# Appunti di Logica e Algebra 2

Pietro Pizzoccheri
Lorenzo Bardelli
https://github.com/PietroPizzoccheri/uni

2024

## Contents

# 1 Teoria degli anelli commutativi e dei campi

## 1.1 Insiemi

Un insieme è una collezione di oggetti, detti elementi dell'insieme.

$$\mathbb{N} := \{0, 1, 2, 3, \cdots\} \quad \text{insieme dei numeri naturali}$$

$$\mathbb{Z} := \{\cdots, -2, -1, 0, 1, 2, \cdots\} \quad \text{insieme degli interi}$$

$$\mathbb{Q} := \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\} \quad \text{insieme dei numeri razionali}$$

$$\mathbb{R} := \text{insieme dei numeri reali}$$

$$\mathbb{C} := \text{insieme dei numeri complessi}$$

### 1.1.1 Operazioni tra insiemi

$$\subseteq \quad \text{inclusione tra insiemi}$$

$$\subsetneq \quad \text{inclusione propria tra insiemi}$$

$$X \subseteq Y \quad \text{si legge "}X\text{ è sottoinsieme di }Y\text{" o "}X\text{ è incluso in }Y\text{"}$$

Se $X$ è un insieme finito, indico con $|X|$ il numero di elementi di $X$, detto anche la **cardinalità di** $X$.

$$\varnothing : \text{Insieme vuoto e } |\varnothing| = 0$$

Siano $X$ e $Y$ due insiemi. L'insieme $X \times Y := \{(x, y) : x \in X, y \in Y\}$ lo chiamiamo **prodotto cartesiano** di $X$ e $Y$.

Sia $A \in \mathcal{P}(x)$, dove $\mathcal{P}(X) := \{A : A \subseteq X\}$ è detto **Insieme delle parti di** $X$. L'insieme $A^c := X \setminus A$ è detto **complementare** di $A$

## 1.2 Funzioni

Siano $X$ e $Y$ due insiemi. **Una funzione** $f$ **da** $X$ **a** $Y$ è un sottoinsieme $F \subseteq X \times Y$ tale che:

- $(x, y_1) \in F$, $(x, y_2) \in F \implies y_1 = y_2$, $\forall x \in X$, $y_1, y_2 \in Y$.
- $x \in X \implies \exists y \in Y$ tale che $(x, y) \in F$

Una funzione $F \subseteq X \times Y$ la indichiamo con $f : X \to Y$. E scriviamo $f(x) = y$ se $(x, y) \in F$.

**Definizione:** *La funzione $Id_x : X \to X$ tale che $Id_x(x) = x, \forall x \in X$ la chiamiamo **funzione identità su** $X$*

**Definizione:** *Una funzione $f : X \to Y$ è **iniettiva** se $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$*

***Definizione:*** *Una funzione $f : X \to Y$ è **suriettiva** se $Im(f) = Y$, dove $Im(f) = \{y \in Y : \exists x \in X$ tale che $f(x) = y\}$ è detta **immagine di** $f$*

***Definizione:*** *Una funzione $f : X \to Y$ è **biunivoca** se è sia iniettiva che suriettiva.*

### 1.2.1 Composizione di funzioni

Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni. La **composizione di $f$ e $g$** è la funzione $g \circ f : X \to Z$ tale che $(g \circ f)(x) = g(f(x))$, $\forall x \in X$.

***Definizione:*** *una funzione $f : X \to Y$ è detta **invertibile** se esiste una funzione $g : Y \to X$ tale che*

- $g \circ f = Id_X$
- $f \circ g = Id_Y$

*la funzione $g$ è detta **funzione inversa di** $f$ e la indichiamo con $f^{-1}$.*

Una funzione $f : X \to Y$ è invertibile se e solo se è biunivoca.

### 1.2.2 Operazioni su insiemi

***Definizione:*** *Una funzione $f : X \times X \to X$ è detta **operazione su** $X$. Invece di $f(x, y)$ scriveremo $x \cdot y$.*

***Definizione:*** *Un'operazione $\cdot$ su $X$ è detta **associativa** se $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall x, y, z \in X$.*

***Definizione:*** *Un'operazione $\cdot$ su $X$ è detta **commutativa** se $x \cdot y = y \cdot x$, $\forall x, y \in X$.*

**Esempio:**

- $\mathcal{P}(X)$con l'operazione di unione $\cup$ è associativa e commutativa, così come lo è con l'intersezione $\cap$.
- $A \backslash B := A \cup B^C$ **(differenza insiemistica)** è un'operazione su $\mathcal{P}(X)$.
  non è associativa: sia $A \neq \varnothing$. Allora $A \backslash (A \backslash A) = A \neq (A \backslash A) \backslash A = \varnothing$
  non è commutativa: $A \backslash \varnothing = A \neq \varnothing \backslash A = \varnothing$, se $A \neq \varnothing$
- $A \Delta B := (A \backslash B) \cup (B \backslash A)$ **(differenza simmetrica)** è un'operazione su $\mathcal{P}(X)$.
  è commutativa e anche associativa, facilmente verificabile coi diagrammi di Venn.
- Sia $F(X) := \{f : X \to X\}$.
  La composizione" $\circ$" è un'operazione su $F(X)$.
  è associativa, ma non è commutativa.
- $a \circ b = \frac{a+b}{2}$ è un'operazione commutativa su $\mathbb{Q}$, ma non associativa.

***Definizione:*** *Sia $\cdot$ un'operazione su $X$. Un elemento $e \in X$ tale che $e \cdot x = x \cdot e = x$, $\forall x \in X$ è detto **elemento neutro** o **identità**.*

L'identità è unica; se $e, e' \in X$ sono due identità, allora $e = e \cdot e' = e'$.

## 1.3 Monoidi e Gruppi

***Definizione:*** *Un insieme $X$ con un'operazione associativa e un'identità è detto* ***monoide****.*

**Esempio:**

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con l'addizione e identità 0 sono monoidi.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la moltiplicazione e identità 1 sono monoidi.
- $\mathcal{P}(X)$ con $\cup$ e come identità l'insieme X è un monoide.
- $\mathcal{P}(X)$ con $\cap$ e come identità l'insieme vuoto è un monoide.
- $F(X) := \{f : X \to X\}$ con la composizione" $\circ$ "e come identità la funzione identità $(Id_X)$ è un monoide.

***Definizione:*** *Sia $X$un monoide. Un elemento $x \in X$ è detto* ***invertibile*** *se esiste $y \in X$ tale che $x \cdot y = y \cdot x = e$, dove $e$ è l'identità di $X$. L'elemento $y$ è detto* ***inverso*** *di $x$.*

Se $x \in X$ è invertibile, il suo inverso è unico e lo indichiamo con $x^{-1}$.
L'identità del monoide è invertibile e il suo inverso è l'identità stessa.

**Esempio:**

- L'insieme degli elementi invertibili di $(\mathbb{N}, +)$ è $\{0\}$.
- Linsieme degli elementi invertibili di $(\mathbb{Z}, +)$ è $\mathbb{Z}$, di $(\mathbb{Q}, +)$ è $\mathbb{Q}$, di $(\mathbb{R}, +)$ è $\mathbb{R}$, di $(\mathbb{C}, +)$ è $\mathbb{C}$.
- L'insieme degli elementi invertibili di $(\mathbb{N}, \cdot)$ è $\{1\}$, di $(\mathbb{Z}, \cdot)$ è $\{1, -1\}$, di $(\mathbb{Q}, \cdot)$ è $\mathbb{Q} \setminus \{0\}$, di $(\mathbb{R}, \cdot)$ è $\mathbb{R} \setminus \{0\}$, di $(\mathbb{C}, \cdot)$ è $\mathbb{C} \setminus \{0\}$.
- L'insieme degli elementi invertibili di $F(X) = \{f : X \to X\}$ è l'insieme delle funzioni invertibili.

***Definizione:*** *Un monoide $X$ è detto* ***gruppo*** *se ogni suo elemento è invertibile. Se l'operazione è commutativa, il gruppo è detto* ***gruppo abeliano****.*

**Esempio:**

- $(\mathcal{P}(x), \Delta)$ è un gruppo abeliano. L'identità è l'insieme vuoto e l'inverso di $A \in \mathcal{P}(x)$ è $A$ stesso. $(A^2 = \varnothing, \forall A \subseteq X)$
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono gruppi abeliani
- $(\mathbb{Q} \backslash \{0\}, \cdot)$, $(\mathbb{R} \backslash \{0\}, \cdot)$, $(\mathbb{C} \backslash \{0\}, \cdot)$ sono gruppi abeliani
- sia $X = \{1, 2, \cdots, n\}$ l'insieme delle funzioni invertibili $f : X \to X$ è il **Gruppo delle permutazioni di n elementi (o gruppo simmetrico)**.Lo indichiamo con $S?n$. $|S_n| = m!$. Non è abeliano se $n \geq 3$.

***Definizione:*** *Sia $X$ un monoide con identità $e$. Un sottoinsieme $Y \subseteq X$ tale che $e \in Y$ e $Y$ è chiuso rispetto all'operazione di $X$ è detto* ***sottomonide di*** *$X$. Analogamente definiamo la nozione di* ***sottogruppo di*** *$X$. il gruppo $\{e\}$ è detto* ***sottogruppo banale di*** *$X$.*

**Esempio:**

- Con l'addizione, $\{0\}$ èun sottomonoide di $\mathbb{N}$. $\{0\}$ è anche sottogruppo banale.
- Con la moltiplicazione abbiamo la catena di sottomonoidi $\{1\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq insiemeR \subseteq \mathbb{C}$ e di sottogruppi $\{1\} \subseteq \mathbb{Q}\backslash\{0\} \subseteq \mathbb{R}\backslash\{0\} \subseteq \mathbb{C}\backslash\{0\}$
- con l'addizione abbiamo la caten di sottogruppi $\{0\} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

***Definizione:*** *Sia $X$ un monoide e $S \subseteq X$ un sottoinsieme. L'insieme $\langle S\rangle := \{x_1 \cdot x_2 \cdots \cdot x_n : n \in \mathbb{N}, x_1, x_2, \cdots, x_n \in S\}$ è detto* ***sottomonoide generato da*** *$S$ (intersezione di utti i sottomonoidi di $X$ che contengono $S$). Se $X$ è un gruppo, $\langle S\rangle$ è detto* ***sottogruppo generato da*** *$S$.*

**Esempio:**

- $S = \{1\} \subseteq (\mathbb{N}, +)$. Allora $\langle S\rangle = \{0, 1, 2, \cdots\} = \mathbb{N}$
- sia $S := \{p \in \mathbb{N} : p \text{ è primo}\} \cup \{0\} \subseteq (\mathbb{N}, \cdot)$. allora $\langle S\rangle = \mathbb{N}$
- $S = \{0, 1\} \subseteq (\mathbb{N}, \cdot)$. Allora $\langle S\rangle = \{0, 1\}$
- sia $S = \{1\} \subseteq (\mathbb{Z}, +)$. il sottogruppo generato da $S$ è $\langle S\rangle = \mathbb{Z}$
- uno spazio ettoriale $V$ è un gruppo abeliano se consideriamo l'operazione di addizione fra vettori. Prendiamo $V = \mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$. Sia $v = (1, 1) \in \mathbb{R}^2$. Il sottogruppo $\langle\{v\}\rangle = \{(n, n) : n \in \mathbb{Z}\}$ è un sottogruppo proprio del sottospazio generato da $\{v\}$. Sia $v_1 = (1, 0)$ ed $v_2 = (0, 1)$, allora il sottogruppo $\langle\{v_1, v_2\}\rangle$ è $\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R} \times \mathbb{R}$

***Definizione:*** *Siano $M_1, M_2$ con identità $e_1, e_2$ rispettivamente. Si definisce prodotto diretto di $M_1$ e $M_2$ l'insieme $M_1 \times M_2$ con l'operazione $(m_1, m_2) \cdot (m_1', m_2') = (m_1 \cdot m_1', m_2 \cdot m_2')$ e identità $(e_1, e_2)$. Analogamente si definisce prodotto diretto di gruppi $G_1 e G_2$.*

L'inverso di una coppia $(a, b) \in G_1 \times G_2$ è $(a^{-1}, b^{-1})$.

