che è un sottogruppo.
- $P \implies Q$: Consideriamo il contrapposto $\neg Q \implies \neg P$.. 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 $H \cup K$ sia un sottogruppo. Allora, $hk \in H \cup K$ e quindi $hk \in H$ o $hk \in K$. Se $hk \in K$ allora $k = h^{-1}hk \in H$ che è una contraddizione. Similmente, se $hk \in H$ allora $h = hkk^{-1} \in K$, che è di nuovo una contraddizione. Quindi $(\neg Q) \implies (\neg P)$.

9.2.1 Gruppi Ciclici

Sia S un sottoinsieme di uno spazio vettoriale V. Allora per definizione, $span(S)$ è l'intersezione di tutti i sottospazi U di V tale che $S \subseteq U$. La stessa definizione funzoina per sottoinsiemi di un gruppo

G.

Definizione: (2.11)
Sia S un sottoinsieme di un gruppo G. Allora il sottogruppo $\langle S\rangle$ è generato da S è l'intersezione di tutti i sottogruppi H di G che contengono S.

Alternativamente, in analogia con gli spazi vettoriali, possiamo definire $\langle S\rangle$ in termini di combinazioni finite.

Lemma: (2.12)
$\langle S'\rangle$ consiste di tutti i prodotti finiti di elementi $s_1 \cdots s_r$ 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, perciò $e \in H$. 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

$$a = s_1 \cdots s_r \in H \implies a^{-1} = s_r^{-1} \cdots s_1^{-1} \in H$$

quindi H è un sottogruppo di G che contiene S, e quindi per definizione $\langle S\rangle \subseteq H$. Viceversa, $H \subseteq S$ perchè ogni sottogruppo K di G che contiene S deve contenere tutti i prodotti finiti di elementi di S e inversi.

Esempio: (2.13)
In $\mathbb{Z}$ abbiamo $\langle 2\rangle = 2\mathbb{Z}$ ma $\rangle 2, 3\rangle = \langle 1\rangle = \mathbb{Z}$ poichè $1 = 3 - 2$.

Esempio: (2.14)
Il gruppo $SL_2(\mathbb{Z}) = \langle A, B\rangle$ dove

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Definizione:(2.15)
Un gruppo si dice 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 $\langle g\rangle$.

9.2.2 Ordine del gruppo e di un elemento

Definizione: (2.17)
Sia G un gruppo. Se G è finito allora $ord(G) = |G|$. Altrimenti, $ord(G) = \infty$. Se $g \in G$ allora $ord(g) = ord(\langle g\rangle)$.

Lemma: (2.18)
Sia g un elemento di ordine finito. Allora $ord(g) = min\{k \in \mathbb{N} \text{ t.c. } g^k = e_g\}$.

Dimostrazione:
Sia $a = min\{k \in \mathbb{N}\ \{0\} \text{ t.c. } g^k = e_g\}$. Quindi $g^a = e_G$ e $g^b \neq e_G$ per ogni $1 \leq b < a$. Vogliamo dimostrare che

$$\langle g\rangle = \{g^0 = e_G, g^2, ..., g^{a-1}\}$$

(Senza ripetizioni). Infatti, se $g^b = g^{b'}$ con entrambi $b < b'$ entrambi più piccoli di a allora $g^{b-b'} = e_G$, ma $b - b' < a$ contro l'ipotesi di minimalità di a. D'altra parte, ogni elemento in $\langle g\rangle$ può essere scritto come g^k con $k \in \mathbb{Z}$ e facendo la divisione con resto otteniamo $k = qa + r$, con $r < a$, quindi in $g^k = (g^a)^q g^r = g^r$.Con questo tipo di costruzione otteniamo $ord(g) = |\langle g\rangle| = |\{e_G, ..., g^{a-1}\}| = a$.

Esempio: (2.19)

Facciamo la tabella di Cayley per il gruppo di unità in $\mathbb{Z}_5$.

$*$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Table 1: Cayley Table of $(U(5), *)$

allora, $ord([1]) = 1$, $ord([2]) = 4$, $ord([3]) = 4$, $ord([4]) = 2$.

Ora facciamo un'osservazione fondamentale: sia G un gruppo e H un sottoinsieme finito non vuoto di G che è chiuso rispetto al prodotto. Allora anche l'insieme.

$$\{h, h^2, h^3, ...\} \subseteq H$$

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 $h^r = h^r hs - r$ il che implica che $h^{s-r} = e$. Se $s - r = 1$ ciò mostra che $h = e$. Altrimenti, $s - r > 1$ allora, hh^{s-r-1} e quindi h contiene anche h^{-1}. Insomma abbiamo dimostrato:

Lemma: (2.20)
Sia H un sottoinsieme 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 deove G non è abeliano.

Esempio: (2.22)
Sia G un gruppo e $x \in G$. Allora $C(x) = \{g \in G$ t.c. $gx = xg$ è un sottogruppo di G chiamato il centralizzante di x.

- $ex = xe \implies e \in C(x)$
- $ax = xa$ e $bx = xb \implies abxabx = axb = xab \implies ab \in C(x)$
- $ax = xa \implies a^{-1}ax = a^{-1}xa \implies x = a^{-1}xa$
  $\implies xa^{-1} = a^{-1}xaa^{-1} \implies xa^{-1} = a^{-1}x \implies a^{-1} \in C(x)$

Esempio: (2.23)
Sia $G = SL_2(\mathbb{R})$ e

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Allora, $C(X) = \{A \in SL_2(\mathbb{R})$ t.c. $AX = XA\}$.

9.3 Gruppi Prodotto

Un'altra costruzione base dell'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 i gruppi.

Proposizione:(3.1)
Siano H e K gruppi. Allora $H \times K$ è un gruppo rispetto all'operazione binaria.

$$(h_1, k_1) * (h_2, k_2) = (h_1h_2, k_1k_2)$$

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.

Per continuare, ricordiamo che un isomorfismo di spazi vettoriali è una bigezione tra due spazi vettoriali U e V.

Definizione: (3.2)
Siano G e H gruppi. Allora $f : G \to H$ è un isomorfismo se e solo se

- f è biettiva
- $f(g_1g_2) = f(g_1)f(g_2)$ 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 $G \cong H$.

Nota: (3.3) L'isomorfismo è una relazione di equivalenza sui gruppi. In particolare è transitiva cioè se G è isomorfo a H e H è isomorfo a L allora G è isomorfo a L(e l'isomorfismo $G \to L$ è dato dalla composizione degli isomorfismi $G \to H$ e $H \to L$.

Esempio: (3.4)
L'insieme $(0, \infty)$ è un gruppo rispetto alla moltiplicazione. La mappa esponenziale $exp : \mathbb{R} \to (0, \infty)$ è un isomorfismo perchè è biettiva(con inversa log) e

$$exp(a + b) = exp(a)exp(b)$$

Si nota che l'operazione del gruppo $(0, \infty)$ è $*$ mentre in $\mathbb{R}$ è $+$.

Esempio: (3.5)
Sia $U(l)$ il gruppo di unità in $\mathbb{Z}_l$ rispetto alla moltiplicazione. Nella lezione 7 abbiamo visto che se m e n sono interi positivi e $mcd(m, n) = 1$ allora

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad f([x]_{mn}) = ([x]_m, [x]_n)$$

è una bigezione che rispetta l'addizione. Quindi f è un isomorfismo tra i gruppi $(\mathbb{Z}_{mn}, +) \to (\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$.Inoltre f rispetta anche la moltiplicazione e si restringe a una bigezione da $U(mn)$ a $U(m) \times U(n)$. Quindi f è un isomorfismo da $U(mn)$ a $U(m) \times U(n)$.

Il prossimo risultato è una forma del teorema cinese del resto:

Proposizione: (3.6)
Siano $n_1, ..., n_k$ interi maggiori di 1 coprimi tra loro. Allora

$$\mathbb{Z}_{n_1 \cdots n_k} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

Dimostrazione:
Poichè $n_1, ..., n_k$ sono primi l'uno con l'altro, non hanno fattori primi in comune. Allora $mcd(n_1, ..., n_j, n_{j+1}, ..., nk) = 1$ e quindi

$$\mathbb{Z}_{n_1 \cdots n_k} \cong \mathbb{Z}_{n_1} \times (\mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}) \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

Esempio: (3.7)
Siccome $mcd(9, 4) = 1$ allora $\mathbb{Z}_{36} = \mathbb{Z}_4 \times \mathbb{Z}_6$.

Se U e V sono spazi vettoriali di dimensione finita, allora U e V 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: (3.8| Th. del Fattore Invariante di Gauss)
Sia G un gruppo abeliano non triviale finito. Allora c'è un unco insieme di divisori $d_1, ..., d_r$ di $|G|$ tali che

- $|G| = d_1 \cdots d_r$ dove ogni $d_j > 1$.

- $G = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$
- $d_r \mid d_{r-1}, ..., d_2 \mid d_1$

La lista $(d_1, ..., d_r)$ 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.

Nota: (3.9) 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 consiste nel trovare la fattorizzazione prima di n per poi raggruppare questi fattori primi a due a due di moso che rispetti la terza condizione $(d_j \mid d_{j-1})$.

Esempio: (3.10)
Siano p e q due (distinti) numeri primi.

- Se $n = p^2q^2$ allora i possibili fattori invarianti di un gruppo abeliano di ordine n sono:

$$(ppqq), \quad (pqq, p), \quad (ppq, q), \quad (pq, pq)$$

- Se $n = p^2q^3$ allora i possibili fattori invarianti di un gruppo abeliano di ordine n sono:

$$(ppqqq), \quad (pqqq, p), \quad (ppqq, q), \quad (ppq, q, q), \quad (pq, pq, q)$$

Esempio: (3.11)

- $n = 36 = 2^2 3^2$. Per l'esempio precedente, i fattori invarianti sono $(36), (18, 2), (12, 3), (6, 6)$.
- $n = 24 = 2^3 3$. I possibili fattori invarianti sono $(24), (12, 2), (6, 2, 2)$.

Esempio: (3.12)
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: (3.13)
Sia un $n > 1$ un intero libero di quadrati. Allora c'è esattamente un gruppo abeliano di ordine n.

Dimostrazione:
Come nell'esempio precedente con il gruppo di ordine 30, poichè n è libero di quadrati, ogni fattori primo di n appare con la potenza 1, e quindi (n) è l'unico possibile fattore invariante.

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 equivalente se sono uguali a meno di riordinamento.

Esempio: (3.14)
A meno di riordinamento le possibili partizioni di 4 sono

$$4, \quad 3+1, \quad 2+1+1, \quad 1+1+1+1$$

Se l è un intero positivo, sia $\pi(l)$ il numero di partizioni equivalenti di l. Una conseguenza della dimostrazione del teorema del fattore invariante è:

Teorema: (3.15)

Sia $n > 1$ un intero con fattorizzazione prima $n = p_1^{k_1} \cdots p_r^{k_r}$. Allora, il numero di gruppi abeliano di ordine n è $\pi(k_1) \cdots \pi(k_r)$.

Esempio: (3.16)
Se p è un numero primo allora ci sono $\pi(n)$ sotto gruppi di ordine $\pi(n)$ per vedere ciò cominciamo con

$$p^n = (p \cdots p)$$

e inseriamo virgole cominciando da destra verso sinistra in modo tale che ogni blocco contiene almento 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 $a_1 \geq a_2 \geq \cdots \geq a_k$.

I gruppi che si trovano aventi stesso ordine non è detto siano isomorfi, per verificare che sono isomorfi occorre controllare che l'ordine dei singoli elementi sono gli stessi. Ad esempio per vedere se un gruppo G avente ordine 16 è isomorfo ad uno tra $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e infine $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}$. Si può controllare gli ordine degli elementi in questi gruppi e confrontarli. Ad esempio $|U(60)| = 16$ non può essere isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. L'ordine di in elemento $g \in \mathbb{Z}_n$ risulta essere in particolare $n/mcd(g, n)$, Dunque per $\mathbb{Z}_{16}$ abbiamo che tutti i coprmi con 16 hanno ordine 16. Tutti i multupli di 2 dove 2 compare una volta sola $\{2, 6, 10, 14\}$ hanno ordine 8, tutti i multipli di 2 dove 2 compare due volte $\{4, 12\}$ hanno ordine 4, infine $\{8\}$ ha ordine 2 e $16 = 0 = e$ ha ordine 1. $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ Usiamo ancora il teorema di Lagrange e diciamo che ogni elemento di $\mathbb{Z}_4$ deve avere ordine $1, 2, 4$. $1, 3$ hanno ordine 4, 2 ha ordine 2 e 0 ha ovviamente ordine 1. Per $\mathbb{Z}_2$ si ha o ordine 1 o ordine 2. Si calcola l'ordine dell'elemento (a, b, c) facendo il minimo comune multiplo degli ordini.Abbiamo dunque 8 elementi di ordine 4, 1 elemento di ordine 1, e 7 elementi di ordine 2. Per $\mathbb{Z}_8$ abbiamo 4 elementi di ordine 8, 2 elementi di ordine 2, e 1 elemento di ordine 1. Risultano 8 di ordine 8, 7 di ordine 2, e 1 di ordine 1 per $\mathbb{Z}_8 \times \mathbb{Z}_2$. Per $\mathbb{Z}_4 \times \mathbb{Z}_4$ risultano 4 elementi di ordine 2, 1 di ordine 1 e 10 di ordine 4.
11 ha ordine 2 in $U(60)$, 31 ha ordine 2, 59 ha ordine 2,dunque $U(16)$ è per forza isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

9.4 Esponente di un gruppo abeliano

In questa sezione esploreremo alcune connessioni tra la teoria dei gruppi e la crittografia.

Definizione: (4.1)
Si dice 'esponente' di un gruppo abeliano G il massimo ordine dei suoi elementi.

Dal teorema di Lagrange sappiamo che se G è finito, gli ordini di tutti gli elementi di G dividono $|G|$. Vale anche un risultato più forte.

Lemma: (4.2)
Sia G un gruppo abeliano e $g, h \in G$ con ordini coprimi. Allora $ord(g) = ord(g)ord(h)$.

Dimostrazione:
Sia $a = ord(g)$ e $b = ord(h)$. Sia $d = ord(gh)$. Allora $(gh)^{ab} = g^{ab}h^{ab} = e$, e quindi $d \mid ab$. Allora abbiamo

$$e = (gh)^{ad} = g^{ad}h^{ad} = h^{ad}$$

e quindi $b \mid ad$, ma poichè $mcd(a, b) = 1$ otteniamo per il lemma di euclide che $b \mid d$. Con un ragionamento simmetrico otteniamo anche $a \mid d$, e quindi $ab \mid d$. Concludiamo che $d = ab$.

Proposizione: (4.3)
Sia λ l'esponente di un gruppo abeliano G. Se λ è finito, allora l'ordine di ogni elemento divide di G divide λ.

Dimostrazione:
Esiste un $h \in H$ con ordine massimo, cioè tale che $ord(h) = \lambda$. Sia $g \in G$ e supponiamo che $ord(g) = a$. Chiamiamo $g' = g^{mcd(a,\lambda)}$. Ricordiamo che $a' = a/mcd(a,\lambda)$ è coprimo con λ è coprimo con λ, e che $ord(g') = a'$. Per il lemma (4.2) abbiamo $ord(g'h) = ord(g')ord(h) = a'\lambda$. Per ipotesi λ è l'ordine massimo quindi $a' = 1$, cioè $mcd(a,\lambda) = a \implies a \mid \lambda$.

