Appunti di Aritmetica

Dalle lezioni dei proff.
Roberto Dvornicich e Massimo Caboara

Simone Cappellini

A.a. 2014/2015

27 agosto 2015

http://poisson.phc.unipi.it/~cappellini

Indice

Capitolo 1

Preliminari

NOTAZIONE: Useremo i seguenti simboli per indicare gli insiemi numerici:
$\mathbb{N}$ per i numeri naturali;
$\mathbb{Z}$ per i numeri interi;
$\mathbb{Q}$ per i numeri razionali;
$\mathbb{R}$ per i numeri reali;
$\mathbb{C}$ per i numeri complessi.

1.1 Operazioni

OPERAZIONE BINARIA: Un'operazione binaria in un insieme X è una funzione $\begin{array}{rccc} f: & X \times X & \longrightarrow & X \\ & (x,y) & \longmapsto & f(x,y) \end{array}$.

PROPRIETÀ DELLE OPERAZIONI:

- **Addizione**:

  Associativa $(x+y)+z = x+(y+z)$
  Commutativa $x+y = y+x$
  Esistenza dell'elemento neutro (zero) $x+0 = x$
  Esistenza dell'elemento opposto y tale che $x+y = 0$

  L'esistenza dell'opposto in $\mathbb{N}$ c'è solo per $x = 0$, in $\mathbb{Z}$ vale sempre.

- **Moltiplicazione**:

  Associativa $(xy)\,z = x\,(yz)$
  Commutativa $xy = yx$
  Esistenza dell'elemento neutro (uno) $x \cdot 1 = x$
  Esistenza dell'elemento opposto y tale che $xy = 1$

L'esistenza dell'opposto in $\mathbb{N}$ c'è solo per $x = 1$, in $\mathbb{Z}$ vale solamente per $x = \pm 1$, in $\mathbb{Q}$ vale $\forall\ x \neq 0$.

- **Addizione e Moltiplicazione**:

$$\text{Distributiva} \qquad \begin{array}{l} x\,(y+z) = xy + xz \\ (x+y)\,z = xz + yz \end{array}$$

Relazione d'Ordine: $x \leq y$ è una relazione che ha 3 particolari proprietà: è *riflessiva* ($x \leq x$), *transitiva* ($x \leq y$ e $y \leq z \Rightarrow x \leq z$) e *antisimmetrica* (ad eccezione di $x = y$).

- **Operazioni e Relazioni d'Ordine**:

$$\begin{array}{l} x \leq y \quad \Rightarrow \quad x + z \leq y + z \\ x \leq y \quad \Rightarrow \quad xz \leq yz \quad (\text{con } z > 0) \\ x \leq x' \text{ e } y \leq y' \quad \Rightarrow \quad x + y \leq x' + y' \quad (x + y \leq x' + y \leq x' + y') \end{array}$$

Capitolo 2

Induzione

2.1 Principio di Buon Ordinamento e Principio di Induzione

Assioma (Principio) di Buon Ordinamento: Ogni sottoinsieme $S \neq \emptyset \ \wedge \ S \subseteq \mathbb{N}$ possiede un elemento minimo, cioè un elemento $m \in S$ tale che $m \leq x \ \forall x \in S$.

Principio (Assioma) di Induzione: Sia $S \subseteq \mathbb{N}$ tale che:

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

Allora $S = \mathbb{N}$.

Osservazione. È possibile dimostrare sia il principio di induzione (PDI) assumendo la verità dell'assioma di buon ordinamento (PBO), sia il contrario. I due enunciati sono pertanto equivalenti.

$PBO \Rightarrow PDI$:

Dimostrazione. Supponiamo per assurdo che $S \neq \mathbb{N}$. Allora $\exists \ T \subseteq \mathbb{N}$ tale che $S \cap T = \emptyset \ \wedge \ S \cup T = \mathbb{N}$. Dunque $S \neq \mathbb{N} \Leftrightarrow T \neq \emptyset$. Quindi per il PBO T possiede un minimo m:
se $m = 0$: $0 \in S \ \wedge \ 0 \in T$, ma $S \cap T = \emptyset$. Assurdo.
se $m \neq 0$: $m \in T \Rightarrow m-1 \in S$, ma $m-1 \in S \Rightarrow m \in S$. Assurdo.
□

$PDI \Rightarrow PBO$:

Dimostrazione. Sia $S \subseteq \mathbb{N}$ che non possiede minimo. Dimostriamo quindi attraverso il PDI che è vuoto. Prendiamo $T \subseteq \mathbb{N}$ tale che $S \cap T = \emptyset \ \wedge$

$S \cup T = \mathbb{N}$.
Passo base: $0 \in T$; se così non fosse allora $0 \in S$ e sarebbe il minimo (poiché 0 è il minimo dell'insieme dei naturali).
Passo induttivo: Se T contiene tutti i numeri da 0 a n, allora deve contenere anche $n+1$; se così non fosse S conterrebbe $n+1$ ma nessuno degli elementi minori di esso, e sarebbe quindi il minimo di S.
Allora $T = \mathbb{N}$, cioè $S = \emptyset$. □

2.2 Applicazione di Induzione

Successione di Fibonacci: Può essere definita induttivamente oppure attraverso una formula esplicita:

$$\begin{cases} F(0) = 0 \\ F(1) = 1 \\ F(n+1) = F(n) + F(n-1) \qquad \text{per } n > 0 \end{cases}$$

$$F(n) = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

Le due definizioni sono equivalenti:

Dimostrazione. Verifichiamo per induzione che la formula esplicita definisce la stessa successione.

- $n = 0 \quad \Rightarrow \quad F(0) = \frac{1}{\sqrt{5}} [1 - 1] = 0$
- $n = 1 \quad \Rightarrow \quad F(1) = \frac{1}{\sqrt{5}} \left[\frac{1+\sqrt{5}-1+\sqrt{5}}{2} \right] = 1$

Sia $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$. Allora α e β sono le radici del polinomio $(x-\alpha)(x-\beta) = x^2 - x - 1$. Dunque abbiamo le relazioni $\alpha^2 = \alpha + 1$ e $\beta^2 = \beta + 1$.

$$\begin{aligned} F(n+1) &= F(n) + F(n-1) = \tfrac{1}{\sqrt{5}} (\alpha^n - \beta^n) + \tfrac{1}{\sqrt{5}} (\alpha^{n-1} - \beta^{n-1}) = \\ &= \tfrac{1}{\sqrt{5}} \left[(\alpha^n + \alpha^{n-1}) - (\beta^n + \beta^{n-1}) \right] = \tfrac{1}{\sqrt{5}} (\alpha^{n+1} - \beta^{n+1}) \end{aligned}$$

□

Osservazione. Da ora in poi ometteremo il passo base nelle dimostrazioni per induzione in caso di banale verifica.

Qui in seguito alcune delle numerose identità dimostrabili attraverso l'Induzione utili da sapere:

$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right)$

$x^{2n+1} + y^{2n+1} = (x+y)\left(x^{2n} - x^{2n-1}y + \cdots - xy^{2n-1} + y^{2n}\right)$

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

$\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2 = \frac{n^2(n+1)^2}{4}$

$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i$ [Teorema del Binomio di Newton]

$(x+y+z)^n = \sum_{i+j+k=n} \binom{n}{i,j,k} x^i y^j z^k$ e così via per ogni potenza n-esima di un m-onio

$\forall h \in \mathbb{R} \setminus \{1\} \quad \sum_{i=0}^{n} h^i = \frac{1-h^{n+1}}{1-h}$

2.3 Teorema Fondamentale dell'Aritmetica

Teorema Fondamentale dell'Aritmetica: Ogni numero naturale ($n > 0$) si scrive in modo unico come prodotto di numeri primi, a meno dell'ordine.

Osservazione. Per $n = 1$ convenzionalmente si ha un prodotto vuoto, cioè di 0 primi.

Dimostrazione. Esistenza. Usiamo l'induzione forte.
Ogni naturale $k = 1 \ldots n$ può essere scritto come prodotto di primi. Considero $n+1$: se $n+1$ è un numero primo non c'è nulla da dimostrare; altrimenti, esiste $a \,|\, n+1 \;\; a \in \mathbb{N}\; a \neq 1\; a \neq n+1$ ed esiste $b \in \mathbb{N}$ tali che $n+1 = ab$.
$a, b \leq n \Rightarrow a = p_1 p_2 \cdots p_k$ e $b = q_1 q_2 \cdots q_h \;\Rightarrow n+1 = ab = p_1 \cdots p_k q_1 \cdots q_h$ prodotto di primi. □

Dimostrazione. Unicità. Tramite induzione forte.
Siano $\begin{matrix} n = p_1 \cdots p_k \\ n = q_1 \cdots q_h \end{matrix}$ due fattorizzazioni in primi di n.
$\Rightarrow p_1 \cdots p_k = q_1 \cdots q_h$. Dunque, poiché $p_1 \,|\, p_1 \cdots p_k$, allora $p_1 \,|\, q_1 \cdots q_h \;\Rightarrow$ $p_1 \,|\, q_1 \vee \cdots \vee p_1 \,|\, q_h$.
Ma essendo tutti primi, si ha che $p_1 = q_1 \vee \cdots \vee p_1 = q_h$. Senza perdita di generalità possiamo suporre $p_1 = q_1$. Possiamo quindi semplificare nell'u-

guaglianza iniziale ed applicare l'ipotesi induttiva:

$$n > \frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_h \Rightarrow \begin{array}{l} p_2 = q_2 \\ \vdots \\ p_k = q_h \end{array} .$$

□

Capitolo 3

Calcolo Combinatorio

3.1 Cardinalità di Insiemi

Siano A, B insiemi e sia $|A| = k$ e $|B| = n$.
$A = \{a_1, a_2, \ldots, a_k\} \quad B = \{b_1, b_2, \ldots, b_n\}$

Quante sono le diverse funzioni $f : A \to B$?

$$\begin{array}{cccc} a_1 \mapsto b_1 & a_2 \mapsto b_1 & \ldots & a_k \mapsto b_1 \\ a_1 \mapsto b_2 & a_2 \mapsto b_2 & \ldots & a_k \mapsto b_2 \\ \vdots & \vdots & \vdots & \vdots \\ n \text{ scelte} & n \text{ scelte} & \ldots & n \text{ scelte} \end{array} \quad = n^k \text{ diverse funzioni}$$

Quante sono le funzioni *iniettive* $f : A \hookrightarrow B$?

$$\left.\begin{array}{ll} a_1 \mapsto b_1, \ldots, b_n & n \text{ scelte} \\ a_2 \mapsto b_{i_1}, \ldots, b_{i_{n-1}} & n-1 \text{ scelte} \\ \vdots & \ldots \\ a_k \mapsto b_{i_1}, \ldots, b_{i_{n-k+1}} & n-k+1 \text{ scelte} \end{array}\right\} \Rightarrow \begin{array}{ll} = \frac{n!}{(n-k)!} & \text{se } n \geq k \\ = 0 & \text{se } n < k \end{array}$$

Quante sono le funzioni *bigettive* $f : B \leftrightarrow B$?

$$\left.\begin{array}{ll} a_1 \mapsto b_1, \ldots, b_n & n \text{ scelte} \\ a_2 \mapsto b_{i_1}, \ldots, b_{i_{n-1}} & n-1 \text{ scelte} \\ \vdots & \ldots \\ a_k \mapsto b_{i_1} & 1 \text{ scelta} \end{array}\right\} \Rightarrow \quad = n!$$

Quanti sono i possibili sottoinsiemi $X \subseteq B$ tali che $|X| = k$, con

$0 \leq k \leq n$**?**

$$X = \{x_1, x_2, x_3, \ldots, x_k\} \quad \begin{array}{l} n \text{ scelte per } x_1 \\ n-1 \text{ scelte per } x_2 \\ n-2 \text{ scelte per } x_3 \\ \vdots \\ n-k+1 \text{ scelte per } x_k \end{array}$$

Ogni diverso sottoinsieme però viene contato $k!$ volte, una per ogni diverso ordinamento delle scelte di $x_1, \ldots, x_k$. Dunque il numero totale di sottoinsiemi di cardinalità k di un insieme di n elementi è

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

Quanti sono i sottoinsiemi $X \subseteq B$**?**

Il numero totale dei sottoinsiemi di un insieme di cardinalità n è 2^n.