## 1.4 Morfismi

***Definizione:*** *Siano $M_1 e M_2$ monoidi con identità $e_1 e e_2$. Una funzione $f : M_1 \to M_2$ è un* ***morfismo di monoidi se:***

- $f(e_1) = e_2$
- $f(xy) = f(x)f(y)$

***Definizione:*** *Siano $G_1 e G_2$ gruppi con identità $e_1 e e_2$. Una funzione $f : G_1 \to G_2$ è un* ***morfismo di gruppi se:***

- $f(e_1) = e_2$
- $f(xy) = f(x)f(y)$

***Definizione:*** *Il* ***nucleo*** *di un morfismo di monoidi $f : M_1 \to M_2$ è il sottomonoide di $M_1$ definito come: $Ker(f) := \{x \in M_1 : f(x) = e_2\}$*

***Definizione:*** *Il nucleo di un morfismo di gruppi $f : G_1 \to G_2$ è il sottogruppo di $G_1$ definito come: $Ker(f) := \{x \in G_1 : f(x) = e_2\}$.* ***Il nucleo è un sottogruppo di*** *$G_1$. e $Im(f)$* ***è un sottogruppo di*** *$G_2$.*

***Definizione:*** *Un* ***isomorfismo di monoidi (e di gruppi)*** *èun morfismo biunivoco, tale che la funzione inversa sia un morfismo.*

**Proposizione:** *Sia $f : M_1 \to M_2$ un morfismo di monoidi. Se $f$ è biunivoco, allora è un isomorfismo. Questo vale anche per i gruppi.*

***Dimostrazione:*** *Dobbiamo far vedere che la funzione inversa $f^{-1} : M_2 \to M_2$ è un morfismo di monoidi. Poiché $f(e_1) = e_2$, allora $f^{-1}(e_2) = e_1$. Siano $x_2, y_2 \in M_2$, allora esistono $x_1, y_1 \in M_1$ tali che $f(x_1) = x_2, f(y_1) = y_2$. Quindi $f^{-1}(f(x_1)f(y_1)) = f^{-1}(f(x_1y_1)) = x_1y_1 = f^{-1}(x_2)f^{-1}(y_2)$*

**Esempio:**

- Siano $M_1 = (\mathcal{P}(X), \cup)$ e $M_2 = (\mathcal{P}(X), \cup)$, dove $X$ è un insieme. Sia $f : M_1 \to M_2$ definita ponendo $f(A) = A^C, \forall A \subseteq X$. la funzione $f$ è biunivoca. Inotre, dalle formule di De Morgan segue che $f(A \cap B) = (A \cap B)^C = A^C \cup B^C = f(A) \cup f(B)$. Quindi $f$ è un isomorfismo di monoidi, poiché $f(X) = X^C = \varnothing$, essendo $X$ l'identità di $M_1$ e $\varnothing$ l'identità di $M_2$.

- Sia $\mathbb{Z}_2 := \{0, 1\}$ con l'operazione definita come: $0+0 = 0, 0+1 = 1+0 = 1, 1+1 = 0$. Sia $X := \{1, 2, \cdots, n\}, n \in \mathbb{N}$. La funzione $f : \mathcal{P}(X) \to \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (n volte) definita da: $f(A) = (a_1, a_2, \cdots, a_n)$, dove $a_i = 1$ se $i \in A$ e $a_i = 0$ se $i \notin A$.
  è un isomorfismo del gruppo $(\mathcal{P}(X), \Delta)$ con il gruppo $\mathcal{P}(X) \to \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 = (\mathbb{Z}_2)^n$

**Vediamo ora come ogni monoide finito è isomorfo a un monoide di matrici quadrate, dove l'operazione è il prodotto righe per colonne.**
Sia $M = \{x_1, \cdots, x_n\}$ un monoide, $|M| = n \in \mathbb{N}$, con identità $e = x_1$. Per ogni $x \in M$ definiamo una matrice $A(x) \in Mat_{n\times n}(\mathbb{Z})$ nel seguente modo: $A(x)_{ij} = 1$ se $x_i \cdot x = x_j$ e $A(x)_{ij} = 0$ altrimenti. La funzione $F : M \to Mat_{n\times n}(\mathbb{Z})$ $(x \mapsto A(x))$ è iniettiva.
Infatti, se $A(x) = a(y)$, allora $A(x)_{i1} = A(y)_{i1}$ , $\forall i \in \{1, \cdots, n\}$.
Quindi se $A(x)_{i1} = A(y)_{i1} = 1$, allora $xx_1 = xe = x = yx_1 = y$.
Risulta inoltre facile vedere che $A(xy) = A(x)A(y)$ (prodotto righe per colonne), ossia che $F$ è un morfismo di monoidi ($Mat_{n\times n}(\mathbb{Z})$ è un monoide con l'operazione di prodotto righe per colonne, la cui identità è la matrice $I_n$).
Quindi $F : M \to Im(F)$ è un isomorfismo di monoidi.

**Esempio:** Sia $M = (\mathbb{Z}_2, \cdot)$ il monoide definito da:

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

costruiamo un sottomonoide di $Mat_{4\times 4}(\mathbb{Z})$ isomorfo a $M \times M = \{(0,0),(0,1),(1,0),(1,1)\}$.

$$(0,0) \mapsto \begin{bmatrix} 1&1&1&1\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{bmatrix}, \quad (0,1) \mapsto \begin{bmatrix} 1&0&1&0\\0&1&0&1\\0&0&0&0\\0&0&0&0 \end{bmatrix}, \quad (1,0) \mapsto \begin{bmatrix} 1&1&0&0\\0&0&0&0\\0&0&1&1\\0&0&0&0 \end{bmatrix},$$
$$(1,1) \mapsto \begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{bmatrix}.$$

| $\cdot$ | $(0,0)$ | $(0,1)$ | $(1,0)$ | $(1,1)$ |
|---|---|---|---|---|
| $(0,0)$ | $(0,0)$ | $(0,0)$ | $(0,0)$ | $(0,0)$ |
| $(0,1)$ | $(0,0)$ | $(0,1)$ | $(0,0)$ | $(0,1)$ |
| $(1,0)$ | $(0,0)$ | $(0,0)$ | $(1,0)$ | $(1,0)$ |
| $(1,1)$ | $(0,0)$ | $(0,1)$ | $(1,0)$ | $(1,1)$ |

Si può verificare direttamnete che le matrici hanno la stessa tabella moltiplicativa. (fine esempio)

Abbiamo quindi visto che un monoide finito di cardinalità $n$ è isomorfo a un monoide di matrici $n \times n$ le cui colonne hanno un unico "1" e altrove sono "0".
Ognuna di queste matrici può essere vista come una funzione da $X = \{1, \cdots, n\} in X$ :

$$A_{ij} = 1 \Leftrightarrow f(j) = i$$

$$A_{ij} = 0 \Leftrightarrow f(j) \neq i$$

Il prodotto righe per colonne corrisponde alla composizione di funzioni.
Quindi un monoide finito di cardinalità $n$ è isomorfo a un sottomonide del monoide delle funzioni $f$ da $\{1, \cdots, n\}$ in $\{1, \cdots, n\}$ con l'operazione di composizione.

Notiamo che un elemento $x \in M$ di un monoide finito M è invertibile se e solo se la matrice associata è invertibile (una matrice $A \in Mat_{n\times n}(\mathbb{Z})$ è invertibile se e solo se il suo determinante è invertibile su $\mathbb{Z}$, ossia se e solo se $det(a) \in \{-1, 1\}$).

Da ciò segue che un gruppo finito $G$ di cardinalità $|G| = n$, è isomorfo a un gruppo di matrici le cui componenti sono"0" e "1" e che hanno un unico "1" in ogni riga e ogni colonna (matrici di permutazioni).
Il gruppo $G$ è inoltre isomorfo a un sottogruppo del gruppo delle funzioni biunivoche da $\{1, \cdots, n\}$ in $\{1, \cdots, n\}$, che abbiamo chiamato **gruppo simmetrico** $S_n$.
Gli elementi di $S_n$ in notazione a una linea sono indicati nel modo seguente: sia $\sigma \in S_n$ una funzione biunivoca da $\{1, \cdots, n\}$ in $\{1, \cdots, n\}$, allora $\sigma$ è indicata come $\sigma(1)\sigma(2)\cdots\sigma(n)$.

***Teorema*** (Teorema di Cayley)**:** *Ogni sottogruppo finito di cardinalità $n \in \mathbb{N} \backslash \{0\}$ è isomorfo a un sottogruppo di $S_n$*

**Esempio:**

- $S_2 = \{12, 21\}$
  $S_3 = \{123, 132, 213, 231, 312, 321\}$

- vediamo il gruppo $(\mathbb{Z}_2, +)$ come gruppo di matrici e come gruppo di permutazioni.
  $(\mathbb{Z}_2, +) \simeq \{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\} \simeq \{12, 21\} = S_2$ ($\simeq$ : isomorfismo di gruppi)

## 1.5 Relazioni

***Definizione:*** *Sia $X$ un insieme. Un sottoinsieme $R \subseteq X \times X$ è detto **relazione su** $X$.*

***Definizione:*** *Una relazione $R \subseteq X \times X$ è detta **relazione di equivalenza** se soddisfa le seguenti proprietà:*

- ***riflessità***: $(x, x) \in R$, $\forall x \in X$
- ***simmetria***: $(x, y) \in R \implies (y, x) \in R$, $\forall x, y \in X$
- ***transitività***: $(x, y) \in R$ e $(y, z) \in R \implies (x, z) \in R$, $\forall x, y, z \in X$

Se $R$ è una relazione di equivalenza su $X$ e $(x, y) \in R$, scriviamo $x \sim y$, che si legge "$x$ è equivalente a $y$".

***Definizione:*** *Sia $X$ un insieme e $R \subseteq X \times X$ una relazione di equivalenza su $X$. L'insieme $[x]_R := \{y \in X : x \sim y\}$ è detto **classe di equivalenza di** $x$ **rispetto a** $R$.*

***Definizione:*** *L'insieme ${}^{X}/_{\sim} := \{[x] : x \in X\}$ è detto **insieme quoziente**.*

***Definizione:*** *La funzione $\pi : X \to {}^{X}/_{\sim}$ , $x \mapsto [x]$ è detta **proiezione canonica**.*

***Definizione:*** *Siano $x, y \in X$. Allora se $x \sim y$ abbiamo che $[x] = [y]$. Se $x \nsim y$ abbiamo che $[x] \cap [y] = \varnothing$. Quindi $X = \biguplus_{[x] \in {}^{X}/_{\sim}} [x]$, ossia ${}^{X}/_{\sim}$ è una partizione di X.*

**Esempio:**

- L'uguaglianza " $=$ " è una relazione di equivalenza su ogni insieme $X$.

- Sia $X = \{1, 2, \cdots, n\}$. Definiamo si $\mathcal{P}(X)$ la seguente relazione: $A \sim B \Leftrightarrow |A| = |B|, \forall A, B \subseteq X$. Questa è una relazione di equivalenza e ${}^{\mathcal{P}(X)}/_{\sim} \equiv \{0, 1, \cdots, n\}$. Se $A \subseteq X$ è tale che $|A| = k \leq n$ allora $|[A]| = \binom{n}{k} := \frac{n!}{k!(n-k)!}$

- Sia $G$ un gruppo e $H \subseteq G$ un sottogruppo. La relazione $\sim$ su $G$ definita da $g_1 \sim g_2 \Leftrightarrow g_1 = g_2 h$ per qualche $h \in H$ è una relazione di equivalenza.