Esempio: (4.4)
Sia $U(15)$ il gruppo delle unità in $\mathbb{Z}_{15}$. Abbiamo $|U(15)| = \phi(15) = 8$. Controllando tutti gli elementi in $U(15)$ possiamo invece verificare che l'esponenete di $U(15)$ è 4.

Possiamo adesso enunciare un risultato importante.

Teorema: (4.5)
Se p è primo, allora il gruppo $U(p)$ delle unità in $\mathbb{Z}_p$ è ciclico.

Posticipiamo la dimostrazione: questa sarà facile una volta che avremmo visto che $\mathbb{Z}_p$ è in realtà un campo e la stessa dimostrazione vale per tutti i campi finiti. Questo segue dal seguente criterio.

Proposizione: (4.6)
Un gruppo abeliano finito G è ciclico se e solo se, per ogni intero r, l'equazione $x^r = e$ ha al più r soluzioni in G.

Dimostrazione:
Sia $n = |G|$ e sia λ l'esponente di G. Se G non è ciclico, allora non ha elementi di ordine n, quindi $\lambda < n$. Dalla proposizione (4.3) otteniamo $x^\lambda = e$ per ogni $x \in G$ quindi l'equazione ha n soluzioni. Se G è ciclico, allora esiste g di ordine n e ogni $h \in G$ può essere scritto come $h = g^m$. Allora le soluzioni dell'equazione $x^r = e$ sono g^m tali che $n \mid mr$. Sia $d = mcd(n, r)$. Allora n/d deve dividere m, quindi ci sono d possibili soluzioni. Notiamo che $d \leq r$.

9.5 Teorema di Lagrange e Cosets

Sia H un sottogruppo di G. Sia $\sim$ la relazione su G definita da

$$a \sim b \iff a^{-1}b \in H$$

Per il prossimo risultato che, come la moltiplicazione di matrici, se G è un gruppo allora $(xy)^{-1} = y^{-1}x^{-1}$ e $(x^{-1})^{-1}$.

Lemma: (5.1)
La relazione descritta è di equivalenza.

Dimostrazione:

- Riflessività: $a \sim a \iff a^{-1}a = e \in H$
- Simmetria: $a \sim b \iff a^{-1}b \in H$. Quindi, $a^{-1}b \in H \implies (a^{-1}b)^{-1} \in H \implies b^{-1}(a^{-1})^{-1} \in H \implies b^{-1}a \in H \implies b \sim a$.
- Transitività: $a \sim b \iff a^{-1}b \in H$ e $b \sim c \iff b^{-1}c \in H$. Allora $(a^{-1}b)(b^{-1}c) \in H \implies a^{-1}(bb^{-1})c \in H \implies a^{-1}c \in H \implies a \sim c$

Esempio: (5.2)
Sia U 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. Per adesso non abbiamo altre struttura sulle classi di equivalenza di un gruppo, anche se già sappiamo che c'è 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: (5.3)
Sia n un intero. Allora $n\mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}_n, +)$ e $a \sim b \iff a - b \in n\mathbb{Z}$. In altre parole, $a \sim b$ se e solo se $(a - b) \mid n$ oppure $a \equiv b \bmod n$. Al momento, questa è solo una costruzione di insiemi, quindi non sappiamo che $\mathbb{Z}/n\mathbb{Z}$ ha addizione e moltiplicazione modulo n.

Esempio: (5.4)
$\mathbb{Z}$ 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 estemi di $[0, 1]$ vengono identificati via $\sim$. Quindi $\mathbb{R}/\mathbb{Z}$ è un 'loop' o cerchio. Per ottenere una mappa da $\mathbb{R}/\mathbb{Z}$, sia

$$f(x) = e^{2\pi i x} = cos(2\pi x) + isin(2\pi x)$$

allora, $f(x) = f(y) \iff x - y \in \mathbb{Z}$ dove l'immagine di f è il cerchio unitario nel piano complesso.

Definizione: (5.5)
Sia H un sottogruppo di G e $a \in G$. Allora

$$aH = \{ah \text{ t.c. } h \in H\}$$

è chiamato il coset (o classe laterale) sinistra di a.

Proposizione: (5.6)
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 $a^{-1}b \in H \implies a \sim b$

Definizione: (5.7)
Sia H un sottogruppo di G. Allora, l'indice $[G : H]$è la cardinalità di G/H.

Esempio: (5.8)
Se $G = (\mathbb{Z}, +)$ e $H = n\mathbb{Z}$ allora $[G : H] = n$ se $G = (\mathbb{R}+ : H)$ è infinito.

Teorema: (5.9| Lagrange)
Sia H un sottogruppo di un gruppo finito G. Allora

$$|G| = [G : H]|H|$$

Dimostrazione Per la proposizione (5.6), ogni classe di equivalenza $[a] = aH$ ha cardinalità $|H| \leq |G| < \infty$. Poichè $\sim$ è una relazione di equivalenza, G è un unione disgiunta di classi di equivalenza. Allora $|G| = [G : H]|H|$ perchè ci sono $[G : H]$ cosets.

Corollario: (5.10)
Sia g un elemento di un gruppo finito G. Allora $ord(g)$ divide $ord(G) = |G|$.

Dimostrazione: $ord(g) = |\langle g \rangle|$ e $H = \langle g \rangle$ è un sottogruppo di G. Quindi

$$|G| = [G : H]|H| \implies ord(g) \mid ord(G)$$

Nota: (5.11) 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, per definizione, un gruppo finito G ha elemento di ordine $|G|$ se e solo se G è ciclico.

Esempio: (5.12)
Sia $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Allora

$$ord(0, 0) = 1, \quad ord((1, 0)) = ord((0, 1)) = ord((1, 1)) = 2$$

In particolare G non ha alcun elemento di ordine 4.

Corollario: (5.13)
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 o $ord(g) = 1$ o $ord(g) = p$. Poichè $g \neq e, ord(g) \neq 1$, 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.

Corollario: (5.14 | Piccolo Teorema di Fermat)
Se p è primo allora $\mathbb{Z}_p - \{0\}$ 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 $a^{p-1} \equiv [1] \bmod p$. Moltiplicando per a, otteniamo $a^p - a \equiv 0 \bmod p$.

Corollario: (5.15 | Teorema di Eulero)
Denotiamo con $U(n)$ il gruppo di unità in $\mathbb{Z}_n$ rispetto alla moltiplicazione. Allora $ord(U(n)) = \phi(n)$. Se $mcd(a, n) = 1$ allora $[a] \in U(n)$ e quindi $[a]^{\phi(n)} = [1]$.

9.5.1 Classi di Coiniugio

Continuando, ricordiamo che una coppia di matrici A e B di tipo $n \times n$ sono simili se e solo se esiste una matrice invertbibile C di tipo $n \times n$ tale che $A = CBC^{-1}$. Più generalemente, 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: (5.16)
$\simeq$ è una relazione di equivalenza.

Dimostrazione:

- Riflessività: $x = exe^{-1} \implies x \simeq x$
- Simmetria: $x \simeq y \implies x = gyg^{-1} \implies y = g^{-1}xg = g^{-1}x(g^{-1})^{-1} \implies y \simeq x$
- Transitività: $x \simeq y \implies x = gyg^{-1}$ e $y \simeq z \implies y = hzh^{-1}$ dunque $x = ghzh^{-1}g^{-1} \implies x = (gh)z(gh)^{-1} \implies x \simeq z$

Denotiamo con $Cl(x)$ la classe di equivalenza $x \in G$ via $\simeq$. Questa è chiamata di solito la classe di coniugio di x.

Esempio: (5.17)
Sia G il gruppo di matrici unitarie di ordine n. Allora per il teorema spettrale, ogni elemento di $A \in G$ è unitariamente simile a una matrice diagonale. In altre parole, c'è una matrice unitaria U tale che $U = UAU^{-1} = D$. Quindi ogni classe di coniugio $Cl(A)$ ha un unica rappresentante, D che è diagonale.

Esempio: (5.18)
Sia G un gruppo, e supponiamo che $x \in G$ e $|Cl(x)| = 1$ allora, $gxg^{-1} = x$ per ogni elemento $g \in G$. In altre parole x commuta con ogni elemento di G. L'insieme

$$Z(G) = \{x \in G \text{ t.c. } gx = xg \quad \forall g \in G\}$$

è chiamato il centro di G. $Z(G)$ è inoltre sottogruppo di G.

In particolare, poichè $\simeq$ è una relazione di equivalenza, quando G è finito, esiste una collezione finita di elementi $x_1, ..., x_n \in G$ tale che

$$G = Cl(x_1) \cup Cl(x_2) \cup \cdots Cl(x_n)$$

dove $Cl(x_i) \cap Cl(x_j) = \emptyset$ se $i \neq j$. In luce dell' esempio precedente possiamo riscrvere l'equazione precedente come

$$G = Z(G) \cup \left(\bigcup_{|Cl(x_j)|>1} Cl(x_j) \right)$$

Per calcolare la cardinalità di $Cl(x)$ quando $x \notin Z(G)$ notiamo che abbiamo una mappa suriettiva.

$$f : G \to Cl(x), \quad f(g) = gxg^{-1}$$

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. Quindi f determina una mappa biettiva.

$$F : G/C(x) \to Cl(x), \quad F(gC(x)9 = gxg^{-1}$$

e quindi se g è finito abbiamo:

$$|Cl(x)| = |G/C(x)| = [G : C(x)]$$

in particolare, per il teorema di lagrange, $|Cl(x)|$ è un divisore di $|G|$.

Teorema: (1.22 | Formula delle classi di Coniugio)
Sia G un gruppo finito allora

$$|G| = |Z(G)| + \sum_{|Cl(x_j)|>1} [G : C(x_j)]$$

Un applicazione di base della formula delle classi è dimostrare che il numero di classi di coniugio limita l'ordine del gruppo. Siccome le classi di couniugio formano una partizione scriviamo

$$|G| = \sum_{i=1}^{n} |Cl(x_i)|$$

Dividendo per $|G|$ e usando il teorema di lagrange otteniamo:

$$1 = \sum_{i=1}^{n} \frac{1}{|C(x_j)|}$$

Inoltre $C(e) = G$, quindi $1/|G|$ appare come la più piccola frazione nella sommatoria. Supponiamo adesso si sapere solo che G è un gruppo che ha $n > 1$ classi di coniugio. Allora, posso considerare tutte le possibili soluzioni dell'equazione

$$1 = \sum_{i=1}^{n} \frac{1}{a_i}$$

dove ciascun $a_i > 1$ è un intero. Per un fissato valore di n, c'è solo un numero finito di soluzioni. e il valore più grande di a_j che appare è un limite dull'ordine di G.

Esempio: (5.24)
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: (5.25)

Il più piccolo gruppo non abeliano è S_3, che ha 6 elementi, ed è isomorfo al gruppo di matrici dell'esercizio 1. In questo caso, un calcolo diretto moostra che $Cl(T_1) = \{T_1, T_2, T_3\}$. Similmente $Cl(I) = \{I\}$. Allora per l'equazione delle classi abbiamo

$$6 = 1 + 3 + |Cl(x_1)| + \cdots$$

Le rimanenti possibilità sono $Cl(R_1) = \{R_1, R_2\}$ o $Cl(R_j) = \{R_j\}$. Nel secondo caso $R_j \in Z(G)$ che è falso.

Proposizione: (5.26)
Sia p 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 $|Cl(g)| \neq 1$ ed è un divisore di $|G|$. Quindi $|Cl(g)| = p^j$ per qualche $j > 0$. Poichè g era un elemento arbitrario di $G - Z(G)$, dalla formula delle classi segue che

$$p^r = |G| = |Z(G)| + |Cl(g_1)| + \cdots + |Cl(g_r)| = 1 + pk$$

per qualche intero k poichè ciascun $|Cl(g_i)| > 1$ è una potenza di p. Ma, in questo modo abbiamo

$$p^r = 1 + kp = kp = p^r - 1 = (p-1)(1 + p + \cdots + p^{r-1})$$

e quindi

$$k \mid kp \implies p \mid (p-1)(1 + p + \cdots + p^{r-1}) \implies p \mid p - 1 \vee p \mid 1 + p + \cdots \cdot p^{r-1} \implies p \mid \pm 1$$

che è una contraddizione. E allora, $|Z(G)| \neq 1$.

9.6 Omomorfismi di Gruppi

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: (6.1)
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 di isomorfismo tra gruppi, vediamo che l'isomorfismo è appunto un omomomorfismo biettivo.

Esempio: (6.2)
Sia $L : U \to V$ una mappa lineare tra spazi vettoriali. Allora, L è anche un omomorfismo tra gruppi da $(U, +)$ a $(V, +)$.

Esempio: (6.3)
Se S è un sottogruppo di G, allora la mappa inclusione $i : S \to G, \quad i(s) = s$ è un omomorfismo di gruppi.

Esempio: (6.4)
Sia $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Allora $K^* = GL_1(K)$ è il gruppo moltiplicativo degli elementi non nulli di K. Per la formula di binet cauchy, $det : GL_n(K) \to K^*$ è un omomorfismo di gruppi.

Esempio: (6.5)
Sia S_n il gruppo di permutazioni $\{1, ..., n\}$ e $\{e_1, ..., e_j\}$ la base standard di $\mathbb{R}^n$. Dato $\sigma \in S_n$ sia L_σ : $\mathbb{R}_n \to \mathbb{R}_n$ la mappa lineare definita da

$$L_{\sigma(e_j)} = e_{\sigma(i)}$$

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 alla base standard è un omomorfismo di gruppi.

Proposizione: (6.6)
Se $f : G \to H$ è un omomorfismo di gruppi allora $f(e_G) = e_H$ e $f(g^{-1}) = f(g)^{-1}$.

Dimostrazione:

$$e_G = e_G e_G \implies f(e_G) = f(e_G)f(e_G) \implies f(e_G)^{-1}f(e_G) = f(e_G)f(e_G)f(e_G)^{-1} \implies e_H = f(e_G)$$

$$g^{-1}g = e_G \implies f(g^{-1})f(g) = e_H \implies f(g_1^{-1})f(g)f(g)^{-1} = e_H f(g)^{-1} \implies f(g^{-1})e_H = f(g)^{-1} \implies f(g^{-1}) = f(g)^{-1}$$

Se $L : U \to V$ è una mappa lineare allora $ker(L)$ è un sottspazio di U e $Im(L)$ è un sottospazio di V. Lo stesso è vero per gli omomorfismi tra gruppi.

Proposizione: (6.7)
Sia $f : G \to H$ un isomorfismo tra gruppi. Allora, $ker(f) = f^{-1}(e_H)$ è un sottogruppo di G e $Im(f)$ è un sottogruppi di H.

Dimostrazione: Per il lemma (2.7) dobbiamo mostrare che $ker(f)$ e $Im(f)$ sono non vuoti e chiusi per l'operazione $a, b \mapsto a^{-1}b$.