Dimostrazione. 1. Induzione.
Passo induttivo: $|B| = n$, poniamo $Y = B \cup \{b_{n+1}\}$. Dobbiamo trovare il numero degli $X \subseteq Y$; $X = (X \cap B) \cup (X \cap \{b_{n+1}\})$.
L'elemento b_{n+1} può stare o meno nel sottoinsieme X (2 scelte); $X \cap B$ dà luogo a 2^n diversi sottoinsiemi (per ipotesi induttiva). Quindi $|\mathcal{P}(Y)| = 2 \cdot 2^n = 2^{n+1}$. □

Dimostrazione. 2. Diretta.
Esiste una corrispondenza biunivoca tra l'insieme $\mathcal{P}(B)$ e l'insieme F delle funzioni $f : B \to \{0, 1\}$ (chiamata funzione caratteristica di un sottoinsieme). Dimostriamo che $\begin{array}{rccc} \Phi: & \mathcal{P}(B) & \to & F \\ & X & \mapsto & f_X \end{array}$ è bigettiva.
Iniettività: $f_X = f_Y \Rightarrow f_X(x) = f_Y(x) \forall x \in B$, ovvero $f_X(x) = 1 \Leftrightarrow f_Y(x) = 1$, cioè $x \in X \Leftrightarrow x \in Y$. $\Rightarrow X = Y$
Surgettività: $\forall f \in F \; \exists \, A \subseteq B$ tale che $f_A = f$. Infatti $A = \{x \in B \mid f(x) = 1\} = f^{-1}(\{1\})$
Poiché $|F| = 2^n$, segue la tesi. □

Dimostrazione. 3.
Dal risultato precedente si ottiene che $|\mathcal{P}(B)| = \binom{n}{0} + \cdots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}$
Dal teorema del binomio di Newton, ponendo $x = y = 1$ si ha che $(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} = 2^n$. Tesi. □

Quante sono le soluzioni dell'equazione $x_1 \cdots + x_k = n$ **con** $x_1, \ldots, x_k \in \mathbb{N} \setminus \{0\}$**?**

Consideriamo le somme parziali:

$$\begin{aligned} S_1 &= x_1 \\ S_2 &= x_1 + x_2 \\ &\vdots \\ S_k &= x_1 + \cdots + x_k = n \end{aligned}$$

$0 < S_1 < \cdots < S_k = n$. Poiché c'è una corrispondenza biunivoca tra le somme parziali e le soluzioni, basta scegliere $k-1$ numeri tra 1 e $n-1$, e ciò è possibile in $\binom{n-1}{k-1}$ modi.

Quante sono le soluzioni della disuguaglianza $x_1 + \cdots + x_k \leq n$ con $x_1, \ldots, x_k \in \mathbb{N} \setminus \{0\}$?

Analogamente a sopra, consideriamo $0 < S_1 < \cdots < S_k \leq n$. In questo caso l'obiettivo è scegliere k numeri compresi tra 1 e n, per un totale di $\binom{n}{k}$ soluzioni.

Quante sono le soluzioni dell'equazione $x_1 + \cdots + x_k = n$ con $x_1, \ldots, x_k \in \mathbb{N}$?

Ci riconduciamo ad un problema precedente aggiungendo k in entrambi i membri:

$$(x_1 + 1) + \cdots + (x_k + 1) = n + k$$

A questo punto si tratta di scegliere $k-1$ numeri tra 1 e $n+k-1$, per un totale di $\binom{n+k-1}{k-1}$ diverse soluzioni.

3.2 Principio di Inclusione-Esclusione

Principio di Inclusione-Eslusione: Serve a calcolare la cardinalità dell'unione di insiemi non disgiunti.

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| = \quad & |A_1| + \cdots + |A_n| - |A_1 \cap A_2| - |A_1 \cap A_3| - \ldots \\ & - |A_{n-1} \cap A_n| + \cdots - \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n| \end{aligned}$$

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{\{i_1,\ldots,i_k\} \subseteq \{1,2,\ldots,n\}} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|$$

Dimostrazione. La formula è corretta se ogni elemento dell'unione viene contato esattamente 1 volta.

Se $x \in$ *unione*, supponiamo che $x \in k$ insiemi ($1 \leq k \leq n\ k \in \mathbb{N}$). Senza perdita di generalità possiamo supporre che $x \in A_1, \ldots, A_k$ e $x \notin A_{k+1}, \ldots, A_n$.

$$\begin{array}{ll} |A_1| + |A_2| + \ldots & x \text{ contato } \binom{k}{1} \text{ volte} \\ -|A_1 \cap A_2| - \ldots & x \text{ contato } \binom{k}{2} \text{ volte} \quad \text{(coppie di 2 insiemi su k)} \\ \vdots & \vdots \end{array}$$

In totale vogliamo che

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \cdots + (-1)^{k-1} \binom{k}{k} \stackrel{?}{=} 1$$

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \binom{k}{4} + \cdots + (-1)^{k} \binom{k}{k} \stackrel{?}{=} 0$$

$$\binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \binom{k}{4} + \cdots + (-1)^{k} \binom{k}{k} \stackrel{?}{=} 0$$

Prendo $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ e pongo $a = -1$ e $b = 1 \Rightarrow 0^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ □

Quante sono le funzioni *surgettive* $f : A \to B$?

Siano $A_i := \{f : A \to B \mid b_i \notin \mathcal{I}m\ f\}$. Contare le funzioni surgettive significa contare la cardinalità del complementare di $\bigcup_{i=1}^{n} A_i$.

$$\begin{aligned} n^k - \left| \bigcup_{i=1}^{n} A_i \right| &= n^k - \sum_{i=1}^{n} (-1)^{i+1} \sum_{1 \leq j_1 < \cdots < j_i \leq n} |A_{j_1} \cap \ldots A_{j_i}| \\ &= n^k - \sum_{i=1}^{n} (-1)^{i+1} \sum_{1 \leq j_1 < \cdots < j_i \leq n} (n-i)^k \\ &= n^k - \sum_{i=1}^{n} (-1)^{i+1} (n-i)^k \sum_{1 \leq j_1 < \cdots < j_i \leq n} 1 \\ &= n^k + \sum_{i=1}^{n} (-1)^{i} (n-i)^k \binom{n}{i} \\ &= \sum_{i=0}^{n} (-1)^{i} (n-i)^k \binom{n}{i} \end{aligned}$$

3.3 Permutazioni senza punti fissi

Sia $a_i := |\{f \in S_n \mid$ almeno i elementi sono fissi$\}| = \binom{n}{i} (n-i)!$.
Sia anche $A_s := \{f \in S_n \mid s$ è fisso$\}$.

Allora contare il numero di permutazioni di n elementi senza punti fissi equivale a trovare la cardinalità del complementare di $\bigcup_{s=1}^{n} A_s$.

$$\begin{aligned} n! - \left| \bigcup_{s=1}^{n} A_s \right| &= n! - \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le s_1 < \cdots < s_k \le n} |A_{s_1} \cap \cdots \cap A_{s_k}| \\ &= n! + \sum_{k=1}^{n} (-1)^k \, a_k = n! + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)! \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \end{aligned}$$

Capitolo 4

$\mathbb{Z}$: Gli Interi

4.1 Divisione Euclidea

PROPOSIZIONE: Dati $a, b \in \mathbb{Z}$, $b \neq 0$ esistono e sono unici due interi tali che:

- $a = qb + r$
- $0 \leq r < |b|$

Dimostrazione. Esistenza.
Consideriamo $A = \{a - qb \mid q \in \mathbb{Z}\}$. Vediamo adesso che $A \cap \mathbb{N} \neq \emptyset$.
Dobbiamo verificare che $\exists\ q \in \mathbb{Z}$ tale che $a - qb = r \geq 0$.

$$a \geq qb \Rightarrow \begin{cases} \text{se } b > 0 & q \leq \frac{a}{b} \\ \text{se } b < 0 & q \geq \frac{a}{b} \end{cases} \Rightarrow \exists \text{ infiniti } q \in \mathbb{Z}$$

Quindi $S = A \cap \mathbb{N}$ è un sottoinsieme non vuoto di $\mathbb{N}$. Chiamo $r = min\,\{S\}$.
$r \in S$, $r = a - qb$ per qualche $q \in \mathbb{Z}$, ovvero $a = qb + r$ (tesi 1).
Per dimostrare la seconda tesi supponiamo $r \geq |b|$.

- se $b > 0$, $r \geq b$. Aggiungo e sottraggo b:

  $$a = \underbrace{(q+1)}_{q'} b + \underbrace{(r-b)}_{r'}$$

  con $r > r - b = r' \geq 0$. Dunque $a - q'b = r' \Rightarrow r' \in S$. Assurdo.

- se $b < 0$, $r \geq -b$. Sottraggo e aggiungo b:

  $$a = \underbrace{(q-1)}_{q'} b + \underbrace{(r+b)}_{r'}$$

  con $r > r + b = r' \geq 0$. Dunque $a - q'b = r' \Rightarrow r' \in S$. Assurdo.

□

Dimostrazione. Unicità.
Supponiamo non siano unici. Allora $\begin{matrix} a = qb + r & 0 \leq r < |b| \\ a = q'b + r' & 0 \leq r' < |b| \end{matrix}$
Senza perdita di generalità possiamo supporre $r \geq r'$. Sottraggo le due equazioni membro a membro.

$$0 = (q - q')\, b + (r - r')$$

Mettiamo tutto sotto valore assoluto:

$$|q' - q| \cdot |b| = |r - r'|$$

$$0 \leq |r - r'| < |b| \qquad\qquad |q' - q| \cdot |b| = \begin{cases} 0 & \text{se } q' = q \\ \geq |b| & \text{se } q' \neq q \end{cases}$$

L'unica soluzione accettabile è quindi $q' = q$ e $r' = r$. □

Algoritmo di Euclide: Detto anche delle divisioni successive.
Dati a, b poniamo $a_1 = a$, $b_1 = b$ e $a_1 = q_1 b_1 + r_1$.
Attraverso la relazione $\begin{matrix} a_{i+1} = b_i \\ b_{i+1} = r_i \end{matrix}$ l'algoritmo prosegue, dati a_i e b_i, trovando q_i e r_i tramite $a_i = q_i b_i + r_i$ fino ad ottenere $r_k = 0$

Definizione: In $\mathbb{Z}$ esiste una relazione d'ordine data dalla divisibilità. Diciamo che a divide b (e si scrive $a \,|\, b$) se b è un multiplo di a, ovvero se

$$\exists\ k \in \mathbb{Z} \text{ tale che } b = ka$$

Definizione: Siano a, $b \in \mathbb{Z}$ non entrambi nulli. Un intero d si dice un *Massimo Comune Divisore* tra a e b se:

- $d \,|\, a$, $d \,|\, b$ (è un divisore comune)
- $\forall x \,|\, a \wedge x \,|\, b \Rightarrow x \,|\, d$

Per scrivere compattamente che d è l'MCD tra a e b si usa la seguente notazione: $(a, b) = d$.

Osservazione. Se $\exists MCD$, allora $d \neq 0$ (0 non divide nessun numero $\neq 0$).
Osservazione. Se d, d' sono 2 MCD, allora $d = \pm d'$.
Osservazione. Se d è un MCD, allora anche $-d$ lo è.
Osservazione. Quando parliamo DEL massimo comun divisore, si intende quello positivo.

Proposizione: $b_n = r_{n-1}$, ossia l'ultimo divisore o l'ultimo resto diverso da 0 è il MCD tra a_1 e b_1.

Dimostrazione. Ponendo $d = b_n = r_{n-1}$ l'ultima delle divisioni successive dice che $a_n = q_n b_n + 0 \Rightarrow b_n \,|a_n$, ovvero $d \,|a_n$, cioè $d \,|b_{n-1}$
Ma $d \,|r_{n-1}$ e $d \,|b_{n-1} \quad \Rightarrow d \,|a_{n-1}$.
Procedendo così a ritroso si arriva a $d \,|a_1$ e $d \,|b_1$ (induttivamente).
Prendiamo adesso un $x \in \mathbb{Z}$ tale che $x \,|a_1$, $x \,|b_1 \Rightarrow x \,|r_1$ Analogamente a sopra, induttivamente si giunge a $x \,|a_{n-1}$, $x \,|b_{n-1} \quad x \,|r_{n-1} = b_n = d$ □

PROPOSIZIONE: Se $(a, b) = d$ allora esistono degli interi s, t tali che

$$as + bt = d \qquad \text{[IDENTITÀ DI BÉZOUT]}$$

PROPOSIZIONE: Siano a, $b \in \mathbb{Z}$ non entrambi nulli e sia $d = (a, b)$. Allora l'insieme $X = \{ax + by \mid x, y \in \mathbb{Z}\}$ è costituito da tutti e soli i multipli di d.

Dimostrazione. Per la proposizione precedente esistono s, t tali che $as+bt = d$; dunque $d \in X$.
Prendiamo un multiplo di d. Allora

$$a\,(ks) + b\,(kt) = kd$$

Viceversa, supponiamo che $c \in X$, cioè $\exists x_0, y_0 \in \mathbb{Z}$ tali che $ax_0 + by_0 = c$.

$$\begin{array}{l} d \,|a \Rightarrow d \,|ax_0 \\ d \,|b \Rightarrow d \,|by_0 \end{array} \Rightarrow d \,|ax_0 + by_0 \Rightarrow d \,|c$$

□

PROPOSIZIONE: Se $a \,|bc$ e $(a, b) = 1$ allora $a \,|c$

Dimostrazione. Esistono s, $t \in \mathbb{Z}$ tali che $as + bt = 1$.
$a \,|bc \Rightarrow bc = au$ $u \in \mathbb{Z}$; moltiplicando per t e poi sommando asc ad entrambi i membri otteniamo

$$asc + btc = aut + asc$$

$$c\,(as + bt) = a\,(ut + sc)$$

$$c = a\,(ut + sc) \quad \Rightarrow a \,|c$$

□

PROPOSIZIONE: Sia p un numero primo. Allora vale la proprietà

$$p \,|ab \Rightarrow p \,|a \;\text{ oppure } p \,|b$$

Dimostrazione. Consideriamo (p, a):

$$(p, a) = \begin{cases} 1 \Rightarrow \text{PROP. precedente } p \,|b \\ p \Rightarrow p \,|a \end{cases}$$

□

Osservazione. Generalizzando: p primo e $n \geq 2$.

$$p \,|a_1 \cdots a_n \Rightarrow p \,|a_1 \text{ oppure } \ldots \text{ oppure } p \,|a_n$$

Dimostrazione. La dimostrazione è una semplice Induzione. □

PROPOSIZIONE: Se $a \,|c$, $b \,|c$ e $(a, b) = 1$ allora $ab \,|c$.