  - $g \sim g : g \cdot e$ , $\forall g \in G, e \in H$
  - $g_1 \sim g_2 \to g_2 \sim g_1 : g_1 = g_2 h \to g_1 h^{-1} = g_2$ $(h^{-1} \in H)$

- $g_1 \sim g_2, g_2 \sim g_3 \to g_1 \sim g_3 : g_1 = g_2 h, g_2 = g_3 h' \to g_1 = g_3 h h' = g_3 h'', \forall g_1, g_2, g_3 \in G$

In questo caso l'insieme quoziente lo indichiamo con ${}^{G}\!/\!{}_{H}$.

***Definizione:*** *Il numero* $\binom{n}{k}$ *è chiamato* ***coefficiente binomiale****, questo perché* $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^n y^{n-k}, \forall x, y \in \mathbb{C}$

## 1.6 Insieme quoziente per gruppi abeliani

Se $G$ è un gruppo abeliano, possiamo definire la seguente operazione "+" su ${}^{G}\!/\!{}_{H}$: $[g_1] + [g_2] := [g_1 + g_2]$, vediamo che è ben definita: se $g_1' = g_1 + h_1$ e $g_2' = g_2 + h_2$, allora $[g_1'] = [g_1]$, $[g_2'] = [g_2]$ e $g_1' + g_2' = g_1 + h_1 + g_2 + h_2 = g_1 + g_2 + h$, dove $h = h_1 + h_2 \in H$. Quindi $[g_1' + g_2'] = [g_1 + g_2]$. L'operazione è ovviamente associativa e commutativa, perché lo è quella su $G$. Inoltre $[g] + [0] = [g]$, $\forall [g] \in {}^{G}\!/\!{}_{H}$ dove con "0" abbiamo indicato l'identità di $G$. Quindi la classe $[0]$ dell'identità di $({}^{G}\!/\!{}_{H}, +)$. Infine $[g] + [-g] = [g - g] = [0]$, dove con $-g$ abbiamo indicato l'inverso di $g$ in $G$. Quindi $-[g] = [-g], \forall [g] \in {}^{G}\!/\!{}_{H}$, ossia $({}^{G}\!/\!{}_{H}, +)$ è un gruppo abeliano.

**Esempio:**

- Se $H = \{0\} \subseteq G$, allora ${}^{G}\!/\!{}_{H}$ è isomorfo a $G$. ($\{0\}$ gruppo banale e $G$ gruppo abeliano)
- Sia $G = (\mathbb{Z}, +)$ e $n \in \mathbb{N}$. Il sottoinsieme $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ è un sottogruppo di $\mathbb{Z}$.
  - $0\mathbb{Z} = \{0\}$
  - $1\mathbb{Z} = \{\mathbb{Z}\}$
  - $2\mathbb{Z} = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$
  - $3\mathbb{Z} = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$

  Definiamo il gruppo abeliano $\mathbb{Z}_n := {}^{\mathbb{Z}}\!/\!{}_{n\mathbb{Z}}$, per $\mathbb{Z}_0 = {}^{\mathbb{Z}}\!/\!{}_{0\mathbb{Z}} = {}^{\mathbb{Z}}\!/\!{}_{\{0\}} = \mathbb{Z}$.
  Sia $n \geq 0$ e siano $x, y \in \mathbb{Z}$.

  - Allora $x \sim y \Leftrightarrow x = y + h$ $(h \in n\mathbb{Z}) \Leftrightarrow x - y = kn$ (per $k \in \mathbb{Z}$) $\Leftrightarrow$ il resto della divisione di $x$ per $n$ è uguale al resto della divisione di $y$ per $n$.

  I possibili resti della divisione per $n$ sono $0, 1, \cdots, n-1$.
  Quindi $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$. ($\{[0], [1], \cdots, [n-1]\}$ sono le classi di resto)

  - $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, $\overline{1} + \overline{1} = [1+1] = [2] = [0]$

| + | $\overline{0}$ | $\overline{1}$ |
|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{0}$ |

  - $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$,

***Definizione:*** *Sia $G$ un gruppo abeliano e $H \subseteq G$ un sottogruppo. La proiezione canonica $\pi : G \to {}^{G}\!/\!{}_{H}$ è un* ***morfismo suriettivo di gruppi***

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{0}$ | $\overline{1}$ |

Se $G$ è un gruppo finito e $H \subseteq G$ è un sottogruppo, allora $[g] \in {}^{G}/_{H} \to |[g]| = |H|$.
Infatti $[g] = \{gh : h \in H\}$ e $gh_1 = gh_2 \to h_1 = h_2$.
Poiché le classi di quivalenza sono una partizione di G , abbiamo $|G| = |{}^{G}/_{H}| \cdot |H|$.
In particolare la cardinalità o (**ordine**) di un sottogruppo di un gruppo finito divide la cardinalità del gruppo.

**Teorema:** *Sia $f : G_1 \to G_2$ un morfismo di gruppi. Allora $f$ è iniettivo se e solo se $Ker(f) = \{e_1\}$.*
*(Questo non vale per i morfismi di monoidi.)*

**Dimostrazione:** *Sia $f$ iniettivo. Sia $x \in Ker(f)$. Allora $f(x) = e_2$ e quindi, poiché anche $f(e_1) = e_2$, si ha che $x = e_1$ per l'ipotesi di iniettività.*
*Sia $Ker(f) = \{e_1\}$. Siano $x, y \in G_1$ tali che $f(x) = f(y)$.*
*Allora $f(x)f(y^{-1}) = e_2 \to f(xy^{-1}) = e_2 \to xy^{-1} \in Ker(f) \to xy^{-1} = e_1 \to x = y$,*

**Esempio:**

- $G = \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$,
  - $\langle\overline{0}\rangle = \overline{0}$ sottogruppo banale $\simeq \mathbb{Z}_1$
  - $\langle\overline{1}\rangle = \mathbb{Z}_4$
  - $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}\} \simeq \mathbb{Z}_2$ $(2 + 2 = 0)$
  - $\langle\overline{3}\rangle = \mathbb{Z}_4$ $(3, 3 + 3 = 6 = 2, 3 + 2 = 5 = 1, 3 + 1 = 4 = 0)$

  I sottogruppi di $\mathbb{Z}_4$ possono averer cardinalità $1, 2, 4$. L'insieme dei sottogruppo di $\mathbb{Z}_4$ è $\{\{\overline{0}\}, \{\overline{0}, \overline{2}\}, \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4\}$

- $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$,
  - $\langle\overline{0}\rangle = \overline{0}$ sottogruppo banale $\simeq \mathbb{Z}_1$
  - $\langle\overline{1}\rangle = \mathbb{Z}_6$
  - $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}\} \simeq \mathbb{Z}_3$
  - $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}\} \simeq \mathbb{Z}_2$
  - $\langle\overline{4}\rangle = \{\overline{0}, \overline{2}, \overline{4}\} \simeq \mathbb{Z}_3$
  - $\langle\overline{5}\rangle = \mathbb{Z}_6$

  I sottogruppi di $\mathbb{Z}_6$ possono averer cardinalità $1, 2, 3, 6$. L'insieme dei sottogruppo di $\mathbb{Z}_6$ è $\{\{\overline{0}\}, \{\overline{0}, \overline{2}, \overline{4}\}, \{\overline{0}, \overline{3}\}, \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \mathbb{Z}_6\}$

**Caso generale:** consideriamo il gruppo $\mathbb{Z}_n = (\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}, +)$ sia $m \in \mathbb{N}, m < n$.
Se $m = 0$, $\langle\overline{0}\rangle = \{\overline{0}\}$.
Sia $m > 0$ e $z := \frac{mcm\{m,n\}}{m}$. (mcm = minimo comune multiplo)

$\overline{m}+\overline{m}+\cdots=\overline{m}=\overline{zm}=\overline{mcm\{m,n\}}=\overline{0}$

Se $i \leq i \leq z$: $im < zm = mcm\{m,n\} \rightarrow n$ non divide $im$.

$\overline{m}+\overline{m}+\cdots=\overline{m}=\overline{im}\neq\overline{0}$ perché $im$ è multiplo di $m$ e $im < mcm\{m,n\}$, quindi $im$ non è multiplo di $n$. Dunque $|\langle\overline{m}\rangle| = z = \frac{mcmc\{m,n\}}{m}$.

In particolare, $\langle\overline{m}\rangle = \mathbb{Z}_n \Leftrightarrow z = n \Leftrightarrow MCD\{m,n\} = 1$. Ossia **l'insieme $\{\overline{m}\}$ genera il gruppo $\mathbb{Z}_n$ sse $m$ e $n$ sono coprimi.**

***Definizione:*** *La funzione definita da $\varphi : \mathbb{N}\backslash\{0\} \rightarrow \mathbb{N}\backslash\{0\}$ ,*
*$\varphi(n) := |\{m \in \mathbb{N}\backslash\{0\} : m < n$ e $MCD\{m,n\} = 1\}|$ è detta **funzione di Eulero**.*
*Quindi ci sono $\varphi(n)$ elementi $\overline{m}$ tali che $\langle\overline{m}\rangle = \mathbb{Z}_n$.*

**Proposizione:** *L'insieme dei sottogruppi di $(\mathbb{Z},+)$ è $\{n\mathbb{Z} : n \in \mathbb{N}\}$.*

***Dimostrazione:*** *Sia $H \subseteq \mathbb{Z}$ un sottogruppo non banale.*
*Sia $k := min(H_{>0})$ dove $H_{>0} := \{h \in H : h > 0\}$.*
*Sia $h \in H_{>0}, h \neq k$.*
*Allora $h > k$ e $h = nk + r$, $n \in \mathbb{N}, 0 \leq r < k$.*
*Dunque $r = h - nk \in H \rightarrow r = 0$ per la minimalità di $k$.*

***Definizione:*** *Un gruppo $G$ è detto **ciclico** se esiste $g \in G$ tale che $\langle g\rangle = G$.*
*Un gruppo ciclico è anche abeliano*

**Esempio:**

- $\mathbb{Z} = \langle 1\rangle$ è ciclico
- $\mathbb{Z}_n = \langle\overline{1}\rangle$ è ciclico
- $\mathbb{Z}\times\mathbb{Z} = \langle(1,0),(0,1)\rangle$ non è ciclico, infatti in $\mathbb{Z}\times\mathbb{Z}$, se $(a,b) \in \mathbb{Z}\times\mathbb{Z}$, $\langle(a,b)\rangle = \{(ka,kb) : k \in \mathbb{Z}\} = \{(x,y) : a$ divide $x, b$ divide $y\} \subsetneq \mathbb{Z}\times\mathbb{Z}$.
- $\mathbb{Z}_2\times\mathbb{Z}_2$ non è ciclico. Infatti, in $\mathbb{Z}_2\times\mathbb{Z}_2$ si ha:
  - $\langle(\overline{0},\overline{0})\rangle = \{(\overline{0},\overline{0})\}$
  - $\langle(\overline{0},\overline{1})\rangle = \{\overline{0}\}\times\mathbb{Z}_2$
  - $\langle(\overline{1},\overline{0})\rangle = \mathbb{Z}_2\times\{\overline{0}\}$
  - $\langle(\overline{1},\overline{1})\rangle = \{(\overline{0},\overline{0}),(\overline{1},\overline{1})\}$

  Quindi nessun elemento di $\mathbb{Z}_2\times\mathbb{Z}_2$ genera $\mathbb{Z}_2\times\mathbb{Z}_2$.