- $ker(f)$ è un sottogruppo di G poichè $e_G \in ker(f)$ e

$$a, b \in ker(f) \implies f(a^{-1}b) = f(a^{-1})f(b) = f(a)^{-1}f(b) = e_H e_H = e_H \implies a^{-1}b \in ker(f)$$

- $Im(f)$ è un sottogruppo di H poichè $e_H = f(e_G) \in H$ e

$$a = f(\alpha), b = f(\beta) \in Im(f) \implies a^{-1}b = f(\alpha)^{-1}f(\beta) = f(\alpha^{-1})f(\beta) = f(\alpha^{-1}\beta) \implies a^{-1}b \in Im(f)$$

Esempio: (6.5)
Il kernel di $det : GL_n(K) \to K^*$ sono le matrici con $det = 1$. L'immagine di det è K^*: Considera la matrice $A = (a_i j)$ tali che $a_{11} = \alpha$, $a_{jj} = 1$ per $j > 1$ e $a_{ij} = 0$ con $i \neq j$. Allora $det(A) = \alpha$.

Esempio: (6.6)
Sia $f : S_n \to GL_n(\mathbb{R})$ l'omomorfismo definito nell'esempio (2.5). Allora $ker(f)$ è la permutazione identità. L'immagine di f è il gruppo $Perm_n$ delle matrici di permutazioni $n \times n$, cioè le matrici che hanno esattamente un 1 su ogni riga e su ogni colonna. Mentre tutte le altre entrate sono 0. La mappa $f : S_n \to Perm_n$ è un isomorfismo.

Sia $P = f(\sigma)$ una matrice permutazione. Allora,

$$(PP^T)_{ij} = \sum_k P_{ik}(P^T)_{kj} = \sum_k P_{ik}P_{jk}$$

Poichè P è una 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 $det(P) = \pm 1$.

Esempio: (6.7)
L'insieme $\{-1, +1\}$ è un gruppo ristretto a moltiplicazione che è isomorfo al gruppo $\mathbb{Z}_2$ tramite la mappa $\mathbb{Z}_2 \to \{-1, 1\}$ data da $j \mapsto (-1)^j$. La mappa $det : Perm_n \to \{-1, +1\}$ è un omomorfismo, che è solitamente chiamato il segno della permutazione. Il sottogruppo di permutazione nel kernel è chiamato gruppo alternato.

Nella sezione precedente, abbiamo visto che dato un sottogruppo H di G, possiamo formare l'insieme G/H. In molti esempi, tale come spazio vettoriale quoziente V/U e $\mathbb{Z}/n\mathbb{Z}$, G/H ha anche struttura del gruppo.
Se R e S sono sottoinsieme di un gruppo G definiamo

$$RS = \{rs \text{ t.c. } r \in R,\ s \in S\}$$

In particolare, se H è sottogruppo di G allora $HH = H$ poichè H è chiuso per la mappa definita. La regola ovvia per definire una struttura di gruppo su G/H è

$$(aH)(bH) = (ab)H$$

Se G è un gruppo abeliano, allora questa formula funziona per definire un prodotto poichè possiamo semplicemente muovere b dopo H. Quando G non è abeliano questa definizione non funziona sempre.

Definizione: (6.8)
Sia H un sottogruppo di G. Allora, H è un sottogruppo normale se e solo $g^{-1}Hg = H \implies gH = Hg$ per ogni $g \in G$. In questo caso scriviamo $H \triangleleft G$.

Esempio: (6.9)
Sia H un sottogruppo normale di G. Se $[G : H] = 2$ allora H è un sottogruppo normale di G. Ovvero, se $g \in H$ allora $gHg^{-1} \in H$ poichè H è un sottogruppo di G. Supponiamo ora che $g \in G - H$. Allora

$$[G : H] = 2 \implies G = gH \cup H, \quad gH \cap H = \emptyset$$

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 una 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 poichè chiuso per inversi. Allora $gg' = ghg^{-1} \in H$.

Se $H \triangleleft G$ allora

$$(aH)(bH) = a(bHb^{-1})(bH) = (abH)H = abH$$

e definisce un operazione binaria su G/H. Poichè G è un gruppo questa operazione è associativa. Similmente, $eH = H$ è l'identità e $(aH)(a^{-1}H) = H$.

Teorema: (6.10)
Sia H un sottogruppo di G. Allora $(aH)(bH) = (ab)H$ definisce una struttura di gruppo su G/H se e solo se $H \triangleleft G$.

Dimostrazione:
Se H è un sottogruppo normale di G allora G/H ha una struttura di gruppo come dimostrato sopra. Se $(aH)(bH) = (ab)H$ definisce una struttura di gruppo allora $H = aa^{-1}H = (aH)(a^{-1}H) \implies H = aHa^{-1}$.

Lemma: (6.11)
Sia $f : G \to H$ un omomorfismo di gruppi e $K = ker(f)$. Allora K è un sottogruppo normale di G.

Dimostrazione:
Sia $k \in ker(f)$ e $g \in G$. Allora

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)e_H f(g^{-1}) = f(g)f(g)^{-1} = e_H$$

e quindi $gkg^{-1} \in ker(f)$.

Lemma: (6.11)
Sia $f : G \to H$ un omomorfismo di gruppi e $K = ker(f)$. Allora G/K è isomorfo a $Im(f)$.

Dimostrazione:
Sia $g \in G$, e $k \in K$. Allora $f(gk) = f(g)f(k) = f(g)$. Allora

$$F : G/K \to H, \quad F(gK) = f(g)$$

è ben definita, e $im(F) = im(f)$. Inoltre, $F(gK) = F(g'K) \iff f(g) = f(g')$ 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 $Im(f)$. Infine poichè K è un sottogruppo normale di G, abbiamo

$$F((gK)(g'K)) = F(gg'K) = f(gg') = f(g)f(g') = F(gK)F(g'K)$$

e quindi F è un omomorfismo.

Ci sono altri tre teoremi standard di isomorfismo per gruppi, che hanno analoghi per anelli commutativi con identità, quindi discuteremo quei teoremi nella lezioni su anellic ommutativi con identità.

Per chiudere questa sezione, ora presentiamo un passo chiave nella dimostrazione del teorema del fattore invariante per gruppi abeliani finiti.

Proposizione: (6.12)
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 proposizione può essere dimostrata per induzione su q come segue:

- $P(1)$: Questo è vero perchè $|A| = p$ e quindi $|A| = \mathbb{Z}_p$ che è ciclico e di ordine p.
- $P(1)....P(q) \implies P(q+1)$: 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. Dal teorema di lagrange otteniamo che $d \mid q(q+1)$ e quindi $d \mid (q+1$. Sia $C = \langle a \rangle$ e $q' = q + 1/d$. Poichè 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. Poichè f è suriettiva, esiste un elemento $x \in A$ tale che $f(x) = y$. Sia $v > 0$ l'ordine di x, e scriviamo $v = pu + r$ dove $0 < r \leq p$. Allora

  $$e_{A/C} = f(e_A) = f(x^v) = f(x)^v = y^v = y^{pq+r} = y^r$$

  è l'elemento identità di A/C. Dunque $r = 0$ perchè y ha rodine p. Pertanto $p \mid v$ e quindi $x^{v/p} \in A$ è un elemento di ordine p.

Nota: (6.13) Infatti, 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 affermano che se p^n è la massima potenza di p che divide $|G|$, allora G ha un sottogruppo di ordine p^n.

9.7 Azione del Gruppo

Con 'azione' di un gruppo G si intende una rappresentazione di G (mediante omomorfismo) come sottogruppo del gruppo di tutte le bigezioni di una struttura (algebrica, geometrica, topologica, o altro) che 'rispettano' la struttura stessa. Ad esempio V è uno spazio vettoriale di dimensione n sui reali e $\mathcal{B}$ è una sua base, allora ad ogni matrice quadrata reale e invertibile di rango n si associa una mappa lineare definita rispetto alla base $\mathcal{B}$, e ciò definisce un isomorfismo del gruppo $GL_n(\mathbb{R})$ del gruppo $Aut_{\mathbb{R}}(V)$ ovvero tutte le mappa lineare invertibili di V in se stesso. Questa è un azione di $GL_n(\mathbb{R})$ come gruppo di applicazioni lineari dello spazio V.

9.7.1 Gruppo Simmetrico

Come abbiamo già detto, una permutazione di un insieme X è un'applicazione biunivoca in se stesso. Da questa sezione in poi, useremo di preferenza la notazione a destra o esponenziali per le permutazioni; così, se $f : X \to X$ è una permutazione e $x \in X$ allora scriviamo xf o x^f al posto di $f(x)$; questo comporta che la composizione rispetta -da sinistra verso destra - l'ordine con cui le mappe vanno applicate.

Definizione: (7.1| Gruppo Simmetrico)

Se X è un inseme con $Sym(X)$ si denota il gruppo, rispetto alla composizione, di tutte le permutazione su X (detto 'gruppo simmetrico' su X). Osserviamo subito che X e Y sono insiemi della stessa cardinalità, e $f : X \to Y$ è una bigezione, allora porre $\alpha \mapsto f^{-1}\alpha f$, per ogni $\alpha \in Sym(X)$, definisce un isomorfismo $Sym(X) \to Sym(Y)$. In particolare, se X è un insieme finito di cardinalità n, possiamo assumere che X coincida con $I_n = \{1, 2, ..., n\}$. In tal caso, invece di $Sym(n)$ viene usato il simbolo S_n. Ricordiamo il fatto ben noto che, se $n \in \mathbb{N}$, allora $|S_n| = n!$.

Definizione: (7.2 | Permutazioni Finitarie)
Se $\sigma \in Sym(X)$ è una permutazione dell'insieme X, chiamiamo 'supporto' di σ l'insieme degli elementi di X che non sono fissati da σ:

$$supp(\sigma) = \{x \in X \text{ t.c. } x\sigma \neq x\}$$

Una permutazione σ si dice finitaria se $supp(\sigma)$ è finito. È quindi banale verifiare che l'insieme delle permutazioni finitarie di un insieme X è un sottogruppo normale di $Sym(X)$ che denotiamo con $FSym(X)$. Una singola permutazione finitaria si comporta come una permutazione su un insieme finito.
In questa sezione ci limitiamo a trattare principalemente, questo tipo di permutazioni.

Definizione: (7.3 | Cicli)
Come prima cosa introduciamo un modo comodo di rappresentare permutazioni finitarie.
Sia k un intero con $k > 1$; una permutazione $\pi \in Sym(X)$ si dice un ciclo di lunghezza k (o un $k - ciclo$) se esiste un sottoinsieme di cardinalità k, $\{i_1, ..., i_k\} \subseteq X$ tale che

- $i_1\pi = i_2,\ i_2\pi = i_3, ..., \ i_{k-1}\pi = i_k,\ i_k\pi = i_1$
- $j\pi = j$ per ogni $j \in X - \{i_1, 1_2, ..., i_k\}$

In tal caso, scriviamo $\pi = (i_1 \ \ ... \ \ i_k)$. Ad esempio la permutazione $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$ è un $4 - ciclo$.
Un ciclo di lunghezza 2, ovvero una permutazione del tipo $\tau = (i_1 \ ; i_2)$ si chiama 'trasposizione'.
Inoltre Due cicli σ e ρ si dicono disgiunti se

$$supp(\sigma) \cap supp(\rho) = \emptyset$$

Le seguenti osservazioni si dimostrano con un po' di pazienza ma facilmente. Sia $\sigma = (i_1 \ \ i_2 \ \ ... \ \ i_k)$, un $k - ciclo$. Allora

- $\sigma = (i_k \ \ i_{k-1} \ \ ... \ \ i_2 i_1) = (i_1 \ \ i_k \ \ ... \ \ i_3 \ \ i_2)$
- $\sigma{-}1 = (i_2 \ \ i_3 \ \ ... \ \ i_k i_1 = (i_3 \ \ i_4 \ \ ... \ \ i_k \ \ i_1 \ \ i_2)$
- Per $1 \leq r \leq k$

$$(i_j)\sigma^r = \begin{cases} i_{j+r} & \text{se} \quad j + r \leq k \\ i_{j+r-k} & \text{se} \quad j + r > k \end{cases}$$

Si ha poi - sempre piuttosto facilmente - la seguente conseguenza.

Lemma: (7.4)
Sia $\sigma \in Sym(X)$ un ciclo di lunghezza k, allora $|\sigma| = k$. Se $\sigma, \rho \in Sym(X)$ sono cicli disgiunti, allora $\sigma\rho = \rho\sigma$.

L'inverso di un $k - ciclo$ è, come abbiamo visto, un $k - ciclo$; mentre in generale la potenza di un ciclo non è un ciclo: ad esempio, se $\sigma = (1 \ \ 2 \ \ 6 \ \ 5 \ \ 4 \ \ 3)$, allora σ^2 non è un singolo ciclo, ma il prodotto di due cicli disgiunti $\sigma^2 = (1 \ \ 6 \ \ 4)(2 \ \ 5 \ \ 3)$. Di fatto ogni permutazione finitaria (non identica) si può fattorizzare come prodotto di cicli a due a due disgiunti.

Teorema: (7.5)

Sia X un insieme. Ogni permutazione $\pi \in FSym(X)$, si può fattorizzare come un prodotto

$$\pi = \sigma_1\sigma_2\cdots\sigma_t$$

di cicli $\sigma_1, ..., \sigma_t \in S_n$ a due a due disgiunti. A meno dell' ordine dei fattori, tale fattorizzazione di π è unica.

Ad esempio, la permutazione

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 7 & 6 \end{pmatrix} \in S_7$$

si scrive come prodotto di due cicli disgiunti $\pi = (1\ \ 3\ \ 5)(6\ \ 7) = (6\ \ 7)(1\ \ 3\ \ 5)$.

Osservazione: (7.5)
Il Teorema (7.5) implica in particolare, che le lunghezza dei cicli disgiunti che compongono la fattorizzazione di una permutazione finitaria σ sono univocamente individuate (con molteplicità) da σ stessa. La sequenza di tali lunghezza (poste in ordine crescente) si chiama il 'tipo ciclico' di σ. Nel caso di permutazioni finite (cioè $\sigma \in S_n$), si suole indicare anche i cicli di lunghezza 1, cioè i punti lasciati fissi da σ: Ad esmepio la permutazione $(1\ \ 3\ \ 4)(6\ \ 8)(2\ \ 5\ \ 9) \in S_9$ ha tipo ciclico $[1, 2, 3, 3]$.

Lemma: (7.6)
Sia $\sigma = (i_1\ \ i_2\ \ ...\ \ i_k)$ un $k - ciclo$ in $Sym(X)$ e $\pi \in Sym(X)$. Allora

$$\sigma^\pi = \pi^{-1}\sigma\pi = (i_1\pi\ \ i_2\pi\ \ ...\ \ i_k\pi)$$

In particolare la permutazione coniugata σ^π è un $k - ciclo$.

Da ciò segue che le permutazioni finitarie coniugate hanno lo stesso tipo ciclico: ad esmepio consideriamo in S_6 gli elementi $\pi = (1\ \ 2\ \ 3\ \ 4\ \ 5)$ e $\gamma = (1\ \ 3)(2\ \ 5\ \ 4\ \ 6)$; allora $\gamma^\pi = (1\ \ 3)^\pi(2\ \ 5\ \ 4\ \ 6)^\pi = (2\ \ 4)(3\ \ 1\ \ 5\ \ 6)$.