Dimostrazione. $a \,|c \Rightarrow \exists x \in \mathbb{Z}$ tale che $c = ax$ $b \,|c$, cioè $b \,|ax$. Ma $(a, b) = 1 \Rightarrow b \,|x$
Quindi $\exists y \in \mathbb{Z}$ tale che $x = by$. Sostituendo si ha $c = aby$, cioè $ab \,|c$. □

4.2 Equazioni Diofantee

$$ax + by = c$$

Un'equazione in una o più incognite a coefficienti interi in cui si cercano le soluzioni intere si dice diofantea.
L'equazione ha almeno una soluzione $\Leftrightarrow (a, b) \,|c$
Supponiamo la condizione verificata, e sia $d = (a, b)$. Scriviamo $a = a_1 d$, $b = b_1 d$, $c = c_1 d$ e semplifichiamo.

$$a_1 x + b_1 y = c_1$$

A questo punto $(a_1, b_1) = 1$, quindi è possibile trovare una soluzione particolare dell'equazione attraverso l'algoritmo di Euclide. Si cerca $\bar{x}$, $\bar{y}$ tali che

$$a_1 \bar{x} + b_1 \bar{y} = 1$$

$$a_1 (c_1 \bar{x}) + b_1 (c_1 \bar{y}) = c_1$$

Sia (x, y) una soluzione qualsiasi di $a_1 x + b_1 y = c_1$. Avendo già trovato una soluzione particolare, sottraendo membro a membro:

$$a_1 (x - c_1 \bar{x}) + b_1 (y - c_1 \bar{y}) = 0$$

$$a_1 (x - c_1 \bar{x}) = -b_1 (y - c_1 \bar{y})$$

$b_1 \,|(x - c_1 \bar{x})$, ovvero $\exists\ k \in \mathbb{Z}$ tale che $x - c_1 \bar{x} = b_1 k \ \Rightarrow\ x = c_1 \bar{x} + b_1 k$.
Risostituendo:

$$a_1 b_1 k = -b_1 (y - c_1 \bar{y})$$

- $b_1 \neq 0$: $a_1 k = c_1 \bar{y} - y \Rightarrow \quad y = c_1 \bar{y} - a_1 k$

$$\text{Le soluzioni sono } \begin{cases} x = c_1 \bar{x} + b_1 k \\ y = c_1 \bar{y} - a_1 k \end{cases} \ \forall\ k \in \mathbb{Z}$$

- $b_1 = 0$: $a_1 x = c_1$. Ma $(a_1, b_1) = (a_1, 0) = 1 \Rightarrow a_1 = 1$

$$\text{Le soluzioni sono } \begin{cases} x = c_1 \\ y = h \end{cases} \quad \forall\, h \in \mathbb{Z}$$

PROPOSIZIONE: Se $p \in \mathbb{N}$, $p > 1$ tale che $p \,|ab \Rightarrow p \,|a \wedge p \,|b$ allora p è primo.

Dimostrazione. Sia a un divisore di p. Posso scrivere $p = ab$. In particolare, $p \,|ab$. Per ipotesi $p \,|a \wedge p \,|b$.

- $p \,|a$: $\Rightarrow\ a = pa_1 \qquad p = pa_1 b \Rightarrow a_1 b = 1$.
  Allora $a_1 = b = \pm 1$, e quindi $a = \pm p$ e $b = \pm 1$.
- $p \,|b$: $\Rightarrow\ b = pb_1 \qquad p = apb_1 \Rightarrow ab_1 = 1$.
  Allora $a = b_1 = \pm 1$, e quindi $a = \pm 1$ e $b = \pm p$.

$\Rightarrow$ p è un intero positivo con unici divisori 1 e p. $\Rightarrow$ p è primo. □

DEFINIZIONE: Siano $a,\ b \in \mathbb{Z}$. Un intero m si dice un *minimo comune multiplo* tra a e b se:

- $a \,|m$, $b \,|m$ (è un multiplo comune)
- $\forall a \,|x \wedge b \,|x \Rightarrow m \,|x$

Per scrivere compattamente che m è l'*mcm* tra a e b si usa la seguente notazione: $[a, b] = m$.

PROPOSIZIONE: $(a, b)\,[a, b] = ab$.

Dimostrazione. Poniamo $d = (a, b)$
Va dimostrato che $\frac{ab}{d}$ è un *mcm*.

$$a = a_1 d, \quad b = b_1 d \quad \Rightarrow (a_1, b_1) = 1$$
$$\frac{ab}{d} = \frac{a_1 d b_1 d}{d} = a_1 b_1 d$$

Chiamiamo $m = a_1 b_1 d$ e verifichiamo che sia un *mcm*.

- $\begin{array}{lll} a \,|m\ , & a_1 d \,|a_1 b_1 d & \text{ok} \\ b \,|m\ , & b_1 d \,|a_1 b_1 d & \text{ok} \end{array}$
- Supponiamo che $a \,|x$ e $b \,|x$, cioè $a_1 d \,|x$ e $b_1 d \,|x$. $\Rightarrow$ $d \,|x$, e quindi possiamo scrivere $x = x_1 d$. $\Rightarrow$ $a_1 d \,|x_1 d$, ovvero $a_1 \,|x_1$ e analogamente $b_1 \,|x_1$
  $\Rightarrow\ a_1 b_1 \,|x_1 \quad \Rightarrow \quad \begin{array}{c} a_1 b_1 d \,|x_1 d \\ m \,|x \end{array}$

□

4.3 Piccolo Teorema di Fermat

Sia p primo, $a \in \mathbb{Z}$. Allora $p \,|a^p - a$

Dimostrazione. Dimostrazione in 2 passi.

- Supponiamo dapprima $a \geq 0$: per Induzione.

$$\begin{aligned}(a+1)^p - (a+1) &= \sum_{k=0}^{p} \binom{p}{k} a^k - (a+1) \\ &= \binom{p}{0} a^0 + \sum_{k=1}^{p-1} \binom{p}{k} a^k + \binom{p}{p} a^p - (a+1) \\ &= \underbrace{a^p - a}_{\text{ip. indutt.}} + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^k}_{\text{fattore } p \text{ al numeratore}} \\ &\Rightarrow p \,|(a+1)^p - (a+1)\end{aligned}$$

- $a < 0$: $\Rightarrow \;\; a = -b$ con $b \in \mathbb{N} \setminus \{0\}$.

$$a^p - a = (-b)^p + b = \begin{cases} p \neq 2 & -b^p + b = -\left(b^p - b\right) \quad \text{ok} \\ p = 2 & b^2 + b = \underbrace{\left(b^2 - b\right)}_{\text{dim. sopra}} + 2b \quad \text{ok} \end{cases}$$

□

4.4 d(n): Numero di Divisori di n

Definizione: Per $n > 1$, $d(n) = \sum_{d|n} 1$. La funzione conta cioè la quantità di divisori positivi di un numero.

Sia $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.
Un divisore d di n è del tipo $d = p_1^{\delta_1} \cdots p_k^{\delta_k}$, con $0 \leq \delta_i \leq \alpha_i \;\; \forall i$.
Il numero dei divisori positivi di n sarà quindi uguale al numero di scelte possibili per gli esponenti. Dunque

$$d(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$$

Osservazione. I divisori positivi di un numero sono dispari se e solo se il numero è un quadrato perfetto. Infatti è possibile accoppiare ogni divisore d con $\frac{n}{d}$ (che a sua volta è un divisore di n), con l'unica eccezione di $d = \sqrt{n}$, poiché in quel caso $d = \frac{n}{d}$ e quindi resta l'unico valore che non può essere accoppiato.

4.5 $\varphi(n)$: Funzione di Eulero

DEFINIZIONE: Per $n \geq 1$, $\varphi(n) = |\{1 \leq x \leq n \mid (x,n) = 1\}|$.

Calcolo di $\varphi(n)$:

- $n = p$ primo: $\varphi(p) = p - 1$.
- $n = p^k$ con p primo e $k \geq 1$: $\varphi(p^k) = p^k - p^{k-1}$.
- n generico: utilizzando il principio di Inclusione-Esclusione.
  $n = p_1^{k_1} \cdots p_s^{k_s}$ con $p_i \neq p_j \Leftrightarrow i \neq j$. Siano $A = \{1 \leq x \leq n \mid (x,n) = 1\}$, $B = \{1 \leq x \leq n \mid (x,n) > 1\}$ e $B_i = \{1 \leq x \leq n \mid p_i \mid x\}$.
  Ovviamente $|A| + |B| = n$ e $B = B_1 \cup B_2 \cup \cdots \cup B_s$.

$$\begin{aligned} |B| &= |B_1| + \cdots + |B_s| - |B_1 \cap B_2| - \cdots + (-1)^{s-1} |B_1 \cap \cdots \cap B_s| \\ &= \frac{n}{p_1} + \cdots + \frac{n}{p_s} - \left(\frac{n}{p_1 p_2} + \ldots\right) + \cdots + (-1)^{s-1} \frac{n}{p_1 p_2 \cdots p_s} \end{aligned}$$

$$\begin{aligned} |A| &= n - |B| \\ &= n\left[1 - \left(\frac{1}{p_1} + \cdots + \frac{1}{p_s}\right) + \left(\frac{1}{p_1 p_2} + \ldots\right) + \cdots + (-1)^s \frac{1}{p_1 p_2 \cdots p_s}\right] \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right) \\ &= \left(p_1^{k_1} - p_1^{k_1 - 1}\right)\left(p_2^{k_2} - p_2^{k_2 - 1}\right) \cdots \left(p_s^{k_s} - p_s^{k_s - 1}\right) \end{aligned}$$

Osservazione. Dall'ultima riscrittura è possibile notare che la funzione φ di Eulero sia una funzione moltiplicativa, cioè

$$\varphi(p^\alpha q^\beta) = \varphi(p^\alpha)\varphi(q^\beta) \text{ con } p \neq q$$

4.6 $\sigma(n)$: Somma dei Divisori di n

DEFINIZIONE: Per $n \geq 1$, $\sigma(n) = \sum_{d|n} d$. La funzione conta cioè la somma di tutti i divisori positivi di un naturale.

Calcolo di $\sigma(n)$:

- $n = p$ primo: $\sigma(p) = p + 1$.
- $n = p^k$ con p primo e $k \geq 1$: $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$
- n generico: poiché la σ è una funzione moltiplicativa, dato che

$$\sigma(n \cdot m) = \sum_{\substack{i = 1, \ldots, k \\ j = 1, \ldots, t}} n_i m_j = \sum_{i=1}^{k} n_i \sum_{j=1}^{t} m_j = \sigma(n)\sigma(m)$$

Dunque

$$\sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \prod_{i=1}^{k} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right)$$

Capitolo 5

Aritmetica Modulare

5.1 Prime Notazioni

DEFINIZIONE: Sia $n \geq 1$, $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$. Si dice che x *è congruo a* y *modulo* n e si scrive $x \equiv y \pmod{n}$ se $n \,|x - y$.
Si tratta di una relazione di equivalenza.

PROPOSIZIONE: Si dice che $x \equiv y \pmod{n}$ se e solo se x e y danno lo stesso resto nella divisione Euclidea per n.

Dimostrazione. $\Rightarrow$. Supponiamo $x \equiv y \pmod{n}$, cioè $n \,|x - y$.
$\begin{matrix} x = q_1 n + r_1 \\ y = q_2 n + r_2 \end{matrix}$ Possiamo supporre senza perdita di generalità $r_1 \geq r_2$.
Allora $x - y = (q_1 - q_2)\, n + (r_1 - r_2)$. $\Rightarrow \quad n \,|(r_1 - r_2)$ Ma $0 \leq r_1 - r_2 < n \;\Rightarrow\; r_1 = r_2$. □

Dimostrazione. $\Leftarrow$. Supponiamo $r_1 = r_2$.
$\begin{matrix} x = q_1 n + r_1 \\ y = q_2 n + r_2 \end{matrix} \Rightarrow\; x - y = (q_1 - q_2)\, n \quad \Rightarrow \quad n \,|x - y\,.$ □

COROLLARIO: Le classi di equivalenza sono in corrispondenza biunivoca con i resti. $\{0, 1, \ldots, n-1\}$

Intendendo con C_x la classe di equivalenza di x si ha che $\mathbb{Z} = C_0 \cup \cdots \cup C_{n-1}$.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_n = \{C_0, \ldots, C_{n-1}\} = \{\overline{0}, \ldots, \overline{n-1}\}$$

Introduciamo una funzione chiamata *proiezione canonica* $\begin{matrix} \Pi : \mathbb{Z} & \to \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto \overline{x} \end{matrix}$ che associa ad ogni intero un rappresentante della classe di equivalenza modulo n.