***Teorema*** **(di isomorfismo per gruppi abeliani)*:*** *Sia $f : G_1 \rightarrow G_2$ un morfismo di gruppi abeliani. Allora esiste un morfismo iniettivo $\varphi : {}^{G_1}/_{Ker\varphi} \rightarrow G_2$ tale che il seguente diagramma è commutativo:*

$$\begin{tikzcd} G_1 \arrow[r, "f"] \arrow[d, "\pi"'] & G_2 \\ {}^{G_1}/_{Ker(f)} \arrow[ur, "\varphi"'] & \end{tikzcd}$$

*In particolare, ${}^{G_1}/_{Ker(f)} \simeq \Im(f)$.*

***Dimostrazione:*** *L'assegnazione* $[g] \mapsto f(g), \forall g \in G$, *definisce una funzione* $\varphi : {}^{G_1}/_{Ker(f)} \to G_2$.
*Infatti, se* $g' \sim g$, *ossia* $[g] = [g']$, *allora* $g = g' + h, h \in Ker(f)$.
*Dunque* $f(g) = f(g' + h) = f(g') + f(h) = f(g')$. *Poiché* $f$ *è morfismo di gruppi, anche* $\varphi$ *lo è.*
*Inoltre* $Ker(f) = \{[g] \in {}^{G}/_{Ker(f)} : \varphi([g]) = O_2\} = \{[g] \in {}^{G}/_{Ker(f)} : f(g) = O_2\} = [O_1]$.
*Quindi* $\varphi$ *è iniettiva.*
*Infine,* $\varphi : {}^{G_1}/_{Ker(f)} \to Im(f)$ *è un morfismo di gruppi, iniettivo e suriettivo, quindi un isomorfismo.*

**Teorema:** Sia $G$ un gruppo ciclico. Allora ogni sottogruppo di $G$ è ciclico.

***Dimostrazione:*** *Sia* $g \in G$ *tale che* $g = \langle g \rangle$. *La funzione* $\varphi : (\mathbb{Z}, +) \to G$ *definita da* $\varphi(g) = g^n, \forall n \in \mathbb{Z}$, *è un morfismo suriettivo di gruppi.*

- *$G$ è infinito: allora* $Ker(f) = \{0\}$ *e quindi* $\varphi$ *è iniettivo. Dunque* $\varphi$ *è un isomorfismo di gruppi. Tutti i sottogruppi di* $\mathbb{Z}$ *sono ciclici.*

- *$G$ è finito: sia* $H \subseteq G$ *un sottogruppo. Allora* $\varphi^{-1}(H) := \{n \in \mathbb{Z} : \varphi(n) \in H\} \subseteq \mathbb{Z}$ *è un sottogruppo di* $\mathbb{Z}$, *quindi esiste* $\varphi^{-1}(H) = \langle k \rangle$ *con* $k \in \mathbb{N}$.
  *La restrizione* $\varphi : k\mathbb{Z} \to H$ *è un morfismo suriettivo di gruppi e* $\varphi(hk) = \varphi(\underbrace{k + k + \cdots + k}_{h\ volte}) = \varphi(k)\varphi(k)\cdots\varphi(k) = [\varphi(k)]^h, \forall h \in \mathbb{Z}$. *Quindi* $H = \langle \varphi(k) \rangle$.

**Corollario:** L'insieme dei sottogruppi di $\mathbb{Z}_n, n \in \mathbb{N}$ è $\{\langle \overline{m} \rangle : \overline{m} \in \mathbb{Z}_n\}$.

**Proposizione:** *Sia* $n \in \mathbb{N}$ e *sia* $d/n$ *(d divide n). Allora esiste al più un unico sottogruppo di* $\mathbb{Z}_n$ *di cardinalità* $d$.

***Dimostrazione:*** *Sia* $H \subseteq \mathbb{Z}_n$ *sottogruppo tale che* $|H| = d$. *Si considerino le proiezioni canoniche* $\mathbb{Z} \to^{\pi_1} \mathbb{Z}_n \to^{\pi_2} {}^{\mathbb{Z}_n}/_H$.
*Poiché* $\pi_1^{-1}(H) = \{m \in \mathbb{Z} : \pi_1(m) \in H\}$ *è un sottogruppo di* $\mathbb{Z}$, *allora esiste* $k \in \mathbb{N}$ *tale che* $\pi_1^{-1}(H) = k\mathbb{Z}$. *Inoltre* $Ker(\pi_1 \cdot \pi_2) = \pi_1^{-1}(H)$ *e quindi, essendo* $\pi_1 \cdot \pi_2$ *un morfismo suriettivo di gruppi,* ${}^{\mathbb{Z}_n}/_H \simeq {}^{\mathbb{Z}}/_{\pi^{-1}(H)} = {}^{\mathbb{Z}}/_{k\mathbb{Z}} = \mathbb{Z}_k$.
*Quindi* $|\mathbb{Z}_k| = k = |{}^{\mathbb{Z}_n}/_H| = {}^{|\mathbb{Z}_n|}/_{|H|} = \frac{n}{d}$, *ossia* $k$ *è univocamente determinato, e allora* $H = \pi_1(k\mathbb{Z})$ *è univocamente determinato.*

**Esempio:** I sottogruppi di $\mathbb{Z}_{899}$ sono quattro, perché $899 = 31 \cdot 29$, quindi c'è un sottogruppo di cardinalità 1 (il sottogruppo banale), uno di cardinalità 31, uno di cardinalità 29 e $\mathbb{Z}_{899}$.
Sono: $\{\{0\}, \langle \overline{29} \rangle, \langle \overline{31} \rangle, \mathbb{Z}_{899}\}$.

## 1.7 Anelli

**Definizione:** *Sia* $X$ *un insieme su cui sono definite due operazioni* $+$ *e* $\cdot$.
$X$ *è un* ***anello*** *con unità* $1_X$ *se:*

- $(X, +)$ *è un gruppo abeliano*

- $(X, \cdot)$ *è un monoide con unità* $1_X$

- *vale la proprietà distributiva:*
  - $a \cdot (b + c) = a \cdot b + a \cdot c$
  - $(a + b) \cdot c = a \cdot c + b \cdot c$ , $\forall a, b, c \in X$

**Definizione:** *Diaciamo che un anello $X$ è **commutativo** se il monoide $(X, \cdot)$ è commutativo.*

Indichiamo con "0" l'identità del gruppo $(X, +)$.

**Esempio:**

- Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con le operazioni di addizione e moltiplicazione sono anelli commutativi con unità, che è il numero "1".
- L'insieme delle matrici $n \times n, n > 1$ a valori su $\mathbb{Z}$, su $\mathbb{Q}$, su $\mathbb{R}$ o su $\mathbb{C}$, con l'operazione di somma e il prodotto righe per colonne, è un anello **non commutativo**, con unità la matrice identità.
  In generale, se $A$ è un anello commutativo con unità, l'insieme $Mat_{n \times n}(A)$ delle matrici a valori in $\mathbb{R}$ con le operazioni di somma e prodotto righe per colonne, è un anello non commutativo con unità.
- $\{X\}$ è un anello, detto **anello nullo**. Le due operazioni sono la stessa e $0 = 1_{\{X\}} = x$.

Considereremo sempre $0 \neq 1_A$ e studieremo solo anelli commutativi con unità. Quindi quando diremo "anello" intendiamo "anello con unità".

**Definizione:** *Sia $A$ un anello commutativo. Un elemento $x \in A$ è detto **zero divisore** se esiste $y \in A \backslash \{0\}$ tale che $xy = 0$.*

**Definizione:** *Diciamo che un elemento $x \in A$ è **invertibile** se è un elemento invertibile del monoide $(A, \cdot)$.*

**Proposizione:** *Sia $A$ un anello commutativo. Allora l'insieme degli elementi invertibili di $A$ è disgiunto dall'insieme degli zero-divisori di $A$.*

***Dimostrazione:*** *Siano $x, y \in A$ tali che $xy = 0$. Se $X$ è invertibile, allora $x^{-1}xy = y = 0$, quindi $x$ non è uno zero-divisore.*

**Proposizione (legge di cancellazione):** *Sia $A$ un anello commutativo e sia $x \in A$ un elemento che non è uno zero-divisore. Allora $xy = xz \rightarrow y = z, \forall y, z \in A$.*

***Dimostrazione:*** *Se $xy = xz$ allora $x(y - z) = 0$. Poiché $x$ non è uno zero-divisore, allora $y - z = 0$, ossia $y = z$.*

**Definizione:** *Un anello commutativo privo di zero-divisori non nulli è detto **dominio di integrità**.*

**Definizione:** *Un anello commutativo i cui elementi non nulli sono tutti invertibili è detto **campo**.*

**Esempio:** L'anello $\mathbb{Z}$ è un dominio di integrità, ma non è un campo.
Gli anelli $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi.

## 1.8 Ideali

**Definizione:** *Sia $A$ un anello commutativo. Un sottoinsieme $I \subseteq A$ è detto* **ideale** *di $A$ se:*

- *$I$ è un sottogruppo di $(A, +)$*
- *$ax \in I, \forall a \in A, x \in I$*

**Esempio:** Abbiamo già visto che ogni sottogruppo di $(\mathbb{Z}, +)$ è del tipo $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$, dove $n \in \mathbb{N}$. Inoltre, se $a \in \mathbb{Z}$ e $x \in n\mathbb{Z}$, ossia $x = kn$ per qualche $k \in \mathbb{Z}$, si ha che $ax = akn \in n\mathbb{Z}$. Quindi $n\mathbb{Z}$ è un ideale di $\mathbb{Z}, \forall n \in \mathbb{N}$, e tutti gli ideali di $\mathbb{Z}$ sono di questo tipo.

**Osservazioni:** Siano $I, J \subseteq A$ ideali di un anello commutativo $A$.
Allora :

- $I \cap J$ è un ideale di $A$
- $I + J := \{x + y : x \in I, y \in J\}$ è un ideale di $A$
- $IJ := \langle\{xy : x \in I, y \in J\}\rangle$ è un ideale di $A$

**Definizione:** *Sia $S \subseteq A$ un sottoinsieme di un anello commutativo.* ***L'ideale generato da*** *$S$ è l'intersezione di tutti gli ideali di $A$ che contengono $S$ e lo indichiamo con $\langle S\rangle$.*
*Se $S = \{x\}$, diciamo che $\langle S\rangle$ è* ***l'ideale principale generato da*** *$x \in A$.*

**Esempio:** Abbiamo visto che gli ideali di $\mathbb{Z}$ sono tutti e soli i sottoinsiemi $n\mathbb{Z} = \langle n\rangle, n \in \mathbb{N}$. Quindi gli ideali di $\mathbb{Z}$ sono tutti principali.