Teorema (7.7)
Due permutazioni finitarie σ e δ sono congiunte in $Sym(X)$ se e solo se hanno lo stesso tipo ciclico.

Dimostrazione:
È sufficiente provare che se γ e δ hanno lo stesso tipo ciclico, esiste $\pi \in Sym(X)$ tale che $\gamma^\pi = \delta$. Sia $\gamma^\pi = \delta$. Sia $\gamma = (a_1\ \ a_2\ \ ...\ \ a_h)(b_1\ \ b_2\ \ ...\ \ b_k)$ e $\delta = (\hat{a_1}\ \ \hat{a_2}\ \ ...\ \ \hat{a_h})(\hat{b_1}\ \ \hat{b_2}\ \ ...\ \ \hat{b_k})$ e siano $fix(\gamma) = X - supp(\gamma)$ e $fix(\delta) = X - supp(\delta)$ gli insieme degli elementi fissati di γ e δ rispettivamente. Chiaramente: $|fix(\gamma)| = |fix(\delta)|$; sia $\beta : fix(\gamma) \to fix(\delta)$ una bigezione. Consideriamo quindi la permutazione $\pi \in Sym(X)$ definita da:

$$(a)\pi = \begin{cases} \hat{a} \text{ se } a \in supp(\gamma) \text{ ovvero } a \in \{a_1, ..., a_h, b_1, ..., b_k\} \\ (a)\beta \text{ se } a \notin supp(\gamma) \end{cases}$$

Per il lemma (7.6) allora segue che $\delta = \pi^{-1}\gamma\pi$. Si osservi che non è difficile mostrare che anche tale permutazione π può essere presa finitaria.

Osservazione: (7.8)
Sia $\gamma = (i_1\ \ i_2\ \ ...\ \ i_k)$ un $k - ciclo$ in $Sym(X)$; allora

$$\gamma = (i_1\ \ i_2)(i_1\ \ i_3)...(i_1\ \ i_k)$$

Ogni $k - ciclo$ è dunque prodotto di $k - 1$ trasposizioni. Unita al teorema (7.5), questa semplice osservazione implica immediatamente il seguente fatto fondamentale.

Teorema: (7.9)
Sia $n \geq 2$, allora ogni permutazione finitaria è il prodotto di un numero finito di trasposizioni.

In altra parole, il gruppo $FSym(X)$ è generato dall'insieme delle sue trasposizioni.

$$\{(i, j) \text{ t.c. } i, j \in X, \quad i \neq j\}$$

Una permutazione finitaria γ può essere scritta in modi diversi come prodotto di trasposizioni, sia per i fattori che per il loro numero; ad esempio, in S_4, $(1\ \ 2\ \ 3) = (1\ \ 2)(1\ \ 3) = (1\ \ 2)(2\ \ 4)(2\ \ 3)(3\ \ 4)$. Quello che tuttavia dipende da γ è la parità o la disparità del numero di trasposizioni che costituiscono una qualsiasi fattorizzazione di γ; cioè se $\gamma = \tau_1\tau_2...\tau_d$, allora il numero $sgn(\gamma) = (-1)^d$ non dipende dalla specifica fattorizzazione. Tale numero si chiama 'segnatura' della permutazione finitaria γ. Una maniera per calcolarla facilmente consiste nel considerare il tipo ciclico $[d_1, d_2, ..., d_k]$ di γ e applicare per i singoli l'applicazione di sopra; si ottiene quindi

$$sgn(\gamma) = \prod_{i+1}^{k}(-1)^{d_i - 1}$$

Osservazione: (7.10)
È poi del tutto ovvio che la segnatura definisce un omomrfismo suriettivo del gruppo $FSym(X)$ nel gruppo moltiplicativo $\{-1, +1\}$. Il nucleo di tale omomorfismo si chiama 'gruppo alterno' su X e si denota cone $Alt(X)$; se X è finito e di cardinalità n, allora il gruppo si denota con A_n. $Alt(X)$ è costituito fa tutte e sole le permutazioni finitarie la cui segnatura è 1, quelle che quindi risultano il prodotto di un numero pari di trasposizioni (e sono per questo chiamate permutazioni (di classe) 'pari'.
Le permutazioni appartenenti a $FSym(X) - Alt(X)$ si dicono ovviamente, (permutazioni finitarie (di classeùù) 'dispari'.
Siccome $Alt(X)$ è un sottogruppo normale di $FSym(X)$, e, per quanto visto precedentemente $[Sym(X) : Alt(X)] = 2$, in particolare per $2 \leq n \in \mathbb{N}$, si ha

$$|A_n| = |S_n/2| = n!/2$$

9.7.2 Orbite e stabilizzatori

Come già detto, un'azione del gruppo G su un insieme non vuoto S è un omomorfismo

$$\phi : G \to Sym(S)$$

Il nucleo $ker(\phi)$ si dice 'nucleo dell'azione'. L'azione di dice fedele se è iniettiva (ovvero se $ker(\phi) = \{e_G\}$): In questo caso l'immagine $\phi(G)$ è un sottogruppo di $Sym(S)$ isomorfo a G, si dice (identificando G con $\phi(G)$) che G è un gruppo di permutazioni su S.

Sia $G \to Sym(S)$ un'azione di G su S e, per goni $g \in G$ e ogni $s \in S$, sia $sg = s^{\phi(g)}$.
Sussitono allora le seguenti proprietà: per ogni $g, h \in G$ e ogni $s \in S$:

$$s(gh) = (sg)h, \quad se_G = s$$

Ciò suggrisce una maniera equivalente per definire il concetto di azione: se G è un gruppo e S un insieme, una azione di G su S è una mappa $S \times G \to S$ data da $(s, g) \mapsto sg$, tale soddisfa le proprietà viste prima per ogni $s \in S$ ed ogni $g, h \in G$. Se ciò avviene, dato $g \in G$ la mappa

$$\phi(g) : S \to S$$

$$s \mapsto sg$$

è una permutazione si S, e questo definisce un omomorfismo di G in $Sym(S)$.

Definizione: (7.11)
Supponiamo di avere data una azione del gruppo G sull'insieme S. Per ogni $s \in S$ si definiscono:

- l'orbita $O_G(s)$ di s (rispetto alla azione di G), come l'insieme dei trasformati di s tramite tutti gli elementi di G:

$$O_G(s) = \{sg \text{ t.c. } g \in G\}$$

- lo stabilizzatore G_s (o anche $Stab_G(s)$) di s in G, come gli insieme degli elementi di G la cui permutazione fissa s:
$$G_s = \{g \in G \text{ t.c. } sg = s\}$$

Nota: (7.12) Prima di proseguire, si osservi il fatto elementare fondamentale che, data una azione del gruppo G sull'insieme S, le $G-orbite$ distinte costituiscono una partizione $\mathcal{P}$ di S.

Teorema: (7.13)
Sia data una azione del gruppo G sull'insieme S, e sia $s \in S$. Allora

- G_s è un sottogruppo di G
- $|O_G(s)| = [G : G_s]$

Dimostrazione:
(i) Poichè $se_G = s$, si ha $e_g \in G_s$ per qualunque $s \in S$. Fissato ora un tale punto s, siano $g, h \in G_s$. Allora $sg = s = sh$ e quindi
$$s(g^{-1}h) = (sg)(g^{-1}h) = s(gg^{-1}h) = sh = s$$
Dunque $g^{-1}h \in G_s$ e dunque G_s è un sottogruppo di G.
(ii) Sia $\mathcal{C} = \{G_s x \text{ t.c. } x \in G\}$ lo spazio quoziente G/G_s.
$$\eta : \mathcal{C} \to O_G(s)$$
$$G_s x \mapsto sx$$
Se $x, y \in G$ sono tali che $G_s x = G_s y$ allora $xy^{-1} \in G_s$, cioè $s(xy^{-1}) = s$ e quindi $sx = s(xy^{-1}y) = (s(xy^{-1}))y = sy$ Dunque η è ben definita.
Proviamo ora che η è biettiva. Essa è suriettiva per definizione dei orbita di s. Siano ora $G_s x, G_s y \in G/G_s$ tali che $sx = sy$, allora
$$sx(y^{-1}) = (sx)y^{-1} = (sy)y^{-1} = s(yy^{-1}) = s$$
Dunque $xy^{-1} \in G_s$, cioè $G_s x = G_s y$. Quindi η è iniettiva e pertanto una bigezione.
In particolare si ha $[G : G_s] = |\mathcal{C}| = |O_G(s)|$. Dunque per Lagrange possiamo anche dire:

Corollario: (7.14)
Se il gruppo finito G opera sull'insieme S, allora per ogni $s \in S$, $|O_G(s)|$ divide $|G|$.

Consideriamo ora il caso in cui sia G che S sono finiti, ed è data una azione di G su S. Siano $O_G(s_1)$, ..., $O_G(s_n)$ le orbite distinte di G su S (l'insieme $\{s_1, ..., s_n\}$ si dice un insieme di rappresentanti per le orbite di G su S. Per quanto osservato, esse costituiscono una partizione di S, quindi
$$|S| = |O_G(s_1)| + |O_G(s_2)| + \cdots + |O_G(s_n)|$$
Ora, per il teorema (7.13) si ha $|O_G(s_i)| = [S : G_{s_i}]$; quindi si ricava l'importante

Teorema: (7.15 | Equazione delle orbite)
Sia $s_1, s_2, ..., s_n$ un insieme di rappresentanti per le orbite di G su S. Allora
$$|S| = \sum_{i_1}^{n} [G : G_{s_i}]$$

Definizione: (7.16 | Punti Fissi)
Se G opera sull'insieme S è tale che $O_G(s) = \{s\}$, allora s si dice un 'punto fisso' per l'azione di G su S. In altri termini, $s \in S$ è un punto fisso se e solo se $sg = s$ per ogni $g \in G$, ovvero se e solo se $G_s = G$. L'insieme (possibilmente vuoto) dei punti fissi lo denoteremo con $Fix_S(G)$.

Come applicazione dell'equazione delle orbite, vediamo un criterio sufficiente all'esistenza di un punto fisso. Sia p un numero primo, sia P un gruppo di ordine p^m, e sia data una azione di P su un insieme finito S. Sia $\{s_1, s_2, ..., s_n\}$ un insieme di rappresentanti per le orbite di G su S, e $F = Fix_s(P)$ l'insieme dei punti fissi. Per il teorema di Lagrange, per ogni $i = 1, .., n$, l'indice $[G : G_{s_i}]$ divide $|P| = p^m$. Allora per ogni $i = 1, ..., n$, o s_i è un punto fisso, cioè $s_i \in F$, oppure G_{s_i} è un sottogruppo proprio di P (numero di elementi strettamente minore) e quindi $[G : G_{s_i}] = p^{k(i)}$ con $m > k(i) \geq 1$; in particolare p divide $[G : G_{s_i}]$. Applicando la formula delle orbite si ha che p divide $sum_{i=1}^n [G : G_{s_i}] = |S| - |F|$. Abbiamo quindi dimostrato

Proposizione: (7.16)
Sia P un $p - gruppo$ finito che opera su un insieme S; allora

$$Fix_S(P) \equiv |S| \bmod p$$

In particolare si ha:

Corollario: (7.17)
Sia P un $p - gruppo$ finito che opera su un inseme S. Se $mcd(|S|, p) = 1$ allora esiste almeno un punto fisso di P su S.

Lemma: (7.18 | Lemma di Burnside)
Sia G un gruppo finito e sia data una azione del gruppo G su un insieme S. Sia t il numero di orbite distinte e, per ogni $g \in G$ denotiamo con $Fix(g)$ l'insieme dei punti fissi per g su S. Allora

$$t|G| = \sum_{g \in G} |Fix(g)|$$

Dimostrazione:
Sia $\mathcal{F} = \{(g, s) \in G \times S \text{ t.c. } sg = s\}$. Calcolando la cardinalità di $\mathcal{F}$ concentrandoci sulla prima componente g, si ha:

$$|\mathcal{F}| = \sum_{g \in G} |Fix(g)|$$

mentre, calcolando la stessa cardinalità concentrandoci sulla seconda componente si ottiene:

$$|\mathcal{F}| = \sum_{s \in S} |G_s|$$

Ora è chiaro che se s_1 e s_2 appartengono alla stessa orbita allora $|G_{s_1}| = |G_{s_2}|$; dunque, se $s_1, ..., s_t$ sono rappresentanti delle diverse orbite per G su S, dalla equazione precedente segue

$$|\mathcal{F}| = \sum_{i=1} t|O_G(s_i)||G_{s_i}| = \sum_{i=1}^{t} [G : G_{s_i}]|G_{s_i}| = t|G|$$

Definizione: (7.19 | Azioni transitive)
Una azione di G sull'insieme S di dice transitiva se esiste $s \in S$ tale che $O_G(s) = S$; ciò avviene se per ogni $t \in S$ esiste $g \in G$ tale che $sg = t$. Si osservi in particolare che se G è finito e l'azione di G su S è transitiva $|S|$ divide $|G|$.

9.7.3 Azioni su cosets

Descriviamo ora una classe fondamentale di azioni transitive su un gruppo G. Sia H un sottogruppo fissato di G, prendiamo G/H l'insieme di tutti i coset destri di H; su questo insieme deifniamo un azione di G, ponendo, per ogni $g \in G$ e ogni $Hx \in G/H$,

$$(Hx)g = Hxg$$

Si verifica immadiatamente che ciò definisce un azione. Tale azione è transitiva: infatti, per ogni $Hx, Hy \in G/H$ si ha

$$Hx(x^{-1}y) = Hxx^{-1}y = Hy$$

Supponiamo ora che l'indice $[G : H] = n$ sia finito. Allora $|G/H| = [G : H] = n$ e l'azione di G su G/H sopra descritta da luogo a un omomorfismo $G \to Sym(G/H) = S_n$. Sia N il kernel di questo omomorfismo, allora

$$N = \{g \in G \text{ t.c. } Hxg = Hx \ \forall Hx \in G/H\} = \{g \in G \text{ t.c. } Hxgx^{-1} = H \ \forall x \in G\}$$

osservando che

$$Hxgx^{-1} = H \iff xgx^{-1} \in H \iff g \in x^{-1}Hx = H^x$$

possiamo concludere che

$$N = \{g \in G \text{ t.c. } g \in H^x \ \forall x \in G\} = \bigcap_{x \in G} H^x$$

Questo sottogruppo di G su denota con H_G. Chiaramente H_G è il massimo sottogruppo noramle di G contenuto in G. Inoltre per quanto visto sugli omomorfismi, G/H_G è isomorfo ad un sottogruppo di S_n, in particolare $[G : H_G]$ divide $n!$.

Nel caso particolare in cui $H = \{e\}$, l'azione delle classi laterali coincide con quella di moltiplicazione a destra sugli elementi. Tale azione è sicuramente fedele, e ciò mostra come ogni gruppo si possa rappresentare come gruppo di permutazioni (transitivo): che è il cosiddetto Teorema di Cayley:

Teorema: (7.19 | Teorema di Cayley)
Sia G un gruppo. Allora G è isomorfo ad un sottogruppo del sottorgruppo simmetrico $Sym(G)$.