Osservazione. Sia $a \in \mathbb{Z}/n\mathbb{Z}$. a ha un inverso se e solo se $\exists\, x \in \mathbb{Z}/n\mathbb{Z}$ tale

che $ax = \overline{1}$, cioè $ax \equiv 1 \pmod{n}$.
Ma $ax \equiv 1 \pmod{n}$ equivale a dire che $n \,|ax - 1$, ovvero $\exists\ y$ tale che $ny = ax - 1$. Questa è una equazione diofantea ($ax - ny = 1$), che quindi è risolubile $\Leftrightarrow (a, n) = 1$.

Possiamo quindi considerare anche l'insieme degli elementi invertibili: $\mathbb{Z}/n\mathbb{Z}^* = \{a \in \mathbb{Z}/n\mathbb{Z} \,|(a, n) = 1\}$.
Tale insieme avrà cardinalità $|\mathbb{Z}/n\mathbb{Z}^*| = \varphi(n)$ e un'operazione interna, il prodotto.
Infatti se $(a, n) = 1$ e $(b, n) = 1$, allora $(ab, n) = 1$.

Dimostrazione.

$$\begin{matrix} as + nt = 1 \\ bu + nv = 1 \end{matrix} \quad \text{Risolubili perché } (a, n) = (b, n) = 1$$

$$\Rightarrow\ ab\underbrace{su}_{x} + n\underbrace{(asv + btu + ntv)}_{y} = 1 \text{ moltiplicando membro a membro}$$

Poiché tale equazione ($abx + ny = 1$) è risolubile, allora $(ab, n) = 1$ □

5.2 Risolvere una Congruenza

- $x + a \equiv 0 \pmod{n} \ \Rightarrow\ x \equiv -a \pmod{n}$ (esiste sempre l'inverso additivo)
- $ax \equiv b \pmod{n} \ \Rightarrow x \equiv a^{-1}b \pmod{n}$ (se e solo se esiste l'inverso moltiplicativo di a)
  Infatti, $ax \equiv b \pmod{n} \ \Rightarrow \exists\ y \in \mathbb{Z}$ tale che $ax = b + ny$. Questa equazione diofantea ha soluzioni $\Leftrightarrow\ (a, n) \mid b$
  Chiamiamo $d = (a, n)$: scriviamo $a = a_1 d$, $b = b_1 d$ e $n = n_1 d$. $\Rightarrow$ $a_1 x + n_1 y = b_1$.
  Risolviamo l'equazione ausiliaria $a_1 x + n_1 y = 1$, che avrà una soluzione del tipo $x \equiv x_0 \pmod{n_1}$; torniamo poi all'equazione al MCD che ha come soluzione $x \equiv x_0 b_1 \pmod{n_1}$. La soluzione completa, modulo n, sarà $x \equiv x_0 b_1, 2x_0 b_1, \ldots, dx_0 b_1 \pmod{n}$.

5.3 Teorema Cinese del Resto

Teorema Cinese del Resto: Siano $m, n \in \mathbb{Z}$ tali che $(m, n) = 1$. Siano $r, s \in \mathbb{N}$ tali che $0 \leq r < m$ e $0 \leq s < n$. Allora esiste un intero x tale che

$$\begin{cases} x \equiv r \pmod{m} \\ x \equiv s \pmod{n} \end{cases}$$

Dimostrazione. Vogliamo trovare le soluzioni x del sistema

$$\begin{cases} x = r + my \\ x = s + nz \end{cases} \Rightarrow \quad my - nz = s - r$$

Ma $(m, n) = 1$, quindi tale equazione è risolubile e ha come soluzioni $\begin{cases} y = y_0 + kn \\ z = z_0 + km \end{cases}$.

$$\Rightarrow \; x = r + my = r + m(y_0 + kn) = \underbrace{r + my_0}_{=} + kmn$$
$$\overbrace{s + nz_0} + kmn = s + n(z_0 + km) = x$$

Dunque

$$\begin{cases} x = r + m(y_0 + kn) \\ x = s + n(z_0 + km) \end{cases} \Rightarrow \begin{cases} x \equiv r \pmod{m} \\ x \equiv s \pmod{n} \end{cases}$$

□

Osservazione. La dimostrazione mostra che le soluzioni del sistema sono tutte e sole

$$x \equiv x' \pmod{mn} \text{ con } x' = r + my_0 = s + nz_0$$

Osservazione. Se nelle ipotesi del TCR c'è $(m, n) = d > 1$ allora:

- Se $d \nmid s - r \;\Rightarrow \nexists\, x \in \mathbb{Z}$ che confermi la tesi.
- Se $d \mid s - r$ possiamo dividere tutto per d:

$$\begin{cases} y \equiv y_0 \pmod{\frac{n}{d}} \\ z \equiv z_0 \pmod{\frac{m}{d}} \end{cases} \Rightarrow \; x = r + my_0 + \frac{mn}{d}k$$

$$\Rightarrow x \equiv x_0 \pmod{\frac{mn}{d}}, \text{ ovvero } x \equiv x_0 \pmod{[m, n]}$$

5.4 Risolvere un Sistema di Congruenze

$$\begin{cases} ax \equiv b \pmod{m} \\ cx \equiv d \pmod{n} \end{cases}$$

La risolubilità di un sistema è data da:

- Risolubilità delle singole equazioni: $(a, m) \mid b \quad (c, n) \mid d$;
- Se le condizioni sono soddisfatte, si risolvono le singole equazioni trovando le soluzioni:

$$\begin{cases} x \equiv x_1 \pmod{m_1} \\ x \equiv x_2 \pmod{n_1} \end{cases}$$

- Se $(m_1, n_1) = 1$, il TCR dice che $x \equiv x_3 \pmod{m_1 n_1}$
- Se $(m_1, n_1) = d > 1$, la condizione di risolubilità è che $d \mid x_1 - x_2$. Se si verifica, allora $x \equiv x_3 \pmod{[m_1, n_1]}$.

In generale la soluzione di un sistema del tipo

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \\ \vdots \\ x \equiv a_n \pmod{b_n} \end{cases}$$

è data dalla formula

$$x = \prod_{i=1}^{n} a_i \left(\prod_{j \neq i} b_j \right) \left[\left(\prod_{k \neq i} b_k \right)^{-1_{b_i}} \right]$$

dove $c^{-1_{b_i}}$ sta a significare l'inverso moltiplicativo di c rispetto a b_i.

5.5 Congruenze Quadratiche

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

$p \neq 2, a \not\equiv 0 \pmod{p} \Rightarrow x \equiv \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \pmod{p}$ dove $\frac{1}{2a} \equiv (2a)^{-1} \pmod{p}$
Esiste una soluzione se e solo se $\exists \delta \in \mathbb{Z}/p\mathbb{Z}$ tale che $\delta^2 \equiv b^2 - 4ac \pmod{p}$.

$$x^2 \equiv a \pmod{p^\alpha} \text{ ha soluzione } \Leftrightarrow x^2 \equiv a \pmod{p}$$

5.6 Piccolo Teorema di Fermat

Piccolo Teorema di Fermat: p primo $\Rightarrow x^p \equiv x \pmod{p}$ $\forall\, x \in \mathbb{Z}$.
Dunque $x\left(x^{p-1} - 1\right) \equiv 0 \pmod{p} \Rightarrow p \mid x\left(x^{p-1} - 1\right) \Rightarrow \begin{cases} p \mid x \to x \equiv 0 \pmod{p} \\ p \mid x^{p-1} - 1 \to x^{p-1} \equiv 1 \pmod{p} \end{cases}$.
Quindi $\forall\, x \in \mathbb{Z}$ tale che $(x, p) = 1$ si ha che $x^{p-1} \equiv 1 \pmod{p}$.

5.7 Teorema di Eulero

Teorema di Eulero: Sia $m \in \mathbb{Z}$. Se $(x, m) = 1$, allora $x^{\varphi(m)} \equiv 1 \pmod{m}$.
In generale, il periodo per i residui delle potenze è un divisore di $\varphi(m)$.

Dimostrazione. Consideriamo $\left\{a_1, \ldots, a_{\varphi(m)}\right\}$ l'insieme $\{x \mid 0 < x < m, (x, m) = 1\}$.
$A = a_1 \cdot \cdots \cdot a_{\varphi(m)} \Rightarrow (A, m) = 1$.
Prendiamo un x tale che $(x, m) = 1$. Costruiamo la funzione

$$\begin{aligned} f_x : &\mathbb{Z}/m\mathbb{Z}^* &&\leftrightarrow \mathbb{Z}/m\mathbb{Z}^* \\ &a_1 &&\mapsto a_1 x \\ &\vdots &&\quad \vdots \\ &a_{\varphi(m)} &&\mapsto a_{\varphi(m)} x \end{aligned}$$

Questa funzione è *iniettiva*: infatti, se $a_i x \equiv a_j x \pmod m$, allora (poiché $(x, m) = 1$) $a_i \equiv a_j \pmod m$.
Questa funzione è allora anche *surgettiva*, data l'iniettività e la cardinalità degli insiemi di partenza e di arrivo.
Ma allora

$$\begin{aligned} a_1 \cdot \cdots \cdot a_{\varphi(m)} &\equiv (a_1 x) \cdot \cdots \cdot \left(a_{\varphi(m)} x\right) \pmod m \\ A &\equiv A x^{\varphi(m)} \pmod m \\ \Rightarrow x^{\varphi(m)} &\equiv 1 \pmod m \quad \text{dato che } (A, m) = 1 \end{aligned}$$

□

Capitolo 6

Teoria dei Gruppi

DEFINIZIONE: Un *gruppo* è un insieme G dotato di un'operazione interna con le seguenti proprietà:

- L'operazione è associativa: $(a * b) * c = a * (b * c)$;
- Esiste un elemento neutro: $a * e = e * a = a$;
- $\forall\ a \in G$ esiste un inverso di a tale che $a * b = b * a = e$.

Se possiede anche la proprietà commutativa allora il gruppo si dice *commutativo* o *abeliano*.

REGOLE DI CANCELLAZIONE:

$$\begin{aligned} a * b = a * c &\Rightarrow b = c \\ b * a = c * a &\Rightarrow b = c \\ a * b = c * a &\not\Rightarrow b = c \end{aligned}$$

Osservazione. L'elemento neutro e l'inverso è unico. Infatti, se e_1, e_2 sono 2 elementi neutri, allora $e_1 = e_1 * e_2 = e_2$. Se invece y_1 e y_2 sono due inversi di x allora $xy_1 = e = xy_2$, che implica, per le regole di cancellazione, $y_1 = y_2$.

Osservazione. $(xy)^{-1} = y^{-1}x^{-1}$.

Osservazione. $\forall\ x \in G$ le funzioni

$$\begin{aligned} T_1(g) : G &\leftrightarrow G \\ x &\mapsto gx \end{aligned} \qquad \begin{aligned} T_2(g) : G &\leftrightarrow G \\ x &\mapsto xg \end{aligned}$$

sono bigettive. L'iniettività è data dalle regole di cancellazione, la surgettività dalla risolubilità delle equazioni.

DEFINIZIONE: Sia G un gruppo. Un sottoinsieme *non vuoto* H di G si

dice un *sottogruppo* di G ($H < G$) se esso stesso è un gruppo con l'operazione indotta da G.

Osservazione. Ogni gruppo G ha come sottogruppi banali $\{e\}$ e G.

6.1 Sottogruppi di $\mathbb{Z}$

Proposizione: I sottogruppi di $\mathbb{Z}$ sono tutti e soli della forma

$$m\mathbb{Z} = \{m\overline{x} \mid x \in \mathbb{Z}\} \text{ con } m \in \mathbb{Z}$$

Dimostrazione. Dimostriamo che $\forall\ m \in \mathbb{Z}\ \ m\mathbb{Z} < \mathbb{Z}$.

- $0 \in m\mathbb{Z}$. Infatti $0 = m0$;
- $x, y \in m\mathbb{Z} \Rightarrow x+y \in m\mathbb{Z}$. Infatti $x = ma$, $y = mb$ e $x+y = m(a+b)$;
- $x \in m\mathbb{Z} \Rightarrow -x \in m\mathbb{Z}$. Infatti $x = ma$, $-x = m(-a)$.

Dimostriamo che sono gli unici sottogruppi.
Se $H = \{0\}$ allora $H = 0\mathbb{Z}$ è del tipo dato. Supponiamo quindi $H \neq \{0\}$.
Allora $\exists\ y \in H$ tale che $y \neq 0$, e quindi anche $-y \in H$ e $-y \neq 0$.
Quindi H contiene un elemento positivo, cioè $H \cap \mathbb{N} \neq \emptyset$.
Sia $S = H \cap \mathbb{N}$. $S \subseteq \mathbb{N}$ e $S \neq \emptyset$.
Sia $m = minS$. Dimostriamo che $H = m\mathbb{Z}$.