**Definizione:** *un anello i cui ideali sono tutti principali si dice* ***anello ad ideali principali****.*

**Proposizione:** *Sia $A$ un anello commutativo e $I \subseteq A$ un ideale.*
*Allora:*

- *$I = A$ se e solo se $I$ contiene un elemento invertibile*
- *$A$ è un campo sse i suoi unici ideali sono $\langle 0\rangle$ e $A = \langle 1_A\rangle$*

***Dimostrazione:***

- *se $I = A$ allora $1_A \in I$ e $1_A$ è invertibile.*
  *Sia $u \cap I$ un elemento invertibile. Allora $u^{-1} \cap A$ e quindi $1_A uu^{-1} \in I$. Ne segue che $A = \langle 1_A\rangle \subseteq I$. e quindi $I = A$.*
- *Sia $A$ un campo e sia $I \neq \langle 0\rangle$.*
  *se $n \in I$ e $x \neq 0$ allora $x$ è invertibile e quindi $I = A$ per il punto sopra.*
  *Viceversa, se $\langle 0\rangle$ e $A$ sono gli unici ideali di $A$, e se $x \in A\backslash\{0\}$, allora $\langle X\rangle = \langle 1_A\rangle$, ossia $ax = 1_A$ per qualche $a \in A$. Quindi $x$ è invertibile.*

## 1.9 Anelli quoziente

Sia $A$ un anello commutativo e $I \subseteq A$ un ideale.
In particolare, $A$ con l'operazione " $+$ " è un gruppo abeliano e $I$ è un sottogruppo di $A$. Allora possiamo definire il gruppo quoziente ${}^{A}\!/\!_{I}$.
Con l'operazione $[x] \cdot [y] := [xy]$, per ogni $[x],[y] \in {}^{A}\!/\!_{I}$, abbiamo che ${}^{A}\!/\!_{I}$ è un anello commutativo con unità $[1_A]$.
Infatti, mostriamo che l'operazione è ben definita. Siano $x' \in [x]$ e $y' \in [y]$. Allora esistono $i_x \in I$ e $i_y \in I$ tali che $x' = x + i_x$ e $y' = y + i_y$.
Quindi $x'y' = (x+i_x)(y+i_y) = xy + \underbrace{xi_y + yi_x + i_x i_y}_{\in I \text{ perchè } I \text{ è un ideale di } A}$
Quindi $[x'y'] = [xy]$.
Inoltre $[1_A][x] = [1_A x] = [x]$, per ogni $[x] \in {}^{A}\!/\!_{I}$, quindi $[1_A]$ è l'unità di ${}^{A}\!/\!_{I}$.

**Esempio:** Abbiamo visto che $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ è un ideale dell'anello $\mathbb{Z}$. Quindi il quoziente $\mathbb{Z}_n = {}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ ha la struttura di anello.

- $\mathbb{Z}_0 \simeq \mathbb{Z}$
- $\mathbb{Z}_1 \simeq \{0\}$ anello nullo.
- $\mathbb{Z}_2 \simeq \{\overline{0}, \overline{1}\}$

| $\cdot$ | $\overline{0}$ | $\overline{1}$ |
|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ |

- $\mathbb{Z}_3 \simeq \{\overline{0}, \overline{1}, \overline{2}\}$ è un campo perchè $\overline{1}$ è invertibile e $\overline{2} \cdot \overline{2} = \overline{1}$, quindi anche $\overline{2}$ è invertibile.

| $\cdot$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{1}$ |

- $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ dove $\overline{2} \cdot \overline{2} = \overline{0}$, quindi $\mathbb{Z}_4$ non è un dominio di integrità.
  In particolare non è un campo.

| $\cdot$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{0}$ | $\overline{2}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Vediamo che $\mathbb{Z}_n$ è un campo se e solo se $n \in \mathbb{N} \backslash \{0,1\}$ è un numero primo (per $n = 0$ abbiamo $\mathbb{Z}_0 \simeq \mathbb{Z}$ e per $n = 1$ abbiamo l'anello nullo).
Un ideale di $\mathbb{Z}_n$ è un sottogruppo di $\mathbb{Z}_n$.
Poiché $\mathbb{Z}_n$ è ciclico, i suoi sottogruppi sono ciclici e sono $\{\langle \overline{m} \rangle : \overline{m} \in \mathbb{Z}_n\}$. Inoltre $\langle \overline{m} \rangle \subseteq \mathbb{Z}_n$

è un ideale, $\forall \overline{m} \in \mathbb{Z}_n$. Infatti, se $\overline{a} \in \mathbb{Z}$, allora $\overline{a}\overline{m} = \overline{am} = \underbrace{\overline{m} + \overline{m} + \cdots + \overline{m}}_{a \text{ volte}} \in \langle \overline{m} \rangle$
Quindi $\{\langle \overline{m} \rangle : \overline{m} \in \mathbb{Z}_n\}$ è l'insieme degli ideali di $\mathbb{Z}_n$ ($\mathbb{Z}_n$ è anello ad ideali principali).
Inoltre, se $n > 1, \{\langle \overline{m} \rangle \overline{m} \in \mathbb{Z}_n\} = \{\{\overline{0}\}, \mathbb{Z}_n\} \cup \{\langle \overline{m} \rangle : MCD_{m \neq 0}\{m, n\} \neq 1\}$
Quindi $\mathbb{Z}_n$ è un campo se e solo se $\{\langle \overline{m} \rangle : \overline{m} \in \mathbb{Z}_n\} = \{\{\overline{0}\}, \mathbb{Z}_n\}$ se e solo se $n$ è un numero primo.

**Esempio:** $\mathbb{Z}_3$ è un campo, si ha che $\overline{2}^{-1} = \overline{2}$. Infatti $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$.
Invece $\mathbb{Z}_4$ non lo è; infatti $\overline{2} \cdot \overline{2} = \overline{0}$ e quindi $\overline{2}$ non è invertibile.

## 1.10 Algoritmo di Euclide e identità di Bézout su $\mathbb{Z}$

Vogliamo calcolare il massimo comun divisore tra 1876 e 365.
Usiamo l'algoritmo di Euclide:

$$\begin{aligned} 1876 &= 5 \cdot 365 + 51 \\ 365 &= 7 \cdot 51 + 8 \\ 51 &= 6 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Quindi $MCD\{1876, 365\} = 1$.
Adesso vogliamo trovare due numeri $x, y \in \mathbb{Z}$ tali che $1876x + 365y = 1$.
Un'identità del tipo $ax + by = MCD\{a, b\}$ si chiama **identità di Bézout**.
Dall'algoritmo di Euclide abbiamo:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 8 - 3 \cdot 2 \\ 3 &= 51 - 6 \cdot 8 \\ 8 &= 365 - 7 \cdot 51 \\ 51 &= 1876 - 5 \cdot 365 \end{aligned}$$

Quindi

$$\begin{gathered} 1 = 3 - 2 = \\ = 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8 \\ = 3 \cdot (51 - 8 \cdot 6) - 8 = 3 \cdot 51 - 8 \cdot 19 \\ = 3 \cdot 51 - 19(365 - 51 \cdot 7) \\ = 136 \cdot 51 - 19 \cdot 365 \\ = 136 \cdot (1876 - 365 \cdot 5) - 19 \cdot 365 \\ = 136 \cdot 1876 - 699 \cdot 365 \end{gathered}$$

Quindi $x = -699$ e $y = 136$.
In generale possiamo enunciare il seguente teorema:

***Teorema:*** *siano $a, b \in \mathbb{N} \setminus 0$, se $a \mid b$, allora $a = MCD\{a, b\}$.*
*se $a \nmid b$ e $r$ è l'ultimo resto non nullo dell'algoritmo di Euclide, allora $r = MCD\{a, b\}$.*
*inoltre esistono $x, y \in \mathbb{Z}$ tali che $ax + by = MCD\{a, b\}$.*

***Dimostrazione:*** *Sia $I = \{ax + by : x, y \in \mathbb{Z}\}$ l'insieme dei multipli di $a$ e $b$.*
*Poiché $I$ è un ideale di $\mathbb{Z}$, allora $I = n\mathbb{Z}$ per qualche $n \in \mathbb{N}$.*
*Poiché $a \in I$, allora $n \mid a$.*
*Poiché $b \in I$, allora $n \mid b$.*
*Quindi $n = MCD\{a, b\}$.*
*Inoltre, poiché $r \in I$, allora $r = ax + by$ per qualche $x, y \in \mathbb{Z}$.*
*Quindi $r = MCD\{a, b\}$.*

*fatta da copilot, controllare a pag 40 di "a concrete introduction to higher algebra" di Lindsay Childs*

## 1.11 Equazioni diofantee lineari

sono equazioni del tipo $ax + by = c$, con $a, b, c \in \mathbb{Z}$.

**Proposizione:** *siano $a, b, c \in \mathbb{Z}$.*
*allora esistono $x, y \in \mathbb{Z}$ tali che $ax + by = c$ se e solo se $MCD\{a, b\} \mid c$.*

***Dimostrazione:*** *Se $ax + by = c$, allora $MCD\{a, b\} \mid c$.*
*Viceversa, se $d := MCD\{a, b\} \mid c$, allora abbiamo un'identità di Bézout $ax + by = d$ $\forall x, y \in \mathbb{Z}$.*
*se $d \mid c$ cioè se $c = d \cdot k$ per qualche $k \in \mathbb{Z}$, $a(kx) + b(ky) = kd = c$*

**Esempio:** l'equazione diofantea:
$365x - 1876y = 24$ ha soluzione perchè $MCD\{365, 1876\} = 1$ e $1 \mid 24$.
Avevamo l'identità di Bézout $365(-699) - 1876(-136) = 1$, moltiplicando per 24 otteniamo
$365(-699 \cdot 24) - 1876(-136 \cdot 24) = 24$.
ossia una soluzione è $x = -699 \cdot 24$ e $y = -136 \cdot 24$.

**Esempio:** in $\mathbb{Z}_{1876}$ calcolare, se esiste, l'inverso moltiplicativo di $\overline{365}$.
abbiamo che $\overline{365} \cdot \overline{a} = \overline{1}$ in $\mathbb{Z}_{1876}$
se e solo se esistono $a, b \in \mathbb{Z}$ t.c. $365 \cdot a = 1 + b \cdot 1876 \leftrightarrow 365 \cdot a - 1876 \cdot b = 1$.
una soluzione è $a = -699$ e $b = 136$, ossia $\overline{365}^{-1} = \overline{-699} = \overline{1177}$.

## 1.12 Morfismi di anelli

***Definizione:*** *se $p \in \mathbb{N}$ è un numero primo, scriviamo $\mathbb{F}_p := \mathbb{Z}_p$ ;*
*il campo $\mathbb{F}_p$ ha $p$ elementi.*

***Definizione:*** *Siano $A, B$ due anelli. Un'applicazione $f : A \to B$ è un* ***morfismo di anelli*** *se:*

- *$f : (A, +) \to (B, +)$ è un morfismo di gruppi.*
- *$f : (A, \cdot) \to (B, \cdot)$ è un morfismo di monoidi.*

***Definizione:*** *il nucleo di un morfismo di anelli*
*$f : A \to B$ è l'insieme $Ker(f) := \{a \in A : f(a) = 0\}$.*

***Osservazione:*** *$Ker(f)$ è un ideale di $A$, $A$ anello commutativo.*

**Esempio:** sia $I \subseteq A$ un ideale di un anello commutativo $A$.
allora la proiezione canonica $\pi : A \to A/I$ che mappa $a \to [a]$
è un morfismo di anelli il cui nucleo è $I$.

**Esempio:** si consideri l'anello dei numeri complessi $\mathbb{C}$.
allora il coniugio $\overline{z} = \overline{a + bi} = a - bi$ è un morfismo di anelli da $\mathbb{C}$ in $\mathbb{C}$:
$\overline{1} = 1, \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

***Teorema*** (di isomorfismo per anelli commutativi)***:*** *Sia $f : A \to B$*
*un morfismo di anelli commutativi. Allora esiste un morfismo iniettivo di anelli*
*$\Psi : A/Ker(f) \to B$ tale che il seguente diagramma è commutativo:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/Ker(f) \arrow[ur, "\Psi"'] & \end{tikzcd}$$

*in particolare, se $f$ è suriettivo, allora $\Psi$ è un isomorfismo di anelli.*

**Notazione:** $\overline{x} \in \mathbb{Z}_n$. La classe di equivalenza $\overline{x}$ la scriveremo anche $x \mod n$.

***Teorema*** (Teorema cinese dei resti)***:*** *siano* $n_1, n_2, ..., n_k \in \mathbb{N} \setminus \{0, 1\}$ *tali che* $MCD\{n_i, n_j\} = 1$ *per ogni* $1 \leq i, j \leq k, i \neq j$.
*sia* $n := n_1 \cdot n_2 \cdot ... \cdot n_k$.
*allora la funzione* $\Psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$ *che mappa* $xmodn \to (xmodn_1, xmodn_2, ..., xmodn_k)$ *è un isomorfismo di anelli.*

***Dimostrazione:*** *vediamo prima di tutto che* $\Psi$ *è un morfismo di anelli dove* $f : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$. *è definita da* $f(x) = (xmodn_1, xmodn_2, ..., xmodn_k) \forall x \in \mathbb{Z}$.