Dimostrazione:
Per ogni $g \in G$, la moltiplicazione a destra $\rho_g : G \to G$, definita da $x \mapsto xg$ (per ogni $x \in G$), è una bigezione (quindi un elemento di $Sym(G)$); e quindi l'applicazione $\phi : G \to Sym(G)$ definita da $x \mapsto \rho_g$ (per ogni $g \in G$), è un omomorfismo iniettivo da G nel gruppo $Sym(G)$. Da ciò si conclude che G è isomorfo a $\phi(G)$ che è un sottogruppo di $Sym(G)$.

9.8 Esercizi

Esercizio 1
Mostra che $Z(G)$ è un sottogruppo di G.

$Z(G)$ è non vuoto perchè $e \in Z(G)$ in quanto commuta con tutti gli elementi di g. Dati $a, b \in Z(G)$ allora consideriamo $ga = ag$ e $gb = bg \implies b^{-1}gb = g \implies g = b^{-1}g(b^{-1})^{-1} \implies b^{-1} \in Z(G)$ infine $gab^{-1} = agb^{-1} = ab^{-1}g \implies ab^{-1} \in Z(G)$.

Esercizio 3
Sia G un gruppo finito. Mostra che se H e K sono sottogruppi normali tali che $|G| = |H||K|$ e $mcd(|H|, |K|) = 1$ allora $HK = G$.

Prendendo in considerazione $hk(kh)^{-1} = hkh^{-1}k^{-1}$ si osserva che $h(kHk^{-1}) \in H$ siccome $H \triangleleft G$. Al contempo si osserva che $(hKh^{-1})k \in K$ siccome $K \triangleleft G$. Dunque $hkh^{-1}k^{-1} \in H \cap K$. $H \cap K$ è un sottogruppo di G in quanto è non vuoto perchè $H \cap K = \{e\}$. A Questo punto scriviamo $|HK| = |H||K|$

$$|HK| = \frac{|H||K|}{|H \cap K|} = |G|$$

La formula si può dimostrare prendendo in considerazione la mappa $\phi : A \times B \to G$ definita ponendo, per ogni $(a, b) \in A \times B, \phi((a, b)) = ab$. Si osserva che l'insieme delle controimmagini $\phi^{-1}(g)$ è una partizione di $A \times B$ il che implica $|A \times B| = |A||B| = \sum_{g \in AB} |\phi^{-1}(G)| = |AB||A \cap B|$. Perciò $HK = G$.

Esercizio 2
Mostra che nel constesto dell'esercizio precedente, se $hk = kh$ per tutti $h \in H$ e $k \in K$ quindi $f : H \times K \to G$ dati per $f((h, k)) = hk$ è un isomorfismo di gruppi.

(i)f è ben definita siccome date due coppie (h, k) e (h', k') con $h = h'$ e $h = k'$ si ha $hk = h'k'$ dato che la mappa del gruppo è ben definita in principio.

(ii)f è suriettiva in quanto come visto prima $HK \subseteq G \wedge |HK| = |G| \implies HK = G = H \times K$.

(iii)f è iniettiva siccome si tratta di insiemi finiti con stessa cardinalità.

(iv) f è un omomorfismo perchè $f((h1h_2, k_1k_2)) = h_1h_2k_1k_2$ è uguale (ricordandoci di $hk = kh$) a $h_1k_1h_2k_2 = f((h_1, k_1))f((h_2, k_2))$.

Esercizio 3
Mostra che se H e K sono sottogruppi normali di G allora

$$HK = \{hk \text{ t.c. } h \in H, \quad k \in K\}$$

è un sottogruppo normale di G.

$H = gHg^{-1}$ in quanto H è normale e $K = g'Kg'^{-1}$. Dunque $HK = gHg^{-1}g'K(g')^{-1}$ siccome deve valere per ogni $g, g' \in G$ senza perdità di generalità possiamo assumere $g = g'$. Perciò $gHg^{-1}gKg^{-1} = gH(g^{-1}g)Kg^{-1} = gHKg^{-1} = HK$ che implica che $HK \triangleleft G$.

Esercizio 4
Sia A un gruppo abeliano e n un numero intero positivo. Mostra che $f(a) = a^n$ è un omomorfismo di gruppi.

Innanzitutto definiamo la funzione $f : A \to A$ A è un gruppo perciò $Im(f) \subseteq A$.A questo punto si osserva $f(ab) = (ab)^n = \prod_{i=1}^{n} ab$ siccome è abeliano riscriviamo la produttoria in modo da avere prima tutti i termini a e poi tutti i termini b. Dunque

$$f(ab) = (ab)^n = \prod_{i=1}^{n} ab = \prod_{i=1}^{n} a \prod_{i=1}^{n} b = a^n b^n = f(a)f(b)$$

Esercizio 7
Verifica che se $f : G \to H$ e $g : G \to H$ sono omomorfismi di gruppo allora $g \circ f : G \to K$ è un omomorfismo di gruppo.

Applicando g a $f(g_1)f(g_2)$ troviamo $g(f(g_1)f(g_2))$tuttavia g è un omomorfismo di gruppi, perciò possiamo scrivere $g(f(g_1)f(g_2)) = g(f(g_1))g(f(g_2))$ ma f era a sua volta un omomorfismo, ricaviamo $g(f(g_1g_2)) = g(f(g_1)g(f(g_2))$ per cui $g \circ f$ è un omomorfismo di gruppi.

Esercizio 5
Sia data un azione del gruppo G su un insieme S. Siano $s \in S$, $g \in G$ e poniamo $sg = t$. Si dimostri che $G_s = g(G_t)g^{-1}$.

Innanzitutto si nota che $s, t \in O_G(s)$. Se $g \in G_s$ allora $sg = s$. Inoltre $g' \in G_t$ se $tg' = t$. Dunque

$$sg = t = tg' = t(G_t), \quad s(G_s) = s$$

Ricaviamo $s(G_s)g = sg(G_t)$ che per le leggi di cancellazione è equivalente a $s(G_s) = sg(G_t)g^{-1}$. Ricordiamo la bigezione tra G/G_s e $O_G(s)$, siccome s e t hanno stessa orbita possiamo fare la seguente osservazione $(G_s)(G_s) = (G_s)g(G_t)g^{-1}$ risultano essere due cosets destri che, per definizione, sono una partizione di G perciò $(G_s) = g(G_t)g^{-1}$.

Esercizio 6
Sia A un gruppo abeliano finito. Sia $f : A \to$ un omomorfismo. Quindi il teorema di decomposizione Fitting dice che esiste un intero postivo tale che $A = ker(f^k) \times Im(f^k)$.

- Verifica il Teorema di decomposizione Fitting per il gruppo $\mathbb{Z}_{36}$ e l'omomorfismo $f(x) = 3x$

- Se p è un fattore primo di A e $f(x) = px$ mostrare che $ker(f^j) \neq \{e\}$ per tutti i $J > 0$

(i) Innanzitutto si nota che il gruppo $\mathbb{Z}_{36}$ è isomorfo a $\mathbb{Z}_9 \times \mathbb{Z}_4$. Si potrebbe dimostrare che esiste un k tale che $Im(f^k) \cong \mathbb{Z}_4$ e $Ker(f^k) \cong \mathbb{Z}_9$. con $K = 3$ si nota che il $ker(f^k) = \{a \in A \text{ t.c. } [9a] = [0]\}$. Questo gruppo è isomorfo a $\mathbb{Z}_9$ in quanto suriettiva perchè partizione di $\mathbb{Z}$ e iniettiva siccome ogni multiplo di 4 è unicamente definito da un intero $[a] \in \mathbb{Z}_9$. $Im(f^k)$ è isomorfo a $\mathbb{Z}^4$ in quanto persiste la suriettività siccome $\mathbb{Z}_4$ identifica una partizione di $\mathbb{Z}$ è iniettiva perchè $a - b \mid 4 \implies a - b \mid 36$.

(ii) Per la proposizione (6.12) essendo A un gruppo abeliano finito con p fattore primo di $|A|$ allora esiste un elemento di ordine p. Ricordiamo che l'identità ha ordine 1. Dunque esiste un elemento in $ker(f^j)$ che non è l'identità per tutti i $j > 0$.

Esercizio 7
Dimostra che tutti i sottogruppi di un gruppo ciclico sono ciclici.

Dato $G = \langle a \rangle$ un gruppo ciclico di ordine n. Per il teorema di Lagange se H è un sottrogruppo di G con $|H| = m$ allora $m \mid n$ a questo punto $H_m = \langle a^{n/m}$ è un sottogruppo di ordine m. A questo punto suppongo che G non abbia altri sottogruppi di ordine m. Il gruppo G/H ha ordine n/m, dunque $x^{n/m} = e$ oer ogni $x \in G/H$. Questo vuol dire che $x^{n/m} \in H$ per ogni $x \in G$ che vuol dire $H_m \leq H$. Questi due sottogruppi hanno però lo stesso ordine dunque $H = H_m$.

Esercizio 8 Siano G e H due gruppi abeliani. Sia λ_G l'esponente di G e λ_H l'esponente di H. Trova l'esponente del gruppo $G \times H$ in funzione di $\lambda_G \lambda_H$.

Si osserva pittosto facilmente che $e_{G \times H} = (e_G, e_H)$ Dato un elemento (g_1, h_1) allora $(g_1, h_1)^{mcm(\lambda_1, \lambda_2)} = (g_1^{mcm(\lambda_1,\lambda_2)}, g_2^{mcm(\lambda_1,\lambda_2))})$ che è uguale a (e_G, e_H) siccome $\lambda_1 \mid mcm(\lambda_1, \lambda_2)$ e $\lambda_2 \mid mcm(\lambda_1, \lambda_2)$ e rispetta la definizione di esponente del gruppo abeliano.

Esercizio 8
Sia p un primo e G un gruppo di ordine p^2. Se G ha un elemento di ordine p^2 allora $G = \mathbb{Z}_{p^2}$. Altrimenti possiamo scegliere $u \in Z(G) - \{e\}$ e $v \in G - \langle u \rangle$. Mostra che la mappa

$$\mathbb{Z}_p \times \mathbb{Z}_p \to G, \quad f(j,k) = u^j v^k$$

è un isomorfismo.

(i)f è ben definita in quanto dati due elementi (a, b) e $(a \pm kp, b \pm k'p)$ allora $f((a \pm kp, b \pm kp)) = u^a u^{\pm kp} v^b v^{\pm k'p}$. L'ordine di u deve dividere $|G|$ dunque o $ord(g) = 1$ o $ord(g) = p$ o $ord(g) = p^2$. 1 non può essere perchè $u \neq e$ e $v \neq e$. Per ipotesi l'ordine di u e v non può essere p^2. Perciò l'ordine di u e v è p, che implica $u^{kp} = e = u^{-kp}$ e $v^{kp} = e = v^{-kp}$.

$$u^a u^{\pm kp} v^b v^{\pm kp} = u^a v^b$$

(ii)f è suriettiva siccome ogni elemento g o è generato da u^k (per qualche k o viene generato da v in quanto è $G - \langle u \rangle$. In particolare se $Z(G) - \{e\}$ è vuoto allora tutti gli elementi g vengono generati da v. Se non $Z(G) - \{e\}$ non è vuoto allora g o è generato da u, in quanto sottogruppo di G, o e generato da v ($g = eg = u^{kp} v$ con $g \in V = G - \langle u \rangle$).

(iii) Siccome I due insiemi hanno stessa cardianlità possiamo dire che suriettività e iniettività sono equivalenti. Perciò la mappa è biettiva.

(iv) Controlliamo adesso se si tratta di un omomorfismo

$$f((aa', bb')) = u^a u^{a'} v^b v^{b'}$$

Siccome $u \in Z(G)$ allora $u^{a'}$ commuta con tutti gli elementi in g, si ha dunque

$$u^a u^{a'} v^b v^{b'} = u^a v^b u^{a'} v^{b'} = f((a,b)) f((a',b'))$$

10 Anelli e Ideali

Abbiamo visto precedentemente un introduzione ad anelli commutativi con identità e domini integrali. Vediamo ora di dare delle proprietà e osservazioni importanti per anelli non commutativi con identità.

Osservazione:
Come visto per la teoria dei gruppi l'elemento neutro per l'addizione 0_R è unico, allo stesso modo si dimostra che 1_R (elemento neutro per la moltiplicazione) è unico. Si può fare una osservazione analoga per l'inverso moltiplicativo se esiste.

Definizione: (1.1)
Sia R un anello commutativo. Diciamo che a è un divisore di R se esiste $b \in R$, $b \neq 0$ tale che $ab = 0$. In particolare, 0 è un divisore di 0. Un anello commutativo R in cui l'unico divisore di 0 è 0 è un dominio integrale.

Definizione: (1,2)
Un elemento u di un anello R si dice invertibile se esiste $v \in R$ tale che $uv = vu = 1$ (cioè deve esistere un inverso sinistro e destro di u rispetto alla moltiplicazione).

Definizione: (1.3)
Un anello R in cui $0 \neq 1$ che soddisfa la seguente proprietà è detto 'corpo':

- ogni $a \in R - \{0\}$ è invertibile

Un corpo commutativo viene detto campo.

Osservazione: (1.4)
Esiste l'anello banale $A = \{0\}$, dove 0 soddisfa le proprietà per la moltiplicazione e per l'addizione allo stesso tempo.

Proprietà fondamentali:

- $a(0) = 0$ e $0(a) = 0$
- L'opposto di a è unico e $-(-a) = a$
- $a(-b) = (-a)b = -(ab)$, in particolare $(-1)a = a(-1) = -a$
- $(-a)(-b) = ab$, in particolare $(-1)(-1) = 1$

La dimostrazione è lasciata come esercizio al lettore.

Osservazione:
Dalla proprietà (1) segue in particolare che se in un anello abbiamo $0 = 1$ allora per ogni elemento possiamo scrivere $a(0) = 0$ come $a = a(1) = a0 = 0$ dunque risulta che A è l'anello banale. Dunque l'unico anello con unità per cui $0 = 1$ è l'anello banale.

Osservazione:
In ogni dominio integrale R vale la legge di cancellazione, ossia, se $a \in R$ diverso da 0 vale la legge di cancellazione:

$$ab = ac \implies a = c$$

Questa si può dimostrare facendo riferimento a un esercizio in particolare nell'introduzione.

Definizione: (1.5)
Dato un anello R, un sottoanello di R è un sottoinsieme $T \subseteq R$ tale che valgano le seguenti 3 condizioni:

- $1 \in T$

- T è un sottogruppo di R rispetto alla operazione $+$
- per ogni $a, b \in T$ vale $ab \in T$

Se $T \neq R$ si dice che T è un sottoanello proprio.

10.1 Omomorfismi di Anelli

Definizione: 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 struttura inerenti a tale anello. In altre parole,

$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1_R) = 1_S$$

Esercizio:
Verificare che se $f : R \to S$ è un omomorfismo di anelli allora $f(0_R) = 0_S$.

Il procedimento è analogo a quello visto per gli omomorfismi di gruppi: $0_S = 0_S + 0_S \implies f(0_S) = f(0_S) + f(0_S) \implies f(0_S) - f(0_S) = f(0_S) + f(0_S) - f(0_S) \implies 0_R = f(0_S)$.

Lemma:
Sia $\phi : R \to S$ un omomorfismo di anello. Allora $ker(\phi)$ è un sottogruppo additivo di R. Inoltre se $a \in ker(\phi)$ e $r \in R$ allora $ra \in ker(\phi)$ e $ar \in ker(\phi)$.