- $m\mathbb{Z} \subseteq H$. Infatti $m \in H \Rightarrow m + m \in H \ldots \Rightarrow km \in H\ \forall\ k \in \mathbb{N}$. Ma allora $(-k)m \in H$ e quindi $km \in H\ \forall\ k \in \mathbb{Z}$;
- $H \subseteq m\mathbb{Z}$. Sia $h \in H$ e facciamo la divisione euclidea.

$$h = qm + r \Rightarrow r \in H (\text{poiché } h \in H \text{ e } qm \in H) \text{ con } 0 \leq r < m$$

$$\text{Ma } m = minS \Rightarrow r = 0 \Rightarrow h = qm$$

□

Relazione di Contenimento tra sottogruppi di $\mathbb{Z}$:

$$m\mathbb{Z} \subseteq n\mathbb{Z} \Leftrightarrow n \mid m$$

Il più grande sottogruppo contenuto in entrambi è $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\,\mathbb{Z}$.
Il più piccolo sottogruppo che contiene entrambi è $(m, n)\,\mathbb{Z}$.

6.2 Sottogruppi Generati

Sia $|G| < +\infty$ e sia $a \in G$.
$\langle a \rangle$ =il più piccolo sottogruppo contenente a.

$e, a, a^2, \ldots, a^{n-1}, \ldots, a^{n+r}, \ldots \in \langle a \rangle$.
Ma G ha cardinalità finita, quindi $\exists n \in \mathbb{N} \setminus \{0\}$ tale che $a^{n+r} = a^r$, che implica $a^n = e$. Allora (scegliendo n come il più piccolo naturale con tale proprietà) $|\langle a \rangle| = n$.

Inoltre $\langle a \rangle$ è un sottogruppo abeliano. Infatti ogni $x \in \langle a \rangle$ è una potenza di a, e per le proprietà degli interi essi commutano tra di loro.

Definizione: Dati 2 sottogruppi H e K di G possiamo considerare:

- Il più grande sottogruppo contenuto in entrambi: $H \cap K$;
- Il più piccolo sottogruppo che contiene entrambi: consideriamo tutti i sottogruppi G_i' tali che $H \cup K \subseteq G_i'$ e prendiamo l'intersezione

$$\bigcap_{i \in I} G_i'$$

In generale, dato un qualunque sottoinsieme S di G, il più piccolo sottogruppo che contiene S è

$$\bigcap_{\substack{H \supseteq S \\ H < G}} H = \langle S \rangle$$

Se $S = \{x\}$ allora $\langle S \rangle = \{x^n \mid n \in \mathbb{Z}\}$.
Se $S = \{x_1, \ldots, x_k\}$ allora definendo $T = S \cup S^{-1} = \{x_1, \ldots, x_k\} \cup \left\{x_1^{-1}, \ldots, x_k^{-1}\right\}$ si ha che $\langle S \rangle = \{t_1 \cdot \ldots \cdot t_n \mid n \in \mathbb{N},\ t_i \in T\ \forall\ i\}$.

6.3 Classi Laterali

Definiamo due nuove relazioni di equivalenza tra elementi di uno stesso gruppo.
Sia $H < G$:

1. $x \sim y \Leftrightarrow y^{-1}x \in H$.
2. $x \sim y \Leftrightarrow xy^{-1} \in H$.

Le verifiche che sia una relazione di equivalenza sono lasciate per esercizio.

Studiamo adesso le classi di equivalenza di un elemento x per la prima

relazione (per la seconda sono analoghe):
Sia $x \in G$. La classe di x per la prima relazione di equivalenza è:

$$C_x = \left\{ y \in G \mid y^{-1}x \in H \right\} = \left\{ y \in G \mid x^{-1}y \in H \right\}$$

DEFINIZIONE: $xH = \{xh \mid h \in H\}$ viene detta *classe laterale sinistra* di x rispetto ad H.

Osservazione. $x^{-1}y \in H \Leftrightarrow \exists\ h \in H$ tale che $y = xh$. Ciò significa che $C_x = xH$.

DEFINIZIONE: La classe di x per la seconda relazione di equivalenza è $Hx = \{hx \mid h \in H\}$ ed è detta *classe laterale destra* di x rispetto ad H.

6.4 Teorema di Lagrange

TEOREMA DI LAGRANGE: Sia G un gruppo finito di ordine n. Sia $H < G$, $|H| = d$. Allora $d \mid n$.

Dimostrazione. Consideriamo una delle relazioni di equivalenza. Le classi formano una partizione di G; poiché ogni classe ha cardinalità d (dato che $f_x : H \to xH$ è bigettiva), posto $k = \#classi$, allora $n = dk$. □

CONSEGUENZE:

1. Se $ord(G) = |G| = p$ con p primo, allora gli unici sottogruppi sono $\{e\}$ e G.

2. Se $ord(G) = n$, $x \in G$ con $x \neq e$ e $h = ord(x)$ allora $x^a = x^b \Leftrightarrow a \equiv b \pmod{h}$.

   Dimostrazione. $\Rightarrow$.

   $$\begin{array}{ll} a = q_1 h + r_1 & x^a = x^{q_1 h} x^{r_1} = x^{r_1} \\ b = q_2 h + r_2 & x^b = x^{q_2 h} x^{r_2} = x^{r_2} \end{array} \Rightarrow\ x^{r_1} = x^{r_2}$$

   $$x^{r_1 - r_2} = e \qquad \text{Ma } r_1 - r_2 < h \Rightarrow r_1 = r_2$$

   □

   Dimostrazione. $\Leftarrow$.

   $$a \equiv b \pmod{h} \Rightarrow\ a = b + ht \Rightarrow x^a = x^b x^{ht} = x^b$$

   □

DEFINIZIONE: Un sottogruppo H di G si dice *normale* (e si scrive $H \triangleleft G$) se $xH = Hx \ \forall \ x \in G$.

Osservazione. Se G è abeliano, allora ogni sottogruppo è normale.

Osservazione. $xH = Hx$ *non* significa $xh = hx \forall \ h \in H$.

Osservazione. Per dimostrare che $H \triangleleft \ G$ basta mostrare che $xH \subseteq Hx \ \ \forall \ x \in G$. Infatti:

$$xH \subseteq Hx$$
$$x^{-1}xH \subseteq x^{-1}Hx$$
$$Hx^{-1} \subseteq x^{-1}H$$

Oppure equivalentemente che $xHx^{-1} \subseteq H \ \forall \ x \in G$.

PROPOSIZIONE: Sia $H \triangleleft G$ e sia G/H l'insieme quoziente per le 2 relazioni di equivalenza. Allora G/H ha una struttura naturale di gruppo con l'operazione $xH * yH := xyH$.

Dimostrazione. Mostriamo che l'operazione è ben definita:
Sia $xH = x'H$ e $yH = y'H$. Vogliamo che $xyH = x'y'H$. Prendiamo $h \in H$:

$$xyh = xy'h' = xh''y' = x'h'''y' = x'y'h''''$$

Le verifiche che G/H sia un gruppo vengono lasciate. □

Osservazione. Se G è un gruppo finito di ordine n e $ord(H) = d$, allora $ord(G/H) = \frac{n}{d}$.

6.5 Omomorfismi di Gruppi

DEFINIZIONE: Siano G, G' gruppi. La funzione $f : G \to G'$ si dice *omomorfismo* se $f(xy) = f(x)f(y) \ \forall \ x, y \in G$.

PROPRIETÀ DEGLI OMOMORFISMI:

- $f(e) = e'$: infatti $e'f(x) = f(x) = f(ex) = f(e)f(x)$;
- $f(x^{-1}) = [f(x)]^{-1}$: infatti $f(x)f(x^{-1}) = f(xx^{-1}) = e' = f(x)\,[f(x)]^{-1}$.

DEFINIZIONE: Sia $f : G \to G'$ un omomorfismo. Si dice *nucleo* o *kernel* di f l'insieme

$$Kerf = \{x \in G \mid f(x) = e'\}$$

PROPOSIZIONE: $Kerf \triangleleft G$.

Dimostrazione. Le verifiche che $Kerf < G$ sono banali. Verifichiamo che sia normale.
Sia $h \in Kerf$: $f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = e'$, ovvero $x\ Kerf\ x^{-1} \subseteq Kerf$. □

PROPOSIZIONE: Sia G gruppo. I sottogruppi normali sono tutti e soli i nuclei degli omomorfismi definiti da G ad un altro gruppo qualsiasi.

Dimostrazione. Abbiamo già visto che $Kerf \triangleleft G$. Resta da dimostrare che se $H \triangleleft G$ allora $H = Kerf$ per una certa funzione f.
Prendiamo la proiezione canonica $\begin{matrix} \pi : G \to G/H \\ x \mapsto xH \end{matrix}$. Tale funzione è un omomorfismo (banale verifica).

$$Ker\pi = \{x \in G \mid \pi(x) = eH = H\} \Rightarrow x \sim e \Rightarrow e^{-1}x \in H$$

dunque $Ker\pi = H$ □

PROPOSIZIONE: Sia $f : G \to G'$ un omomorfismo e sia $K = Kerf$. Allora $f(x) = f(y) \Leftrightarrow xK = yK$.

Dimostrazione. $\Rightarrow$.

$$f(xy^{-1}) = f(x)\,[f(y)]^{-1} = f(y)\,[f(y)]^{-1} = e' \Rightarrow xy^{-1} \in K$$
$$\text{Ovvero } x \in Ky = yK \Rightarrow xK = yK$$

□

Dimostrazione. $\Leftarrow$.

$$xK = yK \Rightarrow x \in yK \quad x = yh \ \ (h \in K)$$
$$f(x) = f(yh) = f(y)f(h) = f(y)$$

□

Osservazione. Un omomorfismo f è iniettivo se e solo se $Kerf = \{e\}$. Quindi $\forall\ x \in G\ \ ord\,(f(x)) = ord(x)$.

DEFINIZIONE: Un omomorfismo bigettivo si dice *isomorfismo*.

PROPOSIZIONE: Sia $H < G$. Se G è un gruppo ciclico allora H è ciclico.

Dimostrazione. Se G è ciclico allora $\exists\ g \in G$ tale che $G = \langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$.
$G \cap H = \{g^{i_1}, \ldots, g_{i_k}\}$ con $i_1, \ldots, i_k \in \mathbb{Z}$.
Sia $h = min\,(\{i_1, \ldots, i_k\} \cap \mathbb{N}_+)$. Dimostriamo che $H = \left\langle g^h \right\rangle$.

Sia $g^j \in H$ con $j > 0$. $\Rightarrow h \leq j \quad \exists\, k, r \in \mathbb{N}$ tali che $j = kh + r$.

$$g^j = g^{kh} g^r = \left(g^h\right)^k g^r \Rightarrow g^r \in H \Rightarrow r = 0 \Rightarrow H = \left\langle g^h \right\rangle$$

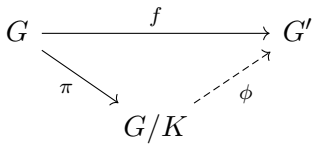
□

Osservazione. Sia $H < \mathbb{Z}/m\mathbb{Z}$. H è ciclico. Sia $H = \langle a \rangle$.
Se $(a, m) = 1 \Rightarrow ord(H) = m$.
Se $(a, m) = d \neq 1 \Rightarrow ord(H) = \frac{m}{d}$.

Corollario:

$$\sum_{d|n} \varphi(d) = m$$

Teorema di Omomorfismi per Gruppi: Sia $f : G \to G'$ un omomorfismo di gruppi e sia $K = Kerf$. Allora esiste uno e un solo omomorfismo $\phi : G/K \to G'$ che renda il seguente diagramma commutativo.



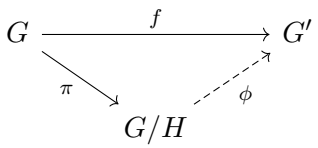
Inoltre ϕ è iniettiva, mentre è surgettiva se e solo se f è surgettiva.

Dimostrazione. Dimostriamo prima che se tale funzione esiste, allora è unica.
Deve essere $f(x) = (\phi \circ \pi)(x) \ \ \forall\, x \in G$, ovvero $f(x) = \phi(xK)$.

Vediamone adesso l'esistenza. Innanzitutto verifichiamo che sia ben definita:
se $xK = x'K$, allora dall'identità sopra trovata discende immediatamente che $f(x) = f(x')$.
È un omomorfismo di gruppi. Infatti $\phi(xKyK) = f(xy) = f(x)f(y) = \phi(xK)\phi(yK)$.
L'iniettività discende dalla definizione di $\phi(xK)$. Ovviamente ϕ ha la stessa immagine di f. □

Osservazione. Se $H \subseteq K = Kerf$ allora è vero che $xH = x'H \ \Rightarrow \ f(x) = f(x')$.

Osservazione. Supponiamo $H \triangleleft G$, $H \subseteq K = Kerf$. Allora nel diagramma



ϕ è un omomorfismo, ma non necessariamente iniettivo.