- $f(a + b) = ((a + b)modn_1, ..., (a + b)modn_k)$
  $= (amodn_1 + bmodn_1, ..., amodn_k + bmodn_k)$
  $= (amodn_1, ..., amodn_k) + (bmodn_1, ..., bmodn_k)$
  $= f(a) + f(b), \forall a, b \in \mathbb{Z}$

- $f(1) = (1modn_1, ..., 1modn_k)$ *e* $(1modn_1, ..., 1modn_k)$ *è l'unità del prodotto diretto di anelli* $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$

- $f(a \cdot b) = ((a \cdot b)modn_1, ..., (a \cdot b)modn_k)$
  $= (amodn_1 \cdot bmodn_1, ..., amodn_k \cdot bmodn_k)$
  $= (amodn_1, ..., amodn_k) \cdot (bmodn_1, ..., bmodn_k)$
  $= f(a) \cdot f(b), \forall a, b \in \mathbb{Z}$

*ora mostriamo che* $f$ *è suriettivo:*
*sia* $(a_1modn_1, ..., a_kmodn_k) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$
*osserviamo che* $MCD\{n_i, n_1n_2...n_{i-1}n_{i+1}...n_k\} = 1, \forall 1 \leq i \leq k$.
*quindi abbiamo le identità di Bézout:* $c_in_i + b_i\frac{n}{n_i} = 1$ *ossia*
$u_i + v_i = 1$ *dove* $u_i = c_in_i \in < n_i >$ *e* $v_i = b_i\frac{n}{n_i} \in < \frac{n}{n_i} >$.
*diefiniamo* $x := a_1v_1 + ... + a_kv_k$ *e abbiamo che* $f(x) = (a_1modn_1, ..., a_kmodn_k)$.
*infatti* $v_imodn_j = \begin{cases} 0 & se\ i \neq j \\ 1 & se\ i = j \end{cases}$
*dal teorema di isomorfismo abbiamo che* $\mathbb{Z}/_{Ker(f)} \simeq \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$ *come anelli.*
*ma abbiamo che* $Ker(f) =< n_1 > \cap < n_2 > \cap ... \cap < n_k >$
$=< mcm\{n_1, ..., n_k\} >=< n_1n_2...n_k >$ *dato che* $n_i$ *e* $n_j$ *sono coprimi* $\forall i \neq j$.
*quindi* $\mathbb{Z}/_{Ker(f)} = \mathbb{Z}/_{<n>} = \mathbb{Z}_n$ *e l'isomorfismo* $\Psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$
*è quello dell'enunciato del teorema.*

**Esempio:** siano $n_1 = 3, n_2 = 7 e n_3 = 10$. Allora $n := n_1 n_2 n_3 = 210$
e abbiamo l'isomorfismo di anelli $\mathbb{Z}_{210} \simeq \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{10}$.
sia $(2mod3, 5mod7, 4mod10) \in \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{10}$, questa terna corrisponde ad un elemento $xmod210 \in \mathbb{Z}_{210}$ che soddisfa il sistema

$$\begin{cases} x \mod 3 = 2 \mod 3 \\ x \mod 7 = 5 \mod 7 \\ x \mod 10 = 4 \mod 10 \end{cases}$$

la dimostrazione del teorema cinese dei resti ci dice come trovare x.
$x = 2v_1 + 5v_2 + 4v_3$ dove se $3a + 70b = 1, 7a + 30b = 1$ e $10a + 21b = 1$ sono identità di Bézout, allora $v_1 = 70b, v_2 = 30b = 30, v_3 = 21b$

$$\begin{gathered} 3a + 70b = 1 \to a = -23, b = 1 \to v_1 = 70 \\ 7a + 30b = 1 \to 30 = 4 \cdot 7 + 2, 7 = 3 \cdot 2 + 1 \\ \to 1 = 7 - 3 \cdot 2 = 7 - 3(30 - 4 \cdot 7) = \\ 13 \cdot 7 - 3 \cdot 30 = 91 - 90 = 1 \to a = 13, b = -3 \to v_2 = -3 \cdot 30 \\ 10a + 21b = 1 \to a = -2, b = 1 \to v_3 = 21 \end{gathered}$$

quindi $x = 2 \cdot 70 - 5 \cdot 3 \cdot 30 + 4 \cdot 21 = 194 \mod 210$

**Corollario:** Sia $U(\mathbb{Z}_n)$ il gruppo degli elementi invertibili dell'anello $\mathbb{Z}_n$.
sia $n := n_1 ... n_k$ dove $MCD\{n_i, n_j\} = 1 \forall 1 \leq i, j \leq k, i \neq j$.
e $n_i \in \mathbb{N} \setminus \{0, 1\} \forall 1 \leq i \leq k$.
allora come i gruppi $U(\mathbb{Z}_n) \simeq U(\mathbb{Z}_{n_1}) \times ... \times U(\mathbb{Z}_{n_k})$

***Dimostrazione:*** *l'isomorfismo $\Psi$ del teo. cinese dei restti, ristretto a $U(\mathbb{Z}_n)$ dà un isomorfismo di gruppi*

Poiché un elemento $\overline{x} \in \mathbb{Z}_n$ è invertibile s.s.e. esiste un'identità di Bézout $ax + bn = 1$ abbiamo che $\overline{x}$ è invertibile s.s.e. $MCD\{x, n\} = 1$.
Quindi $|U(\mathbb{Z}_n)| = \varphi(n)$, con $\varphi$ funzione di Eulero.

dal precedente Corollario e da questo segue un altro Corollario:
**Corollario:** Sia $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ la funzione $\varphi$ di Eulero.
siano $x, y \in \mathbb{N} \setminus \{0\}$ tali che $MCD\{x, y\} = 1$, allora $\varphi(xy) = \varphi(x) \cdot \varphi(y)$.

***Dimostrazione:*** *dal Corollario precedente abbiamo che $U(\mathbb{Z}_{xy}) \simeq U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)$ come i gruppi, quindi:*

$$\varphi(xy) = |U(\mathbb{Z}_{xy})| = |U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)| = |U(\mathbb{Z}_x)| \cdot |U(\mathbb{Z}_y)| = \varphi(x) \cdot \varphi(y)$$

Come conseguenza del corollario precedente otteniamo una formula per calcolare la funzione $\varphi$ di Eulero.
Se $p$ è un numero primo, allora ci sono $p^k$ numeri $1 \leq n \leq p^k$.
Di questi numeri $p, 2p, ..., p^{k-1}p$ hanno fattori comuni con $p^k$ e quindi

$$\varphi(p^k) = p^k - p^{k-1}.$$

se $n = p^{k_1}...p^{k_s}$ per il corollario precedente ($n > 1$):
$\varphi(n) = \varphi(p_1^{k_1}...\varphi(p_s^{k_s}) = (p_1^{k_1} - p_1^{k_1-1})...(p_s^{k_s} - p_s^{k_s-1}) = p_1^{k_1}...p_s^{k_s} \prod_{p|n,pprimo}(1 - \frac{1}{p}) =$
$= n \prod_{p|n,pprimo}(1 - \frac{1}{p})$.

***Teorema*** (di Eulero)***:*** *Sia $n \in \mathbb{N} \setminus \{0,\}$ ed $a \in \mathbb{N} \setminus \{0\}$ tale che $MCD\{a, n\} = 1$.*
*allora $\overline{a^{\varphi(n)}} = \overline{1} \in \mathbb{Z}_n$. (diciamo che $a^{\varphi(n)} \equiv 1 \mod n$)*

***Dimostrazione:*** *sappiamo che la cardinalità del gruppo degli elementi invertibili di $\mathbb{Z}_n$ è $\varphi(n)$.*
*Sia $< \overline{a} > \subseteq U(\mathbb{Z}_n)$ il sottogruppo generato da $\overline{a} in U(\mathbb{Z}_n)$. allora $| < \overline{a} > |$ divide $\varphi(n)$, ossia $\varphi(n) = k| < \overline{a} > |$, per qualche $k \in \mathbb{N}$. Sia $c := | < \overline{a} > |$;*
*abbiamo che $= \overline{1} = \overline{a}^c = (\overline{a^c})^k = \overline{a^{ck}} = \overline{a^{\varphi(n)}}$.*

**Corollario:**(piccolo teorema di Fermat) Sia $p$ un numero primo e $a \in \mathbb{N}$.
allora in $\mathbb{Z}_p$ abbiamo che $\overline{a} = \overline{a^p}(a^p \equiv a \mod p)$.

***Dimostrazione:*** *se $p$ è primo si ha che $\varphi(p) = p - 1$. allora dal Teo. di Eulero segue che, se $a \neq 0, p \nmid a$, $a^{varphi(p) \equiv 1 \mod p} \implies a^{p-1} \equiv 1 \mod p \implies a^p \equiv a \mod p$.*
*se $a = 0 o p|a$ l' uguaglianza si riduce a $\overline{0} = \overline{0}$.*

## 1.13 Caratteristica di un anello

sia $A$ un anello. il sottogruppo $< 1_A > \subseteq (A, +)$è un gruppo ciclico.
quindi esiste un $n \in \mathbb{N}$ tale che $< 1_A > \simeq \mathbb{Z}_n$. $n$ è detto la caratteristica dell'anello $A$.

**Esempio:** la caratteristica di $\mathbb{Z}$ è 0, infatti $< 1 >= \mathbb{Z} \simeq \mathbb{Z}_0$.
la caratteristica degli anelli $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ è sempre 0 poiché $< 1 >= \mathbb{Z} \simeq \mathbb{Z}_0$ in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

**Esempio:** sia $n \in \mathbb{N}$ allora la caratteristica dell'anello $\mathbb{Z}_n$ è $n$.
infatti $< \overline{1} >= \mathbb{Z}_n$, rispetto all'operazione $+$

indichiamo con $CHAR(A)$ la caratteristica di un anello $A$.

***Definizione:*** *sia $A$ un anello e sia $< 1_A >$ il sottogruppo di $(A,+)$ generato da $1_a$. l'intersezione di tutti i sottoanelli di $A$ contenenti $< 1_a >$*
*si chiama* ***sottoanello fondamentale di A****.*

**Esempio:** il sottoanello fondamentale di $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ è $\mathbb{Z}$

***Definizione:*** *sia $K$ un campo*
*l'intersezione di tutti i sottocampi di $K$ contenenti il gruppo $< 1_k > \subseteq (K, +)$ si chiama* ***sottocampo fondamentale di K****.*

**Esempio:** il sottocampo fondamentale di $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ è $\mathbb{Q}$.
se $p \in \mathbb{N}$ è primo, il sottocampo fondamentale di $\mathbb{F}_p$ è $\mathbb{F}_p$ perché $< \overline{1} >= \mathbb{F}_p$.

## 1.14 Anello dei polinomi in una indeterminata a coefficienti in un campo

Sia $K$ un campo. una funzione $f : \mathbb{N} \to K$ si chiama **successione a valori in** $K$.
ad una successione a valori in $K$ corrisponde una serie formale nella variabile $x$ su $K$:

$$\sum_{n=0}^{\infty} f(n)x^n$$

se l'insieme $\{m\ in\mathbb{N} : f(n) \neq 0\}$ è finito diciamo che la serie formale è un polinomio in $x$ di grado $deg(P) := MAX\{n \in \mathbb{N} : f(n) \neq 0\}$.
il grado del poliniomio 0 non è definito.
l'insieme dei polinomi in $x$ a coefficienti in $K$ si indica con $K[x]$ ed è un anello commutativo con le operazioni:

- somma: $(\sum_{n=0}^{\infty} a_n X^n) + (\sum_{n=0}^{\infty} b_n X^n) = \sum_{n=0}^{\infty} (a_n + b_n)X^n$
- prodotto: $(\sum_{n=0}^{\infty} a_n X^n) \cdot (\sum_{n=0}^{\infty} b_n X^n) = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k})X^n$

l'unità di $K[x]$ è il polinomio $1_k$.