Dimostrazione:
La prima parte è stata già dimostrata nella sezione precedente. Siano ora $a \in ker(\phi)$ e $r \in R$. Vediamo che $\phi(ar) = \phi(a)\phi(r) = 0_S\phi(r) = 0 \implies ar \in ker(\phi)$. Simmetricamente si fa per ra.

10.2 Ideali e Anelli Quoziente

Lo studio dei *ker* degli omomorfismi ha messo in luce che in un anello ci sono alcuni sottoinsieme notevoli che non sono sottoanelli. La seguente definizione li individua.

Definizione: (2.1)
Un ideale I di un anello R è un sottogruppo additivo tale che per ogni $r \in R$ e per ogni $h \in I$ allora $rh \in I$ e $hr \in I$. Se $I \neq R$ si dice che I è un 'ideale proprio'.

La proprietà moltiplicativa che caratterizza gli ideali ci dice che I assorbe la moltiplicazione a destra e a sinistra per elementi arbitrari dell'anello (sottolineamo che la definizione è dunque quello di 'ideale bilatero: In questo corso visto che lavoreremo solo con anelli commutativi, non avremo bisogno di approfondire il concetto di 'ideale non bilatero').

Osservazione: (2.2)
Un idele I non è un sottoanello di R, a parte il caso in cui $I = R$. Infatti se $1 \in I$ allora $I = R$ per la proprietà di assorbimento.

Esempio: (2.3)
Sia $R = \mathbb{Z}$. L'insieme $6\mathbb{Z}$ composto da tutti i multipli di 6 ci fornisce l'esempio di un ideale. In generale, dato un anello commutativo R e un elemento $a \in R$, denoteremo $\langle a \rangle$ l'insieme di tutti gli elementi dell'anello che si possono scrivere come ak per un certo $k \in R$. Si verifica facielmente che $\langle a \rangle$ è un ideale, e si chiama ideale generato da a. Notate che, dato un gruppo G e un elemento $g \in G$ avevamo chiamato $\langle g \rangle$ il sottogruppo ciclico generato da g. Le due notazioni riguardano concetti diversi, ma non si creerà confuzione perchè sarà sempre chiaro dal contesto a quale caso ci stiamo riferendo. Per l'appunto se $G = \mathbb{Z}$ le due notazioni coincidono: Il sottogruppo ciclico $\langle 6 \rangle$ (pensando $\mathbb{Z}$ come gruppo con la +) coincide con l'ideale $\langle 6 \rangle$ (pensando $\mathbb{Z}$ come anello.

Osservazione: (2.3)

Il $ker(\phi)$ di un omomorfismo di anello $\phi\ :\ R\ \rightarrow\ S$ è un ideale I di R per quanto dimostrato nella sezione sugli omomorfismi di anello commutativi.

Proporizione: (2.4)
Se I e J sono due ideali dell'anello R allora anche $I + J = \{i + j \text{ t.c. } i \in I, j \in J\}$ e $I \cap J$ sono ideali di R. Le due dimostrazioni sono banali.

Dato un ideale I in un anello R, denotiamo con R/I l'insieme dei laterali di I in R, considerando I come sottogruppo additivo di R. Possiamo scrivere gli elementi di R/I con la notazione additiva $a + I$, con $a \in R$, e possiamo dare a R/I una struttura di gruppo additivo, con la somma definita da: $(a + I) + (b + I) = (a + b) + I$.
Per dotare R/I di una struttura di anello dobbiamo ora definire una moltiplicazione. La cosa più naturale è definire $(a + I)(b + I) = ab + I$. Dobbiamo però assicurarci che si tratti di una buona definizione, ovvero dobbiamo verfificare che se $a+I = a'+I$ e se $b+I = b'+I$ allora vale $ab+I = a'b'+I$. Da quanto visto sui coset affermiamo che se $a + I = a' + I$ allora $a - a' \in I$ stessa cosa si osserva per $b + I = b' + I$ dunque $b - b' \in I$. Ne segue

$$ab = (a' + i_1)(b' + i_2) = a'b' + a'i_2 + i_1b' + i_1i_2$$

Per le proprietà di assorbimento degli ideali gli ultimi 3 termini sono $\in I$ siccome è I è un sottogruppo additivo allora abbiamo verificato che è ben definita come oprazione.

Proposizione: (2.5)
R/I è un anello con identità, in particolare $(1 + J)$ è l'identità per la moltiplicazione.

Osservazione: (2.6)
Abbiamo appena definito la moltiplicazione nell'anello quoziente R/I: $(a + I)(b + I) = ab + I$. Questa è una definizione in cui le classi laterali sono pensate come elementi del quoziente R/I. Pensiamole invece adesso come sottoinsiemi di R. Osserviamo che in R vale, dal punto di vista insiemistico,

$$(a + I)(b + I))\{(a + i_1)(b + i_2) \text{ t.c. } i_1, 1_2 \in I\} \subseteq ab + I$$

dove l'ultima inclusione può essere stretta. Prendiamo come esempio $\mathbb{Z}$ e l'ideale $6\mathbb{Z}$: si ha $(2 + 6\mathbb{Z})(4 + 6\mathbb{Z} \subset 8 + 6\mathbb{Z}$. Infatti 14 appartiene al laterale $8 + 6\mathbb{Z}$ ma non può essere scritto come $(2 + 6k)(2 + 6h)$ con h, k interi.

Compiuta la costruzione dell'anello quoziente di un anello rispetto ad un suo ideale possiamo ora enunciare per gli anelli il primo teorema di omomorfismo, analogo a quello per i gruppi. Lasciamo a voi la dimostrazione come utile esercizio di ripasso, in quanto si dimostra pedissequamente traducendo dal linguaggio dei gruppi a quello degli anelli.

Teorema: (2.7)
Siano R e S due anelli, e sia $\phi : R \rightarrow S$ un omomorfismo di anelli. Allora

$$R/ker(\phi) \cong Im(\phi)$$

Definizione: (2.8)
Un ideale I di un anello commutativo A si dice principale se è generato da un solo elemento, ossia se esiste $a \in A$ tale che $I = \langle a \rangle$.

Definizione: (2.9)
Un dominio integrale si dice 'dominio ad ideali principali' (PID) se tutti i suoi ideali sono principali.

Osservazione: (2.10)
Consideriamo $K[x, y]$, l'anello dei polinomi a coefficienti in un campo K e nelle variabili x e y. Questo anello non è a ideali principali: si può mostrare che l' ideale $I = (x, y)$ generato dalle variabili x e y non può essere generato da un solo elemento.

Osservazione: (2.11)

Consideriamo $\mathbb{Z}[x]$ l'anello dei polinomi con coefficienti in $\mathbb{Z}$ nella variabile x. Anche questo anello non è a ideali principali: si può mostrare che l'ideale $I = (2, x)$ non può essere generato da un solo elemento.

Osservazione: (2.12)
Come abbiamo visto nel capitolo precedente, dati due polinomi $f(x), g(x) \in K[x]$ esiste un massimo comun divisore monico $mcd(f(x), g(x))$. Come sappiamo l'ideale $(f(x), g(x))$ in $K[x]$ è principale che coincide con l'ideale generato da $mcd(f(x), g(x))$.

10.3 Il quoziente $K[x]/\langle f(x)\rangle$

In questa sezione vogliamo capire meglio come funzione il quoziente $K[x]/\langle f(x)\rangle$. Dove K è un campo e $f(x) \in K[x]$.
Ci sono due casi banali: se $f(x) = 0$, allora l'ideale $(0) = \{0\}$ è banale, dunque $K[x]/\langle f(x)\rangle \cong K[x]$. Se $f(x) = a \in K$ costante con $a \neq 0$, allora $(a) = K[x]$ e in questo caso il quoziente è banale ossia l'anello in cui $1 = 0$. L'idea è che nel quoziente $K[x]/\langle f(x)\rangle$ stiamo imponendo la relazione '$f(x) = 0$'. Per capire meglio, vediamo un esmepio.

Esempio: (3.1)
Consideriamo $K = \mathbb{R}$, e $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Allora in $\mathbb{R}[x]/\langle x^2 + 1\rangle$ ' vale la relazione $x^2 + 1 = 0$, ossia $x^2 = -1$'. In questo senso: se ad esempio abbiamo un elemento $3x^4 - 5x^3 + x - \sqrt{3} + \langle f(x)\rangle$, allora possiamo sostituire x^2 con -1, ottenendo ad esempio

$$3(x^2)^2 - 5x^3 + x - \sqrt{3} + \langle f(x)\rangle = 3(-1)^3 - 5x^3 + x - \sqrt{3} + \langle f(x)\rangle$$

$$3(-1)^2 - 5x(-1) + x + \langle f(x)\rangle$$

$$5x + 3 - \sqrt{3} + \langle f(x)\rangle$$

Dall'esempio appena visto è chiaro che facenfo questo tipo di sostituzioni, possiamo scegliere sempre un rappresentante laterale $g(x) + \langle f(x)\rangle \in K[x]/\langle f(x)\rangle$ che abbia grado strettamente minore di $f(x)$: Infatti basta fare la divisione euclidea, che ci da

$$g(x) = q(x)f(x) + r(x) \text{ con } deg(r) < deg(f)$$

ed è ora charo che

$$g(x) + (f(x)) = q(x)f(x) + r(x) + \langle f(x)\rangle = r(x) + \langle f(x)\rangle$$

Dunque ogni elemento del quoziente $K[x](\langle f(x)\rangle$ è il laterale di un polinomio di grado minore di $deg(f) = n$. Vediamo ora gli stessi argomenti ma con un altro tipo di operazione l'estensione di campo.

Definizione: (3.2)
Sia $I \neq A$ un ideale di un anello commutativo A, I è detto massimale se per ogni ideale J di A tale che

$$I \subseteq J \subseteq A$$

si ha $I = J$ o $J = A$. In altre parole un ideale è massimale quando non è possibile inserire in altro ideale J di A che contenga I.

Teorema: (3.3)
Dato R un anello commutativo con identità con $I \subset R$ un ideale proprio. Allora I è un ideale massimale se e solo se R/I è un campo.

Dimostrazione:
Supponiamo I sia un ideale massimale, dimostriamo che $I + a \in R/I$ con $a \in R$ ha sempre inverso moltiplicativo. Definiamo un elemento $I + a \neq I + 0$ che significa $a \notin I$ (in un campo l'elemento neutro per l'addizione non deve avere inverso moltiplicativo). Consideriamo $J = I + Ra = \{i + ra \text{ t.c. } i \in I, \quad r \in R\}$, si nota che J è un ideale a sua volta. In particolare, per ogni $i \in I$, $i = i + 0a \in J$, dunque

$I \subseteq J$. Siccome I è massimale, $J = I$ o $J = R$, e $a = 0 + 1a \in J$, ma $a \notin I$, dunque $J \neq I$, ovvero $J = R$. A questo punto $I + Ra = R$, e siccome 1 è un elemento dell'anello possiamo scrivere $1 = i + ra$ per qualche $i \in I$ e $r \in R$. Allora $1 - ra = i \in I$, dunque $I + 1 = I + ra$, a questo punto possiamo scrivere $(I + r)(I + a) = I + a$, che verifica l'esistenza di $I + r$ inverso moltiplicativo di $I + a$, concludiamo che R/I è un campo. Viceversa supponiamo che R/I sia un campo. Consideriamo un ideale J tale che $J \subset I$. Allora esiste $x \in J - I$, dunque $x \notin I$ per cui possiamo scrivere $I + x \neq I + 0$. Siccome R/I è un campo, esiste $I + y \in R/I$ tale che $(I + x)(I + y) = I + xy = I + 1$. Ciò implica $xy - 1 \in I \subset J$. Consideriamo $1 = xy - (xy - 1)$ dove $x \in J$, $y \in R$ e $(xy - 1) \in I$, per la proprietà degli ideali $xy \in J$, J è un sottogruppo additivo dunque $1 \in J$. Se J è un ideale che contiene 1 allora $J = R$.

Definizione: (3.4)
Un ideale proprio I di un anello commutativo R si dice primo se per ogni $a, b \in R$ allora

$$ab \in I \implies a \in I \vee b \in I$$

Osservazione:
Gli ideali primi non nulli si $\mathbb{Z}$ sono tutti e soli del tipo $\langle p \rangle = p\mathbb{Z}$, con p primo.

Corollario: (3.5)
L'ideale proprio I di A è primo se e solo se l'anello A/I è un dominio.

Dimostrazione:

$$(a + I)(b + I) = I \iff (a + I) = I \vee b + I = I$$

Che è la definizione di dominio integrale.

Corollario: (3.6)
Se l'ideale è massimale allora è primo.

Dimostrazione:
Se l'ideale I di R è massimale, allora R/I è un campo, quindi in particolare R/I è un dominio integrale, perciò I è primo.

Osservazione:
In generale, non vale il viceversa del corollario (3.6). Infatti l'ideale $\langle 0 \rangle$ di $\mathbb{Z}$ è primo, siccome l'anello quoziente $\mathbb{Z}/0 = \mathbb{Z}$ è integro allora $\langle 0 \rangle$ è un ideale primo. Tuttavia $\langle 0 \rangle \subset 2\mathbb{Z} \neq \mathbb{Z}$ dunque $\langle 0 \rangle$ non è massimale.

Osservazione:
Gli ideali massimali di $\mathbb{Z}$ sono tutti e soli gli ideali $p\mathbb{Z}$ con p primo.

Osservazione:
L'ideale $I = 2\mathbb{Z}$ di $\mathbb{Z}$ è massimale, infatti, se J è un ideale di $\mathbb{Z}$ contenente I, allora $J = n\mathbb{Z}$ per qualche numero natuale n tale che $n \mid 2$. Quindi $n = \{1, 2\}$ ossia $J = \mathbb{Z}$ oppure $J = 2\mathbb{Z}$.

Proposizione: (3.7)
Se R è un dominio ad ideali principali, es I è un suo ideale proprio diverso da $\langle 0 \rangle$, allora I è primo implica che I è massimale.

Dimostrazione:
Supponiamo I sia primo, sia $a \in R$ tale che $I = \langle a \rangle$. Allora $a \neq 0$. Sia J un ideale di R contenente I, sia $b \in R$ tale che $J = \langle b \rangle$. Allora $a \in \langle b \rangle$, cioè esiste $x \in A$ tale che $a = xb$. Quindi $a \mid xb$, e dunque, essendo a primo, segue che $a \mid b$ oppure $a \mid x$. Nel primo caso $b \in \langle a \rangle$, dunque $I = \langle a \rangle = \langle b \rangle = J$. Nel secondo caso esiste $y \in A$ tale che $ay = x$. Allora $xby = x$, da cui, data l'integrita dell'anello R, ed essendo $x \neq 0$, segue che $by = 1$. Dunque $1 \in \langle b \rangle$ rendendo $\langle b \rangle = R$.

Si nota che se $f(x)$ è irriducibile in $K[x]$ allora l'ideale $\langle f(x) \rangle$ è massimale. Dunque $R/\langle f(x) \rangle$ è un campo.. Inoltre si nora che se p è primo allora $\mathbb{Z}/p\mathbb{Z}$ è un campo.