6.6 Teorema Cinese del Resto

Teorema cinese del Resto: Siano $m, n \in \mathbb{Z}$ tali che $(m, n) = 1$. Allora

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \ \times \ \mathbb{Z}/n\mathbb{Z}$$

Dimostrazione. Sia $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ tale che $f(x) = ([x]_m, [x]_n)$. Vediamo che si tratti di un omomorfismo:

$$\begin{aligned} f(x+y) &= ([x+y]_m, [x+y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) \\ &= ([x]_m, [x]_n) + ([y]_m, [y]_n) = f(x) + f(y) \end{aligned}$$

Tale funzione è evidentemente surgettiva. Dal primo Teorema di Omomorfismo sappiamo che esiste $\phi : \mathbb{Z}/Kerf \to \mathbb{Z}_m \times \mathbb{Z}_n$ e che si tratta di un isomorfismo (omomorfismo iniettivo e surgettivo). Cerchiamo allora $Kerf$.

$$\begin{aligned} Kerf &= \{x \in \mathbb{Z} \mid f(x) = ([0]_m, [0]_n)\} \\ &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m} \ \wedge \ x \equiv 0 \pmod{n}\} = mn\mathbb{Z} \end{aligned}$$

ϕ è l'isomorfismo cercato. □

Osservazione. $\mathbb{Z}_m \times \mathbb{Z}_n$ è ciclico se e solo se $(m, n) = 1$.

Dimostrazione. $\Rightarrow$.
Supponiamo $d = (m, n)$ con $d \neq 1$ e dimostriamo che il gruppo non è ciclico. Sia $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_m$. Sia $k \in \mathbb{Z}$ tale che $[m, n] \mid k$. Allora $k(x, y) = (0, 0)$. Ma allora $ord\,((x, y)) \leq [m, n] < mn$. Quindi non esiste un generatore per $\mathbb{Z}_m \times \mathbb{Z}_n$, che significa che il gruppo non è ciclico. □

Dimostrazione. $\Leftarrow$. Teorema Cinese del Resto. □

6.7 Corrispondenza tra Sottogruppi

Corrispondenza tra Sottogruppi determinata da un Omomorfismo Surgettivo: Sia $f : G \to G'$ un omomorfismo surgettivo e $K = Kerf$. Allora f induce una corrispondenza biunivoca tra i sottogruppi di G che contengono K e i sottogruppi di G'.

Immagine di Sottogruppi: Sia $f : G \to G'$ un omomorfismo qualsiasi. Allora

1. $H < G \Rightarrow f(H) < G'$;
2. $H' < G' \Rightarrow f^{-1}(H') < G$;

3. $H' \triangleleft G' \Rightarrow f^{-1}(H') \triangleleft G$;

4. $H \triangleleft G \not\Rightarrow f(H) \triangleleft G'$. L'implicazione è vera se f è surgettiva, falsa altrimenti.

Conseguenze:

1. I sottogruppi di $\mathbb{Z}_m$ corrispondono ai sottogruppi $a\mathbb{Z}$ con $a \mid m$;

2. Per ogni $a \mid m$ esiste un unico sottogruppo di $\mathbb{Z}_m$ di ordine a e un unico di ordine $\frac{m}{a}$;

3. Un gruppo ciclico finito ha uno e un solo sottogruppo per ogni a che divide l'ordine del gruppo;

4. I sottogruppi e i quozienti di un gruppo ciclico sono ciclici;

5. Un gruppo abeliano ha almeno un sottogruppo per ogni ordine possibile.

6.8 Teorema di Cauchy

Teorema di Cauchy: Sia G un grupo finito abeliano, sia p primo tale che $p \mid ord(G)$. Allora esiste $x \in G$ tale che $ord(x) = p$.

Dimostrazione. $|G| = n$, $p \mid n$, $|G| = pm = n$. Induzione su m.
Sia $x \in G$, $x \neq e$ e sia $H = \langle x \rangle$. $H \triangleleft G$ (poiché G è abeliano).

$$|G| = |H| \cdot |G/H| \Rightarrow \begin{array}{c} p \mid ord(H) \text{ e quindi tesi, perché } H \text{ è ciclico} \\ \vee \\ p \mid ord(G/H) \end{array}$$

Nel secondo caso allora $ord(G/H) = pm'$ con $m' < m$. Allora per ipotesi induttiva $\exists\, yH \in G/H$ tale che $ord(yH) = p$.
Prendiamo la proiezione canonica

$$\begin{aligned} \pi : G &\to G/H \\ y &\mapsto yH \end{aligned}$$

Essendo un omomorfismo, si ha che $ord(yH) \mid ord(G)$ ma anche $ord(yH) \mid ord(y)$. A questo punto basta prendere il gruppo ciclico $\langle y \rangle$, che quindi contiene un elemento di ordine p. □

6.9 Teoremi di Isomorfismo

TEOREMA: Sia G gruppo e siano $K \subseteq H \subseteq G$, $K \triangleleft G$ e $H \triangleleft G$. Allora

$$(G/K) \,/\, (H/K) \cong G/H$$

TEOREMA: Sia ${\mathbb{Z}_m}^*$ il gruppo degli elementi invertibili per la moltiplicazione di $\mathbb{Z}_m$. Allora

$$\begin{aligned} {\mathbb{Z}_{p^\alpha}}^* &\cong \mathbb{Z}_{\varphi(p^\alpha)} && \text{se } p \neq 2 \text{ oppure } p = 2 \wedge \alpha = 1 \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}} && \text{se } p = 2 \wedge \alpha \neq 1 \end{aligned}$$

Capitolo 7

Anelli

DEFINIZIONE: Un insieme dotato di 2 operazioni (una somma e un prodotto) interne con le seguenti proprietà

- Forma un gruppo abeliano con la somma;
- Proprietà associativa per il prodotto;
- Proprietà distributiva.

è detto *anello*.
Se esiste un elemento neutro per la moltiplicazione allora l'anello è detto *anello unitario*.

In un anello unitario si definisce $A^* := \{x \in A \mid x \text{ ha un inverso}\}$; esso è un gruppo con l'operazione di moltiplicazione.
Infatti, se $x, y \in A^*$, allora $xy \in A^*$ (perché $(xy)(y^{-1}x^{-1}) = 1$).

DEFINIZIONE: Sia A un anello. Un sottoinsieme *non vuoto* S di A si dice un *sottoanello* di A se esso stesso è un anello con le operazioni indotte da A.

DEFINIZIONE: Sia A un anello. Un sottoinsieme I di A è un *ideale* se

- è un sottogruppo rispetto all'addizione;
- $\forall\, a \in A \;\; \forall\, x \in I \;\; ax \in I$ e $xa \in I$ (assorbimento della moltiplicazione).

7.1 L'anello dei polinomi $\mathbb{K}[x]$

DEFINIZIONE: I polinomi in una indeterminata a coefficienti in un campo $\mathbb{K}$ formano un anello unitario commutativo chiamato $\mathbb{K}[x]$. Dati due polinomi $\sum a_j x^j$ e $\sum b_j x^j$ la somma tra i due è definita come $\sum (a_j + b_j) x^j$, mentre

il prodotto è $\sum \sum a_i b_j x^{i+j}$.

DEFINIZIONE: Il *grado* di f, $deg(f)$, è il $max\{i \in \mathbb{N} \mid a_i \neq 0\}$.

$deg(f+g) \leq max\{deg(f), deg(g)\}$
$deg(fg) = deg(f) + deg(g)$

7.2 Divisione Euclidea in $\mathbb{K}[x]$

DIVISIONE EUCLIDEA: Siano $f, g \in \mathbb{K}[x]$ con $g \neq 0$. Allora esistono unici $q, r \in \mathbb{K}[x]$ tali che:

- $f = qg + r$
- $0 \leq deg(r) < deg(g)$

Dimostrazione. Esistenza.
Sia $n = deg(g)$. Se $f = 0$ non c'è niente da dimostrare. Altrimenti sia $m = deg(f)$. Procediamo per Induzione su m.
Se $m < n$ allora $f = 0 \cdot g + f$. Supponiamo allora $m > n$.

$$\begin{array}{ll} f = a_m x^m + \ldots & a_m \neq 0 \\ g = b_n x^n + \ldots & b_n \neq 0 \end{array} \quad \text{Sia } c = a_m b_n^{-1}$$

Consideriamo $f_1 = f - cx^{m-n}g$. Si ha che $deg(f_1) < m$. Per ipotesi induttiva allora $f_1 = q_1 g + r_1 \;\Rightarrow\; f = (cx^{m-n} + q_1)\, g + r_1 = qg + r$. □

Dimostrazione. Unicità.
Supponiamo $f = qg + r = q'g + r'$. Allora $(q - q')\, g = r - r'$. Ma $deg(g) = n$ e $deg(r - r') < n$. Allora $q = q'$ e $r = r'$. □

ALGORITMO DI EUCLIDE PER L'MCD TRA POLINOMI:

$$MCD(f,g) : \bullet\ d \mid f, d \mid g; \qquad \bullet\ h \mid f, h \mid g \Rightarrow h \mid d.$$

Quanti sono i MCD tra due polinomi f e g?
Siano d, d' due MCD. Allora $d \mid d'$ e $d' \mid d$, cioè $d' = dl$ e $d = d'm$. $\Rightarrow d'(ml - 1) = 0$. Poiché $d' \neq 0$ allora $ml = 1$. Quindi $deg(m) = deg(l) = 0$. Gli MCD sono allora tutti i $d \cdot k$ con $k \in \mathbb{R}$ e d un MCD.

Osservazione. Abbiamo quindi visto che $(\mathbb{K}[x])^* = \mathbb{K}^*$.

7.3 Fattorizzazione dei Polinomi

DEFINIZIONE: Un elemento $f \in \mathbb{K}[x]$ ($f \neq 0$ e non invertibile) si dice *irriducibile* se $f = gh \Rightarrow deg(g) = 0$ oppure $deg(h) = 0$.

DEFINIZIONE: Un elemento $f \in \mathbb{K}[x]$ ($f \neq 0$ e non invertibile) si dice *primo* se $f \mid gh \Rightarrow f \mid g$ oppure $f \mid h$.

LEMMA: Se $f \mid gh$ e $(f, g) = 1$ allora $f \mid h$.

Dimostrazione. Usiamo Bézout.
$\exists\, a, b \in \mathbb{K}[x]$ tali che $af + bg = 1$. Moltiplichiamo tutto per h.

$$\underbrace{afh}_{f \mid afh} + \underbrace{bgh}_{f \mid bgh} = \underbrace{h}_{\Downarrow\ f \mid h}$$

□

PROPOSIZIONE: f è primo e e solo se f è irriducibile.

Dimostrazione. $\Rightarrow$. Vero in un caso più generale.
f primo. $f = gh$. In particolare $f \mid gh$ e quindi $f \mid g$ o $f \mid h$.

- $f \mid g \Rightarrow g = kf$. Quindi $f = gh = kfh \Rightarrow (kh - 1)f = 0$. Ma $f \neq 0$, dunque $kh = 1$ e k e h sono invertibili.
- $f \mid h$ Analogamente a sopra g è invertibile.

□

Dimostrazione. $\Leftarrow$.
Supponiamo f irriducibile e $f \mid gh$.

$$(f, g) = \begin{cases} f \to f \mid g \\ 1 \to \textbf{Lemma}\ f \mid h \end{cases}$$

□

FATTORIZZAZIONE UNICA IN $\mathbb{K}[x]$: Ogni polinomio ($\neq 0$) si scrive in modo unico come prodotto di elementi irriducibili e di un elemento invertibile (a meno dell'ordine) e a meno di moltiplicazione dei fattori per elementi invertibili.

Dimostrazione. Esistenza.
Un polinomio di grado 1 è irriducibile. Infatti $f = gh \Rightarrow 1 = deg(f) = deg(g) + deg(h) = 1 + 0 \Rightarrow f$ irriducibile. Procediamo quindi per Induzione sul grado.

Sia $deg(f) = n$. Se f è irriducibile abbiamo finito. Altrimenti $f = gh$ con g e h fattori non banali. Poiché $deg(g) < n$ e $deg(h) < n$ allora essi sono fattorizzabili come richiesto e quindi anche f lo è. □

Dimostrazione. Unicità.
Sia $f = \lambda g_1 g_2 \cdot \ldots \cdot g_r = \mu h_1 h_2 \cdot \ldots \cdot h_s$. Procediamo per Induzione su $max\{r, s\}$.
Poiché g_1 è irriducibile, allora è primo e quindi $g_1 \mid \mu h_1 h_2 \cdot \ldots \cdot h_s \Rightarrow g_1 \mid h_i$ per un qualche indice $1 \leq i \leq s$. Senza perdita di generalità possiamo supporre $g_1 \mid h_1$. Allora $h_1 = g_1 k_1$ con k_1 invertibile.
Semplificando $\frac{f}{g_1} = \lambda g_2 \cdot \ldots \cdot g_r = (\mu k_1) h_2 \cdot \ldots \cdot h_s$. Poiché adesso ci sono meno fattori si può applicare l'ipotesi induttiva. □

7.4 Polinomi e Radici

Definizione: Un elemento $a \in \mathbb{K}$ si dice *radice* di $f(x) \in \mathbb{K}[x]$ se $f(a) = 0$.

Teorema di Ruffini: Un elemento $a \in \mathbb{K}$ è radice di $f(x)$ se e solo se $(x - a) \mid f(x)$.