**Esempio:** in $\mathbb{F}_2[x]$ siano $P := 1 + X^2 + X^3$ e $Q := X + X^2$.
allora $P + Q = 1 + X + X^2 + X^3$ e $P \cdot Q = X + X^2 + X^3 + X^5$

**Proposizione:** *siano $P, Q \in K[x]$ polinomi non nulli. allora il grado del prodotto $P \cdot Q$ è $deg(P) + deg(Q)$.*
*in particolare $K[x]$ è un dominio di integrità.*

***Definizione:*** *un polinomio si dice **monico** se il coefficiente del termine di grado massimo è 1.*

***Definizione:*** *sia $K$ un campo. un polinomio $P \in K[x]$ si dice **irriducibile** se i suoi unici divisori sono del tipo $a, aP$ con $a \in K \setminus \{0\}$.*
*altrimenti si dice **riducibile**.*

**Esempio:** in $\mathbb{F}_2[X]$ il polinomio $X^2 + 1$ è irriducibile, infatti:
$X^2 + 1 = (X + 1)^2$, quindi $X + 1$ divide $X^2 + 1$ e $X + 1 \notin K \setminus \{0\}$.

**Esempio:** in $K[X]$ ogni polinomio di grado 1 è irriducibile, infatti:
se $deg(P) = 1$ allora $P = aX + b$ con $a, b \in K, a \neq 0$.
i suoi divisori sono $c$ e $c^{-1}(aX + b), c \in K \setminus \{0\}$.

***Definizione:*** *sia $\alpha \in K$. l'elemento $\alpha$ è detto **radice** del polinomio $P = \sum_{n=0}^{\infty} a_n X^n \in K[X]$ se $P(\alpha) = \sum_{n=0}^{\infty} a_n \alpha^n = 0$.*

anche nell'anello $K[X]$ come in $\mathbb{Z}$ abiamo un algoritmo di divisione Euclidea.
se $f(X), g(X) \in K[X]$ sono polinomi non nulli allora esistono unici polinomi $q(X), r(X) \in K[X]$ tali che:
$f(X) = q(X) \cdot g(X) + r(X)$ e $r(X) = 0$ oppure $deg(r) < deg(g)$.
$q(X)$ si chiama **quoziente** e $r(X)$ si chiama **resto** della divisione.
ne segue il seguente teorema, dimostrato come in $\mathbb{Z}$:

***Teorema:*** *l'anello $K[X]$ è a ideali principali.*
*se $I =< p(X) >$ allora esiste un unico generatore monico di $I$.*

***Definizione:*** *definiamo il* ***massimo comune divisore*** *di due polinomi $f(X), g(X) \in K[X]$ come l'unico massimo comune divisore monico.*

Come in $\mathbb{Z}$ possiamo trovarlo con l'algoritmo delle divisioni successive
che dà anche un identità di Bézout.

**Esempio:** $f(X) = X^4 - X^3 - 4X^2 + 4X + 1$ e $g(X) = X^2 - 1$ in $\mathbb{Q}[X]$, allora:

$$f(X) = g(X)(X^2 - 3) + (X - 2)$$
$$g(X) = (X - 2)(X + 1) + 1 \implies MCD(f, g) = 1$$

inoltre

$$1 = g(X) - (X - 2)(X + 1) + 1 = g(X) - [f(X) - g(X)(X^2 - 3)](X + 1) =$$
$$= -(X - 1)f(X) + (X^3 + X^2 - 3X - 2)g(X).$$

**proprietà:** sia K un campo e $P(X) \in K[X]$ un poliniomio irriducibile.
allora l'anello quoziente ${}^{K[X]}/_{< P(X) >}$ è un campo.

***Dimostrazione:*** *sia $[f]$ in${}^{K[X]}/_{< P(X) >}$ tale che $[p] \neq [0]$ ossia $p(X)$ non divide $f(X)$.*
*Dunque $MCD\{f(X), p(X)\} = 1$ perchè $p(X)$ è irriducibile.*
*quindi abbiamo un'identità di Bézout $a(X)f(X) + b(X)p(X) = 1$.*
*ossia $[a(X)] = [f(X)]^{-1}$ in ${}^{K[X]}/_{< P(X) >}$.*

**Esempio:** in $\mathbb{F}_2[X]$ il polinomio $P(X) = 1 + X + X^2$ è irriducibile.
infatti non ha radici in $\mathbb{F}_2$.
quindi l'anello ${}^{\mathbb{F}_2[X]}/_{< 1 + X + X^2 >}$ è un campo, che chiamiamo $\mathbb{F}_4$.
un elemento di $\mathbb{F}_4$ è della forma $a_0 + a_1X$ con $a_0, a_1 \in \mathbb{F}_2$.
la tavola moltiplicativa è la seguente:

| $\cdot$ | 0 | 1 | X | 1 + X |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | X | 1 + X |
| X | 0 | X | 1 + X | 1 |
| 1 + X | 0 | 1 + X | 1 | X |

l'inverso di $X$ è $1 + X$.

**Esempio:** in $\mathbb{F}_3[X]$ il polinomio $P(X) = 1 + X^2$ è irriducibile.
indichiamo con $\mathbb{F}_9$ il campo$^{\mathbb{F}_3[X]}/_{<1+X^2>}$.
un elemento di $\mathbb{F}_9$ è della forma $a_0 + a_1X$ con $a_0, a_1 \in \mathbb{F}_3$ quindi sono 9.
la tavola moltiplicativa è la seguente:

| · | 0 | 1 | 2 | X | 1 + X | 2 + X | 2X | 1 + 2X | 2 + 2X |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | X | 1 + X | 2 + X | 2X | 1 + 2X | 2 + 2X |
| 2 | 0 | 2 | 1 | 2X | 2 + 2X | 1 + 2X | X | 2 + X | 1 + X |
| X | 0 | X | 2X | 2 | 2 + X | 2 + 2X | 1 | 1 + X | 1 + 2X |
| 1 + X | 0 | 1 + X | 2 + 2X | 2 + X | 2X | 1 | 1 + 2X | 2 | X |
| 2 + X | 0 | 2 + X | 1 + 2X | 2 + 2X | 1 | X | 1 + X | 2X | 2 |
| 2X | 0 | 2X | X | 1 | 1 + 2X | 1 + X | 2 | 2 + 2X | 2 + X |
| 1 + 2X | 0 | 1 + 2X | 2 + X | 1 + X | 2 | 2X | 2 + 2X | X | 1 |
| 2 + 2X | 0 | 2 + 2X | 1 + X | 1 + 2X | X | 2 | 2 + X | 1 | 2X |

l'inverso di $X$ è 2.

***Teorema*** (di Ruffini)**:** *sia $f(X) \in K[X]$ un polinomio non nullo.*
*se $\alpha \in K$, il resto della divisione di $f(X)$ per $X - \alpha$ è $f(\alpha)$,*
*in particolare $\alpha$ è una radice di $f(X)$ s.s.e. $X - \alpha$ divide $f(X)$ in $K[X]$.*

***Dimostrazione:*** $f(X) = (X - \alpha)q(X) + r(X)$ *con* $r(X) = 0$ *oppure* $deg(r(X)) < 1$.
*quindi* $r(X)$ *è un polinomio costante,* $r(X) = x \in K$.
*calcolando in* $\alpha$ *otteniamo* $f(\alpha) = c$.

**Esempio:** il polinomio $X^2 + 1 \in \mathbb{R}[X]$ non ha radici in $\mathbb{R}$
quindi è irriducibile e $^{\mathbb{R}[X]}/_{<X^2+1>}$ è un campo isomorfo a $\mathbb{C}$,
dove l'isomorfismo è dato dall'assegnazione $1 \to 1$ e $x \to i$

enunciamo il seguente importante risultato, senza fornire la dimostrazione.
(vedi proposizione 4.3.5 di "Teoria delle equazioni e teoria di Galois" - S.Gabelli).

**Proposizione:** *se $K$ è un campo, ogni sottogruppo finito del gruppo moltiplicativo $K \setminus \{0\}$ è ciclico. in particolare, se $K$ è un campo finito, $K \setminus \{0\}$ è un gruppo ciclico.*

**Esempio:**

- in $\mathbb{F}_4 = {}^{\mathbb{F}_2}/_{<1+X+X^2>}$ si ha che $\{X, X^2, X^3\} = \{X, 1+X, 1\} = \mathbb{F}_4 \setminus \{0\}$ quindi $X$ è un generatore del gruppo moltiplicativo $\mathbb{F}_4 \setminus \{0\}$, l'altro è $1+X$

- in $\mathbb{F}_9 = {}^{\mathbb{F}_3}/_{<1+X^2>}$ abbiamo:
  $< X >= \{X, X^2, X^3, X^4\} = \{X, 2, 2X, 1\}$
  $< 1+X >= \{1+X, (1+X)^2, (1+X)^3, (1+X)^4, (1+X)^5, (1+X)^6, (1+X)^7, (1+X)^8\} =$
  $= \{1+X, 2X, 1+2X, 2, 2+2X, X, 2+X, 1\}$
  $= \mathbb{F}_9 \setminus \{0\}$ quindi $1+X$ genera il gruppo moltiplicativo.

Sia $p \in \mathbb{N}$ un numero prima e sia $n \in \mathbb{N} \setminus \{0\}$.
sia $Q(X), \mathbb{F}_p[X]$ un qualsiasi polinomio irriducibile di grado n.
definiamo il campo

$$\mathbb{F}_{p^n} = {}^{\mathbb{F}_p[X]}/_{<Q(X)>}$$

vogliamo ora mostrare che se $Q(X), Q'(X) e \mathbb{F}_p[X]$ sono polinomi irriducibili di grado n,
allora

$${}^{\mathbb{F}_p[X]}/_{<Q(X)>} \simeq {}^{\mathbb{F}_p[X]}/_{<Q'(X)>}, \text{ isomorfismo tra campi}$$

quindi la definizione di $\mathbb{F}_p$ è ben posta, a meno di isomorfismi.

***Definizione:*** *siano $F \subseteq K$ due campi (ampliamento di campi).
un elemento $\alpha \in K$ si dice algebrico su $F$ se è radice di qualche polinomio non nullo su $f(X) \in F(X)$, altrimenti si dice trascendente su $F$.*

dato un ampliamento di campi $F \subseteq K$ e $\alpha \in K$, si consideri il morfismo di anelli

$$\begin{gathered} v_\alpha : F[X] \to K \\ f(X) \to f(\alpha). \end{gathered}$$

$Ker(v_\alpha)$ è l'ideale di $F[X]$ costituito dai polinomi che si annullano in $\alpha$.
quindi $\alpha$ è algebrico su F s.s.e. $Ker(v_\alpha)$ è un ideale non nullo di $F[X]$.
poiche $F[X]$ è ad ideali principali, $ker(v_\alpha) =< m(X) >$
dove $m(X)$ è l'unico polinomio monico di grado minimo in $Ker(v_\alpha)$.

***Definizione:*** *se $\alpha \in K$ è algebrico su $F$, il polinomio $m(X)$ definito sopra si chiama* ***polinomio minimmo di $\alpha$ su F****, se $deg(m(X)) = n$, $\alpha$ si dice algebrico di grado $n$*

**Nota:** sia $\alpha \in K$ e $P(X) \in F[X] \setminus \{0\})$ tale che $p(\alpha) = 0$,
allora $p(X)$ è il polinomio minimo di $\alpha$ su F s.s.e. $p(X)$ è monico e irriducibile.