10.4 Campo dei quozienti

La csotruzione del campo dei quozienti di un dominio d'integrità ricalca la costruzione formale dei razionali a partire dagli interi: nel prodotto cartesiano $D \times D - \{0\}$ si definisce la relazione di equivalenza:

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

Nell'insieme quoziente di questa relazione si definiscono poi le due operazioni tra classi di equivalenza.

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

$$[(a, b)] \cdot [(c, d)] = [(ac, bd)]$$

che sono operazioni interne e definite in F e danno ad esso la struttura di campo. All'interno di F gli elementi del tipo $[(a, 1)]$ rappresentano gli elementi di D, ovvero l'insieme $D^* = \{[(a, 1)] \text{ t.c. } a \in D\} \subset F$ è una copia isomorfa di D. L'elemento di F costituito dalla classe di equivalenza $[(a, b)]$ di una coppia (a, b) viene anche indicato col simbolo di frazione a/b. Possiamo dunque mappare ogni elemento di D a un elemento di F grazie alla seguente mappa di inclusione (iniettiva per definizione):

$$\phi : D \to F$$

$$a \mapsto \frac{1_D a}{1_D}$$

Si nota dalla definizione del campo dei quozienti che questa mappa è è un omomorfismo. Spesso questo tipo di mappa si indica $D \hookrightarrow F$ e viene chiamata 'embedding'.

11 Teoria dei Campi

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 moltilicativo. Di solito indichiamo un campo con K o L.

Esempio: (1.2)
$K = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_p$ dove p è un numero primo. Se $n = ab$ con $a, b > 1$ allora $\mathbb{Z}_n$ non è un campo perchè $[a][b] = [ab] = 0$.

Un omomorfismo di campi $f : K \to L$ è un caso particolare si un omomorfismo di anelli commutativi con identità, in altre parole:

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1_K) = 1_L$$

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 $x = x - y \neq 0$ 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.

Pertanto un omomorfismo di campi suriettivo è un isomorfismo.

Definizione: (1.4)
Sia L un campo. Allora un sottoinsieme $K \subseteq L$ si chiama un sottocampo se $1 \in K$ e K è chiuso rispetto all'addizione, la moltiplicazione, l'inverso additivo e all'inversione moltiplicativa si 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 e l'immagine dello spazio vettoriale attraverso una mappa lineare è un sottospazio.

Proposizione: (1.6)
(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.

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.

Esempio: (1.8)
$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} = \{a + b\sqrt{2} \text{ t.c. } a, b \in \mathbb{Q}\}$ La chiusura rispetto ad addizione sottrazione e moltiplicazione è chiara. Per la divisione usiamo un trucco dalla costruzione dei numeri complessi.

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{(ac + 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2}$$

Possiamo usare questo trucco anche al contrario: Supponiamo che $x^2 + 1 = 0$ non abbia soluzioni del campo K. Siano $e = (1, 0)$ e $f = (1, 0)$ 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

$$(ae + bf)(ce + df) = (ac - bd)e + (ad + bc)f$$

Allora, $e = 1_L$ e

$$\frac{ae+bf}{ce+df} = \frac{(ae+bf)(ce+df)}{(ce+df)(ce-df)} = \frac{(ae+bf)(ce+df)}{(c^2+d^2)e} = \frac{(ae+bf)(ce+df)}{(c^2+d^2)}$$

Se $(c,d) \neq (0,0)$, allora $c^2 + d^2 = 0$ da una soluzione a $x^2 + 1$ 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: (1.9)
$x^2 + 1 = 0$ non ha una soluzione in $\mathbb{Z}^{\nvDash}$. Quindi, possiamo costruire $\mathbb{Z}_3(\sqrt{-1})$.

L'intersezione di tutti i sottocampi di K è anch'essa un campo, che viene chiamato il sottocampo $\mathbb{F}$ 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.

Dimostrazione:
Definiamo la seguente mappa:

$$\phi : \mathbb{Z} \to \mathbb{F}$$

$$n \mapsto n \cdot 1_K$$

Si può dimostrare che ϕ è un omomorfismo:

$$\phi(n_1 + n_2) = (n_1 + n_2)1_K = n_1 \cdot 1_K + n_2 \cdot 1_K = \phi(n_1) + \phi(n_2)$$

$$\phi(n_1 \cdot n_2) = n_1 \cdot n_2 \cdot 1_K = n_1 \cdot 1_K \cdot n_2 \cdot 1_K = \phi(n_1) \cdot \phi(n_2)$$

- $\mathit{Char}K = 0$: Dato $n \in \mathit{ker}(\phi) \implies n \cdot 1_K = 0 \implies n = 0$ siccome la caratteristica è 0. Dunque $\mathit{ker}(\phi) = \{0\}$ e ϕ è iniettiva. Questo significa che ϕ è un embedding.

  $$\mathbb{Z} \cong \phi(\mathbb{Z}) \subseteq \mathbb{F}$$

  Siccome $\mathbb{Z}$ è un dominio integrale anche $\phi(\mathbb{Z})$ è un dominio integrale. Poniamo $\mathit{Frac}(\phi(\mathbb{Z}))$ il campo dei quozienti in cui è incluso $\phi(\mathbb{Z})$ tramite l'embedding visto prima. A questo punto è chiaro che $\mathit{Frac}(\phi(\mathbb{Z})) \cong \mathbb{Q}$.

  $$\mathit{Frac}(\phi(\mathbb{Z})) \cong \mathbb{Q} \subseteq \mathbb{F} \subseteq K$$

  Ma $\mathbb{F}$ è il sottocampo primo di K dunque $\mathbb{F} \subseteq \mathbb{Q} \implies \mathbb{Q} \cong \mathbb{F}$.

- $\mathit{Char}K = p$: Controlliamo un'altra volta il kernel di ϕ in caratteristica p. Si nota che il kernel è proprio l'ideale $\langle p \rangle$. Inoltre per quanto visto precedentemente $\mathbb{Z}/p\mathbb{Z}$ è un campo in quanto $p\mathbb{Z}$ è un ideale massimale. A questo punto si usa il teorema fondamentale per gli omomorfismi che è valido come visto precedentemente anche per gli anelli. Dunque $\phi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ ed è un campo. Ma come prima $\mathbb{F}$ è il sottocampo più piccolo di K dunque $\mathbb{F} \cong \phi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$.

Se il campo primo di K è $\mathbb{Z}_p$, diciamo che K ha caratteristica p ($\mathit{char}(K) = p$). Altrimenti, diciamo che K ha caratteristica zero ($\mathit{char}(K) = 0$).

11.1 Estensioni finite

Sia K un campo. Allora uno spazio vettoriale sul campo K è un insieme V dotato di due operazioni, dette moltiplicazioni scalari

$$K \times V \to V, \quad (c,v) \mapsto cv$$

e addizione vettoriale

$$V \times V \to V, \quad (u,v) \mapsto u + v$$

che soddisfano tutti i soliti assiomi di uno spazio vettoriale sopo aver sostituito il solito insieme di scalare $\mathbb{R}$ è $\mathbb{C}$ 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 vettoriali 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

$$(f + g)(x) = f(x) + g(x), \quad (cf)(x) = cf(x)$$

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

$$(x, y) \in L \times L \mapsto (x + y)$$

$$(c, x) \in K \times L \mapsto cx$$

In questo caso diciamo che L è un estensione di K e scriviamo $[L : K]$.

Se K è un sottocampo di L, scriviamo $[L : K]$ per la dimensione du L come uno spazio vettoriale su K (potrebbe essere ∞). Diciamo che L è un'estensione finita di K se $[L : K]$ è finito.

Esempio: (2.4)
(i) $\mathbb{C}$ è un estensione di $\mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$.
(ii)$\mathbb{Z}_3(\sqrt{-1})$ è una estensione di $\mathbb{Z}_3$ e $[\mathbb{Z}_3(\sqrt{-1}) : \mathbb{Z}_3] = 2$ (iii)$\mathbb{R}$ è una estensione di $\mathbb{Q}$ e $[\mathbb{R} : \mathbb{Q}]$. Ciò deriva del 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 teorma 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

$$1, A, A^2, ..., A^{n^2}$$

non può essere linearmente indipendente, pochè 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 perdere di genralità possiamo assumere 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 $adj(M)M = det(M)I$ e quindi ponendo $M = tI - A$. Il resto della dimostrazione è algebra tra matrici.

Sia L un'estensione di campo di K. Allora, $\alpha \in L$ si dice essrere algebrico su K se esiste un polinomio non costante $f(\alpha)$ 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 sole che se $[L : K] = n$ allora $\{1, \alpha, ..., \alpha^n\}$ non può essere un insieme linearmente indipendente.

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 polinimio di grado strettamente inferiore che valuta zero su α.

Esempio: (2.9)
Se $\alpha \in K$ allora $m_\alpha(t) = t - \alpha$ e $K(\alpha) = K$. Un particolare, il polinomio minimo di 0 è t.

Supponuamo 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)
Sia $K \subseteq L \subseteq M$ 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:
Dato $L : K$ un estesnsione di campo tale che $[L : K] = m$ ovvero la dimensione dello spazio vettoriale L su K è m. Definiamo la base $\mathcal{B}' = \{x_1, ..., x_m\}$ di L su K. Nello stesso modo $M : L$ è un estensione finita dunque possiamo definire una base $\mathcal{B}'' = \{x_1, ..., x_n\}$ di M su L dove $n = [M : L]$. Ogni elemento di$\alpha \in M$ può essere espresso come

$$\alpha = \beta_1 y_1 + \cdots + \beta_n y_n, \quad \beta_i \in L$$

Allo stesso modo ogni elemento $\beta \in L$ può essere espresso come

$$\beta = \gamma_1 x_1 + \cdots + \gamma_m x_m, \quad \gamma_i \in K$$

Allora, possiamo scrivere $\alpha \in M$ come

$$\alpha = \sum_{i=1}^{n} \beta_i y_i = \sum_{i=1}^{n} \left(\sum_{i=1}^{m} \gamma_{ij} x_j \right) y_i = \sum_{i,j} \gamma_{ij} x_j y_i$$

Dunque $\{y_1x_1, ..., y_1x_m, ..., y_nx_1, ..., y_nx_m\}$ spanna M su K. Questa risulta essere una base $\mathcal{B}''$ per M su K se e solo se sono linearmente indipendenti. Se α è 0 allora $\beta_i = 0$ per ogni $i \in \{1, ..., n\}$ siccome $\mathcal{B}'$ era un insieme di elementi L.I. . allo stesso modo si fa per i β_i. Dunque $\mathcal{B}''$ risulta essere una base per M su K e perciò $[M : K] = mn = [M : L][L : K]$.

Esempio: (2.11)
Se $[M : K] = 4$ e $K \subseteq L \subseteq M$ 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 linearmenti indipendenti. Dunque la dimesnione si K e $k - finita$. In quanto tale, come uno spazio vettoriale, $K \cong \mathbb{F}^n$ e quindi $|K| = |\mathbb{F}^n| = p^n$.

Nota: (2.13) A meno di isomorfismo, c'è solo un campo di ordine p^n. L'idea della dimostrazione è che l'insieme di 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 da un modo per costruire il campo ottenuto unenfo le radici di $x^{p^{n-1}} - 1 = 0$ a $\mathbb{Z}_p$. I generatori di K^* sono detti elementi primitivi di K.

11.2 Polinomi e campi

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 significa che ogni elemento $f \in R[x]$ può essere scritto come

$$f(x) = a_n x^n + \cdots + a_o, \quad a_n, ..., a_0 \in R$$

La definizione del grado di un polinomio, termine di ordine massimo, e polinomio monico sono esattamente le stesse nel caso di $\mathbb{Q}[x]$ discusso nella lezione sui polinomi. La definizione formale è la seguente.

Definizione: (3.1)
Sia R^N l'insieme di tutte le funzioni $\mathbb{N} \to R$ dove $\mathbb{N} = \{0, 1, ...\}$. Dato $f \in R^N$ sia $supp(f) = \{x \in \mathbb{N}\}$. Allora, $R[x] = \{f \in R^N \text{ t.c. } |supp(f)| < \infty\}$. In notazione convenzionale,

$$f \in R^N \subset R^N \iff \sum_k f(k) x^k$$

dove la somma a destra ha solo un numero finito di termini.

Esempio: (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

$$\{1, x - r, (x - r)^2, ..., (x - r)^d\}$$

è una base di $P_d[x]$.

Ripetiamo il nostro avvertimento dalla lezione sugli anelli commutativi: Un polinomio $f \in R[x]$ definisce una funzione $ev_f : R \to R$ secondo la regola

$$ev_f(a) = f(a)$$

ma in generale il polinomio f contiene più informazioni di ev_f.

Nella lezione sui polinomi abbiamo lavorato si $\mathbb{Q}[x]$, si può notare però che possiamo sostituire $\mathbb{Q}$ con un campo arbitrario K fino a raggiungere il teorema della radici razionali. A quel punto, utilizzaimo davvero il fatto che gli elementi di $\mathbb{Q}$ sono frazioni intere p/q.

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) $r(x) \neq 0 \wedge deg(r) < deg(g)$.

Nello stesso modo siano $f, g \in K[x]$ due polinimi tali che $(f, g) \neq (0, 0)$ sia

$$T = \{af + bg \in K[x] - \{0\} \text{ t.c. } a, b \in K[x]\}$$

Lemma: (3.4)
T contiene un unico polinomio monico di grado minimo.

Lemma: (3.5)
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 $h \mid f$ e $h \mid g$.

Dimostrazione: (stessa della lezione sui polinomi) Se $f = 0$ allora h è l'unico polinomio monico che è un multiplco 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 f e g siano diversi da zero. Chiaramente

$$f, g \in K[x] \implies deg(h) \leq min(deg(f), deg(g)) \text{ dove } h \in T \text{ è } min(T)$$

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

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

Per la minimalità sul grado su h dobbiamo avere $r = 0 (\implies h \mid f)$. Simmetricamente $h \mid g$ (scambiando i ruoli di f e g).

Definizione: (3.6)
L'unico polinomio h di grado minimo in (3.4) si chiama massimo comun divisore $mcd(f, g)$ di f e g.

Per calcolare $mcd(f, g)$, usiamo l'algoritmo euclideo per $K[x]$:

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

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: (3.7)
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: (3.8)
(i) Un Polinomio di grado 1 è irriducibile. $deg(h) \geq 1$.
(ii) Se $f \in K[x] - \{0\}$ ha una radice $r \in K$ allora f è riducibile perchè $(x - r) \mid f$.
(iii)Sia $f \in K[x]$ un polinomio di grado 2. Allora, f è irriducibile se e solo se f non ha una radice $r \in K$.

Lemma: (3.9)
Siano $f, g \in K[x]$. Se f è irriducibile allore $mcd(f, g) = 1$ oppure $f \mid g$.

Dimostrazione:
Sia $m = mcd(f, g)$. Allora $m \mid f$ e quindi $f = mq$ per qualche $q \in K[x]$. Per definizione, poichè f è irriducibile, segue che o m o q ha grado 0, cioè o (i) $m = 1$ o (ii) $m = uf$ per qualche $u \in K^*$. Nel caso (i), $m = mcd(f, g) = 1$. Nel caso (ii), $m = mcd(f, g) = uf \mid g \implies f \mid g$.

Lemma: (3.10)
Sia $f \in K[x]$ irriducibile. Se $f \mid gh$ allora $f \mid g \vee f \mid h$.