Dimostrazione. Usiamo la divisione Euclidea.

$$\begin{aligned} &f(x) = g(x)(x-a) + r \\ &f(a) = g(a)(a-a) + r \Rightarrow \ f(a) = 0 \Leftrightarrow r = 0 \\ &f(a) = 0 + r \end{aligned}$$

□

Corollario: Un polinomio di grado n ha al più n radici distinte.

Dimostrazione. Induzione su $deg(f) = n$.
Se f non ha radici in $\mathbb{K}$ non c'è niente da dimostrare. Altrimenti, se a è radice, usiamo Ruffini: $f(x) = g(x)(x - a)$.
$deg(g) = n - 1 \Rightarrow$ g ha al più $n - 1$ radici distinte per ipotesi induttiva $\Rightarrow$ f ha al più n radici distinte. □

Definizione: Sia f un polinomio in $\mathbb{K}[x]$. Si definisce *funzione polinomiale* la funzione $F : \mathbb{K} \to \mathbb{K}$ tale che $x \mapsto a_n x^n + \ldots + a_0$.

Principio di Identità dei Polinomi: Se $\mathbb{K}$ è un campo con infiniti elementi, allora l'omomorfismo $f \to F$ è iniettivo.

Dimostrazione. Siano f, g tali che $F = G$, ovvero $\forall\ x \in \mathbb{K}\ f(x) = g(x)$.
Quindi $f(x) - g(x) = (f - g)(x) = 0$, cioè $f = g$. □

Elementi Irriducibili (o Primi):

Caso $\mathbb{K} = \mathbb{C}$:

Teorema Fondamentale dell'Algebra: Ogni polinomio $f \in \mathbb{C}[x]$ di grado > 0 ha una radice in $\mathbb{C}$ ($\mathbb{C}$ è algebricamente chiuso).

Corollario: Ogni polinomio $f \in \mathbb{C}[x]$ con $f \neq 0$ si scrive come prodotto di un elemento invertibile e fattori di primo grado.

Dimostrazione. Induzione con Ruffini + Torema Fondamentale. □

Caso $\mathbb{K} = \mathbb{R}$:

Proposizione: Sia $f(x) \in \mathbb{R}[x]$. Se $\alpha \in \mathbb{C}$ è una radice di $f(x)$ allora $\bar{\alpha}$ è una radice di $f(x)$.

Dimostrazione.

$$0 = \overline{f(\alpha)} = \overline{c_n\alpha^n + \ldots + c_0} = \overline{c_n\alpha^n} + \ldots + \overline{c_0} = c_n\overline{\alpha^n} + \ldots + c_0 = f(\bar{\alpha})$$

□

Corollario: I polinomi irriducibili in $\mathbb{R}[x]$ hanno grado 1 o 2.

Caso $\mathbb{K} = \mathbb{Q}$:

Proposizione: In $\mathbb{Q}[x]$ esistono polinomi irriducibili di qualsiasi grado.

Dimostrazione. Ad esempio, $f(x) = x^n - 2$ è irriducibile $\forall\ n \in \mathbb{N}$. □

Caso $\mathbb{Z}/p\mathbb{Z}$:

Proposizione: In $\mathbb{Q}[x]$ esistono polinomi irriducibili di qualsiasi grado.

Osservazione. Se $f(x) \in \mathbb{Q}[x]$ allora esiste $d \in \mathbb{N}_+$ tale che

$$f(x) = \frac{g(x)}{d} \quad \text{con } g(x) \in \mathbb{Z}[x]$$

Osservazione. Se, dato $f(x) = c_nx^n + \ldots + c_0 \quad \in \mathbb{Z}[x]$, esistono radici razionali, allora sono del tipo $x = -\frac{b}{a}$ con $b \mid c_0$ e $a \mid c_n$. Quindi $(ax+b) \mid f(x)$.

Osservazione. Se $f(x) \in \mathbb{Q}[x]$ ha grado ≤ 3 allora f è riducibile se e solo se ha almeno una radice in $\mathbb{Q}$.

Osservazione. Per trovare le radici di un polinomio $p(x)$ in $\mathbb{Z}_p[x]$, basta calcolare il $MCD\,(p(x), x^p - x)$. In questo modo otteniamo tutte le radici del polinomio, ma senza saperne le molteplicità. Questo perché $x^p - x = x(x-1)(x-2)\cdot\ldots\cdot(x-p+1) = \prod_{i\in\mathbb{Z}_p}(x-i)$.

7.5 Lemma di Gauss

Definizione: Sia $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$. Definiamo *contenuto* di f

$$c(f) := MCD(a_n, \ldots, a_0)$$

Lemma di Gauss:

$$c(fg) = c(f)c(g)$$

Dimostrazione. Consideriamo dapprima il caso $c(f) = c(g) = 1$. Dimostriamo che $c(fg) = 1$.
Supponiamo per assurdo $c(fg) \neq 1 \;\Rightarrow \exists\, p$ primo tale che $p \mid c(fg)$. Consideriamo i coefficienti modulo p.
Per ipotesi $\overline{f}(x) \neq 0$, $\overline{g}(x) \neq 0$ ma $\overline{fg} = 0$. Assurdo.
Guardiamo adesso il caso generale. Sia $f \in \mathbb{Z}[x]$ e $g \in \mathbb{Z}[x]$.

$$\begin{matrix} f = c(f)f_1 \\ g = c(g)g_1 \end{matrix} \quad \Rightarrow fg = c(f)c(g)f_1g_1$$

Passando ai contenuti in entrambi i membri:

$$c(fg) = c(f)c(g)c(f_1g_1)$$

Ma f_1 e g_1 sono primitivi ($c(f_1) = c(g_1) = 1 \Rightarrow c(f_1g_1) = 1$), da cui la tesi. □

Corollario: Sia $f \in \mathbb{Z}[x]$, $f = gh$ con $g,\ h \in \mathbb{Q}[x]$. Allora esistono $g', h' \in \mathbb{Z}[x]$ tali che $f = g'h'$ e $deg(g) = deg(g')$ e $deg(h) = deg(h')$.

Dimostrazione. Sia $b = mcm\,\{\text{denominatori di } g\}$. Allora posso scrivere $g = \frac{g'}{b}$ con $g' \in \mathbb{Z}[x]$ (g e g' hanno lo stesso grado).
Inoltre $g' = c(g')g_1$ con g_1 primitivo. Quindi $g = \frac{c(g')}{b}g_1$ con $g_1 \in \mathbb{Z}[x]$.

Analogamente $h = \frac{c(h')}{d}h_1$ con $h_1 \in \mathbb{Z}[x]$ e primitivo.
Allora $f = gh = \frac{c(g')c(h')}{bd}g_1h_1$. Poiché $f \in \mathbb{Z}[x]$, $c(f) \in \mathbb{Z}$ e passando ai contenuti nell'identità precedente si ha che $c(f) = \frac{c(g')c(h')}{bd}c(g_1h_1) = \frac{c(g')c(h')}{bd}$.
Dunque $bd \mid c(g')c(h')$ e quindi $f = g''h''$ con $g'' = kg'$ e $h'' = th'$ per certi $k, t \in \mathbb{Z}$. □

7.6 Criterio di Eisenstein

Criterio di irriducibilità di Eisenstein: Sia $f \in \mathbb{Z}[x]$. f è irriducibile su $\mathbb{Q}[x]$ se $\exists\ p \in \mathbb{N}$ primo tale che

$$\begin{cases} p \nmid a_n \\ p \mid a_i\ \forall\ i = 0, \ldots, n-1 \\ p^2 \nmid a_0 \end{cases}$$

Dimostrazione. Sia $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ l'omomorfismo di anelli tale che $\phi(a_n x^n + \ldots + a_0) = \overline{a_n} x^n + \ldots + \overline{a_0}$.
Poiché $p \mid a_i \forall\ i < n$, allora $\phi\left(p(x)\right) = cx^n$. Dunque se fosse riducibile, per la fattorizzazione unica in $\mathbb{Z}_p[x]$ i due divisori sarebbero del tipo bx^k e $\frac{c}{b}x^{n-k}$. Ma allora entrambi i termini noti sarebbero divisibili per p, che significa $p^2 \mid a_0$, dato che a_0 è il prodotto dei due termini noti. Assurdo. □

Osservazione. $f(x)$ è irriducibile $\Leftrightarrow$ $f(x+b)$ è irriducibile.

Osservazione. $f(x)$ è irriducibile $\Leftrightarrow$ $f(\frac{1}{x})$ è irriducibile.

$$\text{Anello di polinomi}/(f) \cong \text{ Campo } \Leftrightarrow f \text{ è irriducibile}$$

Capitolo 8

Teoria dei Campi

DEFINIZIONE: Un anello commutativo unitario in cui ogni elemento ($\neq 0$) ha un inverso moltiplicativo si dice *campo*.

8.1 $\mathbb{C}$: il Campo dei Complessi

$$\mathbb{C} = \left\{ a + ib \,|\, a, b \in \mathbb{R}, i^2 = -1 \right\}$$

Esiste un altro modo per rappresentare un numero complesso, usando le *coordinate polari*. In tal modo la moltiplicazione tra complessi risulta più semplice:

$$\begin{cases} \rho = \sqrt{a^2 + b^2} \\ \tan\theta = \frac{b}{a} \end{cases}$$

Per passare invece da coordinate polari a cartesiane si usa le seguenti relazioni:

$$\begin{cases} a = \rho\cos\theta \\ b = \rho\sin\theta \end{cases} \qquad \rho \neq 0 \quad \theta \in \mathbb{R}/2\pi\mathbb{R}$$

Vediamo come si comporta il prodotto nelle 2 rappresentazioni.

$$\begin{aligned} (a+ib)\,(a'+ib') &= aa' - bb' + i\,(ab' + ba') \\ &= \rho\rho'\,(\cos\theta\cos\theta' - \sin\theta\sin\theta' + i\,(\sin\theta\cos\theta' + \cos\theta\sin\theta')) \\ &= \rho\rho'\,(\cos(\theta+\theta') + i\sin(\theta+\theta')) \end{aligned}$$

Quindi rappresentando $\mathbb{C}$ come un prodotto diretto tra i gruppi $\mathbb{R}_+ \times \mathbb{R}/2\pi\mathbb{R}$ si ha che

$$(\rho, \theta)(\rho', \theta') = (\rho\rho', \theta + \theta')$$

RADICI n-ESIME DELL'UNITÀ: L'equazione $x^n = a$ in $\mathbb{C}$ ha n radici distinte se $a \neq 0$, unica radice (quella nulla) se $a = 0$.
Per trovarle passiamo in coordinate polari:

$$\begin{array}{l} a \mapsto (\rho, \theta) \\ x \mapsto (\xi, \omega) \end{array} \Rightarrow x^n \mapsto (\xi^n, n\omega)$$

$$\text{Soluzioni: } \begin{cases} \xi^n = \rho \\ n\omega = \theta \end{cases} \quad \begin{cases} \xi = \sqrt[n]{\rho} \\ \omega = \frac{\theta + 2k\pi}{n} \end{cases} \quad \text{con } k = 0, 1, \ldots, n-1$$

CONIUGIO: L'applicazione $^-: \mathbb{C} \to \mathbb{C}$ tale che $z = a + ib \mapsto \bar{z} = a - ib$ vista nel piano complesso opera come una simmetria rispetto all'asse reale.

8.2 Elementi Algebrici e Trascendenti

DEFINIZIONE: Sia $\mathbb{K}$ un campo. Un insieme V si dice $\mathbb{K}$-spazio vettoriale se è un gruppo abeliano rispetto all'addizione e se l'operazione esterna chiamata prodotto per scalari $\cdot : \mathbb{K} \times V \to V$ ha le seguenti proprietà:

- $\forall\ a, b \in \mathbb{K}$, $\forall\ x \in V\ \ a(bx) = (ab)x$;
- $\forall\ x \in V\ \ 1 \cdot x = x$;
- Le proprietà distributive dell'addizione rispetto al prodotto per scalari e viceversa.

Osservazione. Siano $\mathbb{K} \subseteq \mathbb{F}$ due campi. $\mathbb{F}$ è in modo naturale un $\mathbb{K}$-spazio vettoriale.

DEFINIZIONE: Siano $\mathbb{K} \subseteq \mathbb{F}$ due campi e sia $\alpha \in \mathbb{F}$.

- α si dice *algebrico* su $\mathbb{K}$ se esiste $f(x) \in \mathbb{K}[x]$, $f \neq 0$ tale che $f(\alpha) = 0$;
- α si dice *trascendente* su $\mathbb{K}$ se $\forall\ f \in \mathbb{K}[x]$, $f \neq 0$ si ha $f(\alpha) \neq 0$.

PROPOSIZIONE: Sia α algebrico su $\mathbb{K}$. L'insieme dei polinomio in $\mathbb{K}[x]$ che si annullano in α è costituito dai multipli di un polinomio.

Dimostrazione. Consideriamo $A = \{f \in \mathbb{K}[x] \mid f(\alpha) = 0\}$. $A \neq \{0\}$.
Sia $h(x) \in A$ un polinomio di grado minimo ($h \neq 0$). Dimostriamo che $A = \{\text{multipli di } h\}$.

$\supseteq$. Sia $f = gh$. Allora $f(\alpha) = g(\alpha)h(\alpha) = 0 \ \Rightarrow f \in A$.
$\subseteq$. Divisione Euclidea. Sia $f \in A$, $f = qh + r$. $f(\alpha) = q(\alpha)h(\alpha) + r(\alpha) \Rightarrow 0 = r(\alpha)$. Ma h ha grado minimo, e r ha grado minore. Dunque $r = 0$. $\square$

DEFINIZIONE: Siano $\mathbb{K} \subseteq \mathbb{F}$ due campi, $\alpha \in \mathbb{F}$ algebrico su $\mathbb{K}$. Il polinomio *minimo* di α su $\mathbb{K}$ è il polinomio monico di grado minimo tra quelli che si annullano in α.

PROPOSIZIONE: Siano $\mathbb{K} \subseteq \mathbb{F}$ campi, $\alpha \in \mathbb{F}$ algebrico su $\mathbb{K}$. Allora l'insieme

$$E = \{f(\alpha) \mid f \in \mathbb{K}[x]\}$$

è un campo.
Inoltre $dim_{\mathbb{K}} E$ =grado del polinomio minimo di α su $\mathbb{K}$.

Dimostrazione. Sia $h(x) \in \mathbb{K}[x]$ il polinomio minimo di α su $\mathbb{K}$.
Osserviamo che $f(\alpha) = g(\alpha) \Leftrightarrow h \mid f - g \Leftrightarrow (f-g)(\alpha) = 0$.
Quindi $E = \{r(\alpha) \mid deg(r) < deg(h)$ oppure $r = 0\}$. Si verifica facilmente che E è chiuso rispetto all'addizione e alla moltiplicazione.

Il polinomio minimo di α su $\mathbb{K}$ è irriducibile. Infatti $h(x) = a(x)b(x) \Rightarrow 0 = a(\alpha)b(\alpha)$, ma $deg(a), deg(b) < deg(h)$, quindi è impossibile.
Consideriamo $r(\alpha) \in E$, $r \neq 0$ e applichiamo Bézout: dato che $(r, h) = 1$ allora esistono s, t tali che $rs + ht = 1$.
$\Rightarrow r(\alpha)s(\alpha) = 1$. Quindi $r(\alpha)$ ha un inverso moltiplicativo.

Sia $deg(h) = d$. $h = a_0 + \ldots + a_d x^d$. Allora $E = \left\{c_0 + \ldots + c_{d-1}\alpha^{d-1} \mid c_i \in \mathbb{K} \ \forall\ i\right\}$.
Una base di E è $\left\{1, \alpha, \ldots, \alpha^{d-1}\right\}$: la caratterizzazione precedente di E assicura che lo generino; vediamo che siano linearmente indipendenti. Se $c_0 + \ldots + c_{d-1}\alpha^{d-1} = 0$ allora $g(x) = c_0 + \ldots + c_{d-1}x^{d-1}$ si annulla in α nonostante abbia grado minore del polinomio minimo. Allora $g = 0$. □

Osservazione. In notazione breve $E = \mathbb{K}(\alpha)$.

Osservazione. Siano $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$ e $\alpha \in \mathbb{F}$. Se $dim_{\mathbb{K}}\mathbb{K}(\alpha) = [\mathbb{K}(\alpha) : \mathbb{K}] = d$ allora $[\mathbb{L}(\alpha) : \mathbb{L}] \leq d$. Infatti $h(x) \in \mathbb{K}[x] \subseteq \mathbb{L}[x]$ può non essere il polinomio minimo in $\mathbb{L}[x]$, di sicuro però è un suo multiplo.

PROPOSIZIONE: Sia $\mathbb{K} \subseteq \mathbb{F}$, $\alpha, \beta \in \mathbb{F}$ algebrici su $\mathbb{K}$. Sia $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ e $[\mathbb{K}(\beta) : \mathbb{K}] = m$. $\mathbb{K}(\alpha, \beta)$ è il più piccolo campo contenente α e β. Allora $[\mathbb{K}(\alpha, \beta) : \mathbb{K}] = nm_1$ con $m_1 \leq m$.

PROPOSIZIONE: Siano $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{F}$ campi.

$$\left.\begin{array}{l}[\mathbb{E} : \mathbb{K}] = a \\ [\mathbb{F} : \mathbb{E}] = b\end{array}\right\} \Rightarrow [\mathbb{F} : \mathbb{K}] = ab$$

DEFINIZIONE: Sia $f(x) \in \mathbb{K}[x]$ e siano $\alpha_1, \ldots, \alpha_n$ le sue radici in un campo algebricamente chiuso Ω che contiene $\mathbb{K}$. Si dice *campo di spezzamento* di

$f(x)$ (in Ω) il campo $\mathbb{F} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$.

Osservazione. Se $f(x) \in \mathbb{K}[x]$ ha grado n, è irriducibile e $\mathbb{F}$ è il campo di spezzamento di $f(x)$, allora $[\mathbb{F} : \mathbb{K}] \leq n!$. Inoltre $n \mid [\mathbb{F} : \mathbb{K}]$.

$$\mathbb{K} \underbrace{\subseteq}_{\text{grado } n} \mathbb{K}(\alpha_1) \underbrace{\subseteq}_{\text{grado } \leq n-1} \ldots \subseteq \mathbb{F}$$

8.3 Campi Finiti

PROPOSIZIONE: Per ogni campo con un numero finito di elementi $\mathbb{K}$ esistono un p primo e un $n \geq 1$ tali che $|\mathbb{K}| = p^n$. Per ogni p e per ogni $n \geq 1$ esiste un unico campo con p^n elementi a meno di isomorfismi.

Dimostrazione. Sia $\mathbb{K}$ un campo finito.
$1 \in \mathbb{K}$, quindi esiste un sottogruppo additivo ciclico generato da 1 isomorfo a $\mathbb{Z}_n$ per un certo $n \in \mathbb{N}$.
Poiché $\mathbb{K}$ è finito, ha caratteristica non nulla. Ma essendo un campo esso non ha divisori di 0, quindi la caratteristica è un primo p.
Ciò significa che $\mathbb{Z}_p \subseteq \mathbb{K}$. p è primo, quindi $\mathbb{Z}_p$ è un sottocampo di $\mathbb{K}$ che assume quindi forma di $\mathbb{Z}_p$-spazio vettoriale.
Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di tale spazio vettoriale; allora

$$\mathbb{K} = \{c_1\alpha_1 + \ldots + c_n\alpha_n \mid c_i \in \mathbb{Z}_p \ \forall i\}$$

Da ciò deriva che $|\mathbb{K}| = p^n$.

Costruiamo adesso un campo con p^n elementi.
Consideriamo $\mathbb{K}$ immerso in un campo algebricamente chiuso Ω e consideriamo il polinomio $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ che ha tutte le radici ditinte. Infatti, se ne avesse con molteplicità > 1, avrebbe soluzioni comuni con $f'(x) = p^n x^{p^n - 1} - 1 = -1$.
Sia X l'insieme di tutte le radici di $f(x)$. $|X| = p^n$ ed è un campo (le verifiche sono lasciate). □

Osservazione. Se $|\mathbb{K}| = p^n$ allora $\mathbb{K}$ è costituito dalle radici del polinomio $x^{p^n} - x$.

Dimostrazione. $\mathbb{K} = \{0\} \cup \mathbb{K}^*$.
Sia $\alpha \in \mathbb{K}^*$. Allora $\alpha^{p^n - 1} = 1$ (perchè $ord(\mathbb{K}^*) = p^n - 1$). $\Rightarrow \alpha^{p^n} - \alpha = 0$.
Gli elementi di $\mathbb{K}^* \cup \{0\}$ sono quindi tutte e sole le radici del polinomio $x^{p^n} - x$. □

TEOREMA: In un campo algebricamente chiuso Ω che contiene $\mathbb{Z}/p\mathbb{Z}$ esiste uno e un solo campo di ordine p^n per ogni $n \geq 1$.

TEOREMA: A meno di isomorfismo esiste uno e un solo campo finito di ordine p^n.

PROPOSIZIONE: Sia $\mathbb{K}$ un campo e sia $G < \mathbb{K}^*$ un sottogruppo moltiplicativo finito di $\mathbb{K}$. Allora G è ciclico.

Dimostrazione. Sia $|G| = n$.
Per ogni $d \mid n$ sia n_d il numero di elementi di G di ordine esattamente d.

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

Dimostriamo che esiste un elemento n_n i ordine uguale all'ordine di G.
Vediamo che $n_d = 0$ oppure $n_d = \varphi(d)$. Infatti se $\alpha \neq 0$, $ord(\alpha) = d$ allora $\alpha^d = 1$, cioè α è radice di $x^d - 1$. $\langle\alpha\rangle = \{$insieme delle radici$\}$. In un gruppo ciclico ci sono esattamente $\varphi(d)$ elementi di ordine d.
A questo punto, poiché $\sum_{d|n} \varphi(d) = n$ allora $\varphi(d) = n_d \ \forall \ d$, compreso $d = n$. □

PROPOSIZIONE: Dati $p, n \ \exists \ \alpha \in \mathbb{F}_{p^n}$ tale che $\mathbb{F}_{p^n} = \mathbb{F}(\alpha)$.

Dimostrazione. Basta prendere α un generatore del gruppo ciclico $\mathbb{F}^*_{p^n}$. □

COROLLARIO: $\forall \ p, \forall \ n$ esistono polinomi irriducibili di grado n in $\mathbb{F}_p[x]$.

Dimostrazione. Basta prendere $f(x)$ il polinomio minimo di un α su $\mathbb{F}_p$. □

PROPOSIZIONE: $\mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b} \Leftrightarrow a \mid b$.

Dimostrazione. $\Rightarrow$.
$\mathbb{F}_{p^b}$ è uno spazio vettoriale su $\mathbb{F}_{p^a}$. Sia d la dimensione di questo spazio vettoriale. Allora $\mathbb{F}_{p^b} \cong (\mathbb{F}_{p^a})^d$. Guardando le cardinalità $p^b = p^{ad}$. □

Dimostrazione. $\Leftarrow$.
Basta dimostrare che $x^{p^a} - x \mid x^{p^b} - x$, ossia $x^{p^a-1} - 1 \mid x^{p^b-1} - 1$.
Sia $b = ad$. Allora $p^b - 1 = p^{ad} - 1 = (p^a - 1)(p^{a(d-1)} + \ldots + 1)$. Quindi $p^a - 1 \mid p^b - 1$, cioè $x^{p^a-1} - 1 \mid x^{p^b-1} - 1$. □

8.4 Campi di Spezzamento su $\mathbb{F}_p$

Sia $f(x) \in \mathbb{F}_p[x]$ con f irriducibile di grado n. Siano $\alpha_1, \ldots, \alpha_n$ le radici tutte distinte.

$$\begin{aligned} c.d.s. &= \mathbb{F}_p(\alpha_1, \ldots, \alpha_n) \\ [\mathbb{F}_p(\alpha_1) : \mathbb{F}_p] = n &\Rightarrow \mathbb{F}_p(\alpha_1) = \mathbb{F}_{p^n} \\ \ldots &\Rightarrow \ldots \\ [\mathbb{F}_p(\alpha_n) : \mathbb{F}_p] = n &\Rightarrow \mathbb{F}_p(\alpha_n) = \mathbb{F}_{p^n} \end{aligned}$$

Quindi

$$c.d.s. = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n) = \mathbb{F}_p(\alpha_i) = \mathbb{F}_{p^n}$$

CdS di un polinomio qualisiasi: Sia $f(x) \in \mathbb{F}_p[x]$ polinomio qualsiasi. Sia $f(x) = f_1(x) \cdot \ldots \cdot f_k(x)$ con f_i irriducibili di grado n_i.
Allora i c.d.s. dei fattori sono $\mathbb{F}_{p^{n_i}}$. Il c.d.s. di $f(x)$ invece è $\mathbb{F}_{p^m}$ con $m = mcm\{n_1, \ldots, n_k\}$.

CdS di $x^n - 1$ su $\mathbb{F}_p$: Cerchiamo il c.d.s. di $x^n - 1$ su $\mathbb{F}_p$.

Sia $n = p^a m$, con $(m, p) = 1$. Allora $x^n - 1 = (x^m - 1)^{p^a}$ perché $\mathbb{F}_p$ ha caratteristica p. Quindi il problema equivale a trovare il c.d.s. di $x^m - 1$ con $(m, p) = 1$.
Le radici sono tutte distinte, poichè $f'(x) = mx^{m-1} = 0 \Leftrightarrow x = 0$.
Il c.d.s. è il più piccolo campo che contiene il gruppo ciclico delle radici di $f(x)$.
$c.d.s. = \mathbb{F}_{p^k}$; il gruppo ciclico $\subseteq \mathbb{F}_{p^k}^* \Leftrightarrow k$ =minimo naturale tale che $m \mid p^k - 1$, ossia

$$p^k \equiv 1 \pmod{m}$$

Dunque k è l'ordine di p in $(\mathbb{Z}/m\mathbb{Z})^*$.