Dimostrazione:
In base al lemma precedente, se f non divide g allora $mcd(f, g) = 1$. Pertanto, esistono $a, b \in K[x]$ tali che $1 = af + bg$ e quindi $h = afh + bgh$. Per ipotesi segue che $f \mid gh$ e $f \mid afh$ segue che $f \mid h$.

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

$$f(x) = p_1(x) \cdots p_r(x), \quad f(x) = q_1(x) \cdots q_s(x)$$

sono due fattorizzazioni in un prodotto di irriducibili allora (i) $r = s$ e (ii) esiste una permutazione σ di $\{1, ..., r\}$ e una collezioni di costanti non nulle c_j tali che.

$$q_j(x) = c_j p_{\sigma(j)(x)}, \quad j = 1, ..., r$$

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 visto precedentemente.

Corollario: (3.11)
Siano $f, g \in K[x]$ polinomi monici non costanti. Allora

$$fg = mcm(f, g)mcd(f, g)$$

Proposizione: (3.12)
Sia $f \in K[x]$ un polinomio di grado d. Allora f ha al più d radici distinte.

Dimostrazione:
Se r è una radice di f allora $(x - r) \mid f$. Se $r_1, ..., r_k$ sono radici, allora per la fattorizzazione unica abbiamo $(x - r_1) \cdots (x - r_k) \mid f \implies k \leq d$.

Torniamo ora alla nostra discussione sui polinomi minimi:

Lemma: (3.13)
Sia L un'estensione del campo K e sia $\alpha \in L$ un elemento algebrico. Allora, il polinomio minimo in $K[t]$ di α è irriducibile.

Dimostrazione:
Supponiamo che $m = fg$ dove f e g sono non costanti. Allora, poichè $K[t]$ è un dominio integrale, $0 = m(\alpha) = f(\alpha)g(\alpha) \implies f(\alpha) = 0 \vee g(\alpha) = 0$ che contraddice la minimalità del grado di m.

Lemma: (3.14)
Sia L un'estensione del campo K e $\alpha \in L$ 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:
Poichè m è il polinomio monico di grado minimo che annulla α, possiamo scrivere $f = qm + r$ dove o $r = 0$ oppure $deg(r) < deg(q)$. Valutando su 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. Poichè sia f che m sono monici, questo implica che $q = 1$.

Esempio: (3.15)
$x^3 - 2 \in \mathbb{Q}[x]$ annulla $\sqrt[3]{2}$ ed è irriducibile in $\mathbb{Q}[x]$. Pertanto $x^2 - 2$ è il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}[x]$.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 (3.16)

Se $\alpha \in L$ è algebrico su K con polinomio minimo m di grado d allora $\{1, \alpha, ..., \alpha^{d-1}\}$ 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 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.

Per continuare, dato $\alpha \in L$ che è algebrico su K con polinomio minimo m di grado d, sia

$$W = span_K(1, ..., \alpha^{d-1}\}$$

Allora W è un sottospazio K di L, e quindi W è chiuso rispetto ad addizione, sottrazione e moltiplicazione per scalari di K. Per vedere che W è chiuso rispetto alla moltiplicazioni (come sottinsieme 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

$$f_1 f_2 = qm + r, \quad r = 0 \vee deg(r) < d$$

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: Poichè $deg(f) < deg(m)$ e m è irriducibile, segue che $mcd(f, m) = 1$. Quindi per il teorema di bezout esistono $u, v \in K[x]$ tali che $u(t)f(t) + v(t)m(t) = 1$. Senza perdità di generalità, possiamo supporre che $deg(u) < deg(m)$ scrivendo $u = qm + r$ se $deg(u) \geq deg(m)$. Valutare questo in $t = \alpha$ da

$$1 = u(\alpha)f(\alpha) + v(\alpha)m(\alpha) = u(\alpha)f(\alpha)$$

In sintesi abbiamo dimostrato:

Proposizione: (3.17)
Sia $\alpha \in L$ algebirco su K con m polinimio minimo di grado d e $W = span(1, \alpha, ..., \alpha^{d-1})$. Quindi $K(\alpha) = W$.

Dimostrazione:
Per il paragrafo precedente, W è un sottocampo di L che contiene $\alpha \in K$. Pertanto $K(\alpha) \subseteq W$ perchè $K(\alpha)$ è il sottocampo più piccolo di L che contiene α e K. Per vedere che $W \subseteq K(\alpha)$ osserviamo che poichè $K(\alpha)$ è un campo che contiene K e α, deve contenere tutte le combinazioni $K-$*lineari* di $1, \alpha, \alpha^{d-1}$ in quanto campo.

Esempio:
Il polinomio minimo di $\alpha = \sqrt[3]{2}$ su $\mathbb{Q}[x]$ è $x^3 - 2$. Quindi

$$1 = (x+1)(x^2 - x + 1)/3 + (x^3 - 2)(-1/3) \implies$$

$$1 = (\alpha + 1)(\alpha^2 - \alpha + 1)/3 + (\alpha^3 - 2(-1/3) = (\alpha + 1)(\alpha^2 - \alpha + 1)/3$$

$$\implies \frac{1}{\alpha + 1} = (\alpha^2 - \alpha + 1)/3$$

Proposizione: (3.17)
Se α è algebrico su K e β è algebrico su K allora $\alpha + \beta$ è algebrico su K.

Dimostrazione:
Se α è algebrico su K allora $K(\alpha)$ è un estensione finita di grado uguale a $deg(m_\alpha) = a$. Allo stesso modo $K(\beta)$ è un estensione finita di grado uguale a $deg(m_\beta) = b$. Facciamo la seguente torre di estensioni $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K]$. L'estensione $K(\alpha) : K$ ha grado a, mentre

l'estensione $K(\alpha,\beta) : K(\alpha)$ avrà al massimo grado b in quanto il polinomio minimo si potrebbe spezzare su $K(\beta)$. Dunque $[K(\alpha,\beta) : K] = n < \infty$, Si nota che siccome è uno spazio vettoriale di dim n allora $\{1, \alpha+\beta, (\alpha+\beta)^2, ..., (\alpha+\beta)^n\}$ non può essere una base di elementi linearmenti indipendenti. Stesso ragionamento di può fare per $\alpha\beta$.

Esempio:
Si dimostri che $\mathbb{Q}(e^{\pi i/4}) = \mathbb{Q}(i, \sqrt{2})$.

Analizziamo il campo $\mathbb{Q}(e^{\pi i/4})$ esso contiene per definizione $e^{i\pi/4}$ che per il teorema di eulero è $cos(\pi/4)+ i(sin(\pi/4)) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. Che è una combinazione lineare di i e $\sqrt{2}$ perciò sta in $\mathbb{Q}(i, \sqrt{2})$. Siccome $\mathbb{Q}(e^{\pi i/4})$ è il più piccolo campo (estensione di $\mathbb{Q}$ contenente questo elemento allora sarà perforza un sottocampo di $\mathbb{Q}(i, \sqrt{2})$. A questo punto eleviamo al quadrato e al cubo $y = e^{i\pi/4}$. Si nota $y^2 = i$ e $y^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, perciò $y^3 - y = 2\frac{\sqrt{2}}{2} = \sqrt{2}$ e appartiene a $\mathbb{Q}(y)$ dunque $i, \sqrt{2} \in \mathbb{Q}(y)$. A questo punto si nota che $\mathbb{Q}(i, \sqrt{2})$ è il più piccolo campo (estensione di $\mathbb{Q}$ contenente $i, \sqrt{2}$ segue $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(e^{i\pi/4}) \implies \mathbb{Q}(e^{\pi i/4}) = \mathbb{Q}(i, \sqrt{2})$.

11.3 Esercizi

Esercizio 1
Verificare proposizione (1.6).

Dato un campo K definiamo un omomorfismo f tra K e L se e solo se:

$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1_k) = 1_L$$

Risulta chiaro che dati due elementi $\alpha = f(x)$ e $\beta = f(y) \in Im(f)$ allora $\alpha+\beta = f(x)+f(y) = f(x+y) \in Im(f)$ perciò è chiuso per l'addizione. Inoltre $\alpha\beta = f(x)f(y) = f(xy) \in Im(f)$ dunque è chiuso per la moltiplicazione. Per gli inversi invece dato k in K allora $k - k = 0 \implies f(k-k) = f(0_K) \implies f(k) + f(-k \in K) = f(0_K) = 0_L$ dunque $-k \in K$ allora $f(-k) \in Im(f)$ è inverso di $f(k)$. Dunque esiste sempre l'inverso additivo. Stesso ragionamento possiamo fare per l'inverso moltiplcativo infatti $kk^{-1} = 1_K \implies f(k)f(k^{-1}) = f(1_K) = 1_L$. Sappiamo che 0_L e 1_L sono in Im_f perchè f è un omomorfismo di anelli commutativi con identità, dunque $f(1_K) = 1_L$ e $f(0_K) = 0_L$. Abbiamo dunque dimostrato che $Im(f)$ è un sottocampo di L.

Esercizio 2
Dimostrare che se $x^2 + a$ non ha una soluzione del campo K allora possiamo costruire $K(\sqrt{-a})$ in analogia con $K(\sqrt{-1})$. Verificare che $x^2 + 2 = 0$ non ha soluzione in $\mathbb{Z}_[5]$ e quindi abbiamo $\mathbb{Z}_5(\sqrt{-2})$. Spiega perchè $x^2 + 1$ non ha soluzioni mod p quando p è congruente a 3 mod 4.

(i) Allora costruiamo un estensione di K, ossia uno spazio vettoriale L generato dalla base $\mathcal{B} = \{1, \sqrt{-a}\}$ in quanto linearmente indipendenti. Si osserva che ogni elemento in L è generato dallo $span_K(\mathcal{B})$ in particolare siccome 0_K e 1_K appartengono a K per definizione allora $\sqrt{a} = (0_K)1 + \sqrt{-a}(1_K)$ e dunque $\sqrt{-a} \in L$.

(ii) $x^2 + [2] = 0 \implies x^2 = [3]$ basta controllare calcolando i residui quadratici in $\mathbb{Z}_5$

$$\begin{array}{c|ccccc} [x] & 0 & 1 & 2 & 3 & 4 \\ [x]^2 & 0 & 1 & 4 & 4 & 1 \end{array}$$

[3] non è un residuo quadratico dunque l'equazione non ha soluzione. Allo stesso modo possiamo costruire $\mathbb{Z}_5(\sqrt{-2})$ in analogia con quanto fatto prima.

(iii) Usare Reciprocità Quadratica di Gauss.

Esercizio 3

Supponiamo che $M : K$ sia un'estensione di campo tale che $[M : K]$ è un numero pirmo p. Esiste un campo intermedio L tra K e M in altre parole $K \subseteq L \subseteq M$?.

Se esiste un estensione intermedia L, allora $M \subseteq L \subseteq K$ è una torre di campi. Perciò per la legge delle torri i gradi $[L : K]$ e $[M : L]$ devono dividere p. Dunque o $[L : K] = 1$ e $[M : L] = p$ o $[L : K] = p$ e $[M : L] = 1$. Perciò L e M coincidono. Dunque non esiste un estensione intermedia L.

Esercizio 4
Mostra che se $f : L \to L$ è un omomorfismo allora

$$K = \{x \in L \text{ t.c. } f(x) = x\}$$

è un sottocampo di L.

L'elemento 0_L e l'elemento 1_L sono punti fissi per un omomorfismo tra campi dunque appartengono a K. Inoltre se $f(x + y) = f(x) + f(y)$ e se x e y sono punti fissi allora $f(x + y) = x + y$ che rende $x + y$ un punto fisso. Si dimostra simmetricamente per la chiusura sulla moltiplicazione. Per gli inversi si osserva dato x punto fisso allora $f(x - x) = f(x) + f(-x) = x + f(-x) = 0_L$ perciò $-x$ deve essre un punto fisso. Si dimostra simmetricamente per l'inverso moltiplcativo.

Esercizio 5
Dimostrare che se R è un dominio integrale e $|R|$ è finito allora R è un campo.

Si nota che R^* è finito in quanto R è finito. A questo punto di nota la mappa:

$$f : R^* \to R^*$$

$$x \mapsto ax, \quad \text{con } a \in R^*$$

Se questa mappa fosse suriettiva allora vuol dire che esiste un $\hat{x} \in R$ che è inverso moltiplicativo in quanto $a\hat{x} = 1$. Abbiamo dimostrato (Esercizi anelli e domini integrali) che questa mappa è una bigezione perciò è anche suriettiva. Dunque ogni elemento non zero ha un inverso moltiplicativo ergo R è un campo.

Esercizio 6
(i) Dato il campo $L = \mathbb{Z}_3(\sqrt{-1})$ estensione semplice di $\mathbb{Z}_3$ e $f : K \to K$ definita da $f(x) = x^3$, si trovino in punti fissi di f.

$(0 + i)^3$	$2i$
$(0 + 2i)^3$	i
$(1 + i)^3$	$1 + 2i$
$(1 + 2i)^3$	$2 + 2i$
$(2 + i)^3$	$1 + i$
$(2 + 2i)^3$	$2 + i$
$(0 + 0i)^3$	0
$(1 + 0i)^3$	1
$(2 + 0i)^3$	2

Dunque 0, 1 e 2 sono punti fissi per la mappa f. L'insieme di tutti gli automorfismi che mantegono fissi gli elementi in K in un estensione $L : K$ è in realtà un gruppo sotto la composizione di funzioni che si denota $Gal(L/K)$

(ii) Mostra che, in generale, se K ha caratteristica p allora $f(x) = x^p$ è un omomorfismo di campi.

Si nota subito che gli elementi 0_K e 1_K sono punti fissi. Dunque rimane da dimostrare le due proprietà per l'omomorfismo tra campi.
(i) $f(ab) = (ab)^p = a^p b^p = f(a)f(b)$

(ii) $f(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$ inoltre, per un campo tale che $char(K) = p$, il coefficiente binomiale svanisce in quanto $p \mid \binom{p}{i}$ e $char(K) = p \implies 1 \cdot p = 0$. A questo punto basta notare che $a^p + b^p = f(a) + f(b)$.

Esercizio 7
Trova un polinomio monico $f(t) \in \mathbb{Q}(t)$ di grado 4 tale che $f(\sqrt{2} + \sqrt{3})$, dimostra poi che f è irriducibile.

(i) Sappiamo che $x^2 - 2 = 0$ e $x^2 - 3 = 0$ sono i polinomi minimi per $\sqrt{2}$ e $\sqrt{3}$ rispettivamente. Supponiamo che $m(\sqrt{3})$ sia lo stesso polinomio per l'estensione $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})$. Dunque $(x - \sqrt{2})^2 - 3$ è il polinomio minimo $(x^2 - 2\sqrt{2}x - 1)(x^2 + 2\sqrt{2}x - 1) = x^4 + 2\sqrt{2}x^3 - x^2 - 2\sqrt{2}x^3 - 8x^2 + 2\sqrt{2}x - x^2 - 2\sqrt{2}x + 1 = x^4 - 10x^2 + 1$.
(ii) A questo punto basta osservare per il teorema delle radici razionali che l'unica radice razionale possibile sarebbe 1 ma 1 non è nel $ker(ev_f)$ dunque f è irriducibile in $\mathbb{Q}$.