**Esempio:** si consideri l'ampliamento $\mathbb{R} \subseteq \mathbb{C}$. allora $1+X^2 \in \mathbb{R}[X]$
è il polinomio minimo di $i \in \mathbb{C}$ su $\mathbb{R}$.

**Proprietà:** sia $F \in K$ un ampliamento di campi e $\alpha \in K$.
si consideri il morfismo di anelli $v_\alpha : F[X] \to K$.
allora $Im(v_\alpha)$ è il più piccolo sottoanello di K contenente sia F che $\alpha$

***Dimostrazione:*** *si osservi che l'immagine di un morfismo di anelli è un sottoanello.
di conseguenza $Im(v_\alpha)$ è un sottoanello di K.
sia $c \in F$ e si consideri il polinomio costante $c \in F[X]$. allora $v_\alpha(c) = c$.
quindi $F \subseteq Im(v_\alpha)$ e $v_\alpha(X) = \alpha \implies \alpha \in Im(v_\alpha)$
d'altra parte per chiusura aditiva e moltiplicativa,
ogni sottoanello di K contenete sia F che $\alpha$ contiene anche $Im(v_\alpha)$.*

**Proposizione:** *sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$.
il più piccolo sottocampo di K contenente sia F che $\alpha$ si chiama
**ampliamento di F in K generato da** $\alpha$ e si indica con **F(**$\alpha$**)** tale ampliamento si dice **semplice** (poichè generato da un solo elemento)*

da questa proposizione segue questo Corollario:

**Corollario:** sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$.
allora $F(\alpha) = \{f(\alpha)g(\alpha)^{-1} : f(X), g(X) \in F[X], g(\alpha) \neq 0\}$.

***Dimostrazione:*** *per la proposizione precedente
il più piccolo sottoanello di K contenente sia F che $\alpha$ è $Im(v_\alpha = \{f(\alpha) : f(X) \in F[X]\})$.
prendendo gli inversi in K si ottiene la tesi.*

se $\alpha \in K$ è algebrico su F si ha che $Im(v_\alpha \simeq {}^{F[X]}/_{< m(X) >})$,
dove $m(X)$ è il polinomio minimo di $\alpha$. quindi $Im(v_\alpha)$ è un campo e $F(\alpha) = Im(v_\alpha)$.
se n è il grado di $\alpha$ si ha quindi:

$$F(\alpha) = \{c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1} : c_i \in F\}$$

**Esempio:** si consideri l'ampliamento $\mathbb{Q} \subseteq \mathbb{R}$. l'elemento $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ è akgebrico su $\mathbb{Q}$ con polinomio minimo $X^2 - 2$. quindi $\sqrt{2}$ ha grado 2 su $\mathbb{Q}$ e

$$\mathbb{Q}(\sqrt{2}) = \{c_0 + c_1\sqrt{2} : c_0, c_1 \in \mathbb{Q}\}).$$

adesso mostriamo che il campo $\mathbb{F}_{p^n}$ è un ampliamento semplice di $\mathbb{F}_p$

**Proposizione:** *sia $\alpha \in \mathbb{F}_{p^n}$ un generatore del campo moltiplicativo $\mathbb{F}_{p^n} \setminus \{0\}$.
allora $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$.*

***Dimostrazione:*** *$\mathbb{F}_p(\alpha)$ è il più piccolo sottocampo di $\mathbb{F}_{p^n}$ contenente sia $\mathbb{F}_p$ che $\alpha$
quindi $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$. Poiché $\alpha$ genera il gruppo moltiploicativo $\mathbb{F}_{p^n} \setminus \{0\}$ anche $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$*

Ora, se $P(X), Q(X) \in \mathbb{F}_p[X]$ sono due polinomi irriducibili di grado n, vogliamo costruire un isomorfismo

$$f : {}^{\mathbb{F}_p[X]}\!/_{< P(X) >} \rightarrow {}^{\mathbb{F}_p[X]}\!/_{< Q(X) >}$$

ci serve il seguente risultato:

**Proposizione:** *siano $F \subseteq K$ e $F \subseteq K'$ due ampliamenti di campi.*
*se $\alpha \in K$ è algebrico di grado n su F, con polinomio minimo $m(x)$,*
*esiste un morfismo di campi $\varphi : F(\alpha) \rightarrow K'$ che fissa F in K'.*
*in questo caso i morfismi $\varphi$ sono tanti quante le radici distinte $\beta_1, ..., \beta_s$ di $m(X)$ in K'.*
*sono tutti e soli quelli definiti da:*

$$c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1} \rightarrow c_0 + c_1\beta_i + ... + c_{n-1}\beta_i^{n-1}$$

***Dimostrazione:*** *se $\alpha$ è algebrico di grado n su F con polinomio minimo $m(X)$*
*e $\varphi : F(\alpha) \rightarrow K'$ è isomorfismo, allora $0 = \varphi(0) = \varphi(m(\alpha)) = m(\varphi(\alpha))$*
*quindi $\varphi(\alpha)$ deve essere radice di $m(X)$ in K'.*
*viceversa, sia $\beta$ una radice di $m(X)$ in K' e consideriamo il morfismo di anelli*

$$v_\beta : F[X] \rightarrow K'$$
$$f(X) \rightarrow f(\beta)$$

*poiché $m(X) \in Ker(v_\beta)$, dal Teorema di isomorfismo per anelli*
*abbiamo che il seguente diagramma è commutativo:*

$$\begin{tikzcd} F[X] \arrow[r, "v_\beta"] \arrow[d, "\pi"] & K' \\ F(\alpha) \simeq {}^{F[X]}\!/_{< m(X) >} \arrow[ur, "\varphi"] & \end{tikzcd}$$

*infatti $Ker(v_\beta) =< m(X) >$, essedo $m(X)$ irriducibile.*
*quindi abbiamo trovato un morfismo iniettivo $\varphi : F(\alpha) \rightarrow K'$ che soddisfa le proprietà dell'enunciato.*

sia F un campo e $f(X) \in F[X]$ un polinomio di grado $n \geq 1$.
un campo K, ampliamento di F, si dice **campo di spezzamento di f(X) su F** se:

- $f(X)$ fattorizza in polinomi di grado 1 su $K[X]$
- non ci sono campi intermedi $F \subseteq L \subsetneq K$ con la stessa proprietà.

**Esempio:** $\mathbb{Q}(\sqrt{2})$ è un campo di spezzamenro di $X^2 - 2 \in \mathbb{Q}[X]$.
$\mathbb{C}$ è un campo di spezzamenro di $X^2 + 1 \in \mathbb{R}[X]$.

Ora vogliamo mostrare che un campo che ha cardinalità $p^n$
è un campo di spezzamento del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$.
infatti se K è un campo e $|K| = p^n$, allora il suo gruppo moltiplicativo $K \setminus \{0\}$ ha cardinalità $p^n - 1$
e quindi oer ogni $\alpha \in K \setminus \{0\}$ si ha $\alpha^{p^n-1} = 1$.
quindi ogni elemento di K è radice del polinomio $X^{p^n} - X$.
per il teorema di Ruffini, K è un campo di spezzamento di $X^{p^n} - X$.
Adesso mostriamo che ogni poliniomio di grado n irriducibile in $\mathbb{F}_p[X]$
divide $X^{p^n} - X \ \in \mathbb{F}_p[X]$.

**Proposizione:** *tutti e soli i polinomi irriducibili su $\mathbb{F}_p$ di grado n dividono $X^{p^n} - X \in \mathbb{F}_p[X]$.*

***Dimostrazione:*** *sia $P(X) \in \mathbb{F}_p[X]$ irriducibile di grado n e sia $K := {}^{\mathbb{F}_p[Y]}/_{<P(Y)>}$.
allora K ha $p^n$ elementi che sono le radici di $X^{p^n} - X \in K[X]$.
poichè $Y \in K$ è una radice $P(X) \in K[X]$, $P(X) e X^{p^n} - X$ hanno una radice in comune in K,
allora per il teorema di Ruffini hanno un fattore comune $X - Y in K[X]$.
quindi, poiché $\mathbb{F}_p \subseteq K$ e $MCD$ in $\mathbb{F}_p = MCD$ in $K[X]$
$\implies P(X), X^{p^n} - X$ hanno $MCD \neq 1$ in $\mathbb{F}_p[X]$.
poiché $P(X)$ è irriducibile in $\mathbb{F}_p[X]$, $P(X)$ divide $X^{p^n} - X$.*

adesso vogliamo costruire un isomorfismo di campi

$$f : {}^{\mathbb{F}_p[X]}/_{<P(X)>} \longrightarrow {}^{\mathbb{F}_p[X]}/_{<Q(X)>}$$

dove $P(X), Q(X) \in \mathbb{F}_p[X]$ sono monici irriducibili di grado n.
basta costruire un isomorfismo di anelli.
Infatti un morfismo di anelli che sono campi è iniettivo. Inoltre:

$$\left|{}^{\mathbb{F}_p[X]}/_{<P(X)>}\right| = \left|{}^{\mathbb{F}_p[X]}/_{<Q(X)>}\right| = p^n$$

quindi tale morfismo è biunivoco, ossia è isomorfismo.

Si ha che, se $y \in {}^{\mathbb{F}_p[Y]}/_{<P(Y)>}$ allora $P(X) \in \mathbb{F}_p[X]$ è il polinomio minimo di $y$ su $\mathbb{F}_p$.
quindi, se $P(X)$ ha una radice in ${}^{\mathbb{F}_p[Y]}/_{<Q(Y)>}$,
possiamo usare la proposizione sull'estensione di morfismi di campi per definire
il morfismo f, che sarà un isomorfismo. Infatti $\mathbb{F}_p \subseteq {}^{\mathbb{F}_p[X]}/_{<Q(X)>}$.
Inoltre ${}^{\mathbb{F}_p[X]}/_{<P(X)>} = \mathbb{F}_p([X])$, dove $[X]$ è la classe di $X$ in ${}^{\mathbb{F}_p[X]}/_{<P(X)>}$.
poiché ${}^{\mathbb{F}_p[Y]}/_{<Q(Y)>}$ è un campo di spezzamento di $X^{p^n} - X$ e $P(X)$ divide $X^{p^n} - X$,
allora $P(X)$ si fattorizza in fattori di grado 1 in ${}^{\mathbb{F}_p[Y]}/_{<Q(Y)>}$.

sia $\beta \in {}^{\mathbb{F}_p[Y]}/_{<Q(Y)>}$ tale che $p(\beta) = 0$.
allora l'assegnazione

$$c_0 + c_1 x + ... + c_{n-1} x^{n-1} \to c_0 + c_1 \beta + ... + c_{n-1} \beta^{n-1}$$

definisce un morfismo di anelli

$$f : {}^{\mathbb{F}_p[X]}/_{<P(X)>} \to {}^{\mathbb{F}_p[X]}/_{<Q(X)>}$$

**Esempio:** in $\mathbb{F}_3[X]$ si considerino i polinomi irriducibili

$$1 + X^2 \text{ e } 2 + X + X^2.$$

il polinomio minimo di $X$ in ${}^{\mathbb{F}_3[X]}/_{< 1 + X^2 >} := K$ su $\mathbb{F}_3$ è $1 + X^2$.
in $K' := {}^{\mathbb{F}_3[Y]}/_{< 1 + Y + Y^2 >}$ si ha che

$$1 + X^2 = (X + Y + 2)(X + 2Y + 1)$$

quindi in $K'[X], 1 + X^2$ ha due radici:

$$-Y - 2 = 2Y + 1 \text{ e } -2Y - 1 = y + 2.$$

abbiamo quindi due isomorfismi

$$\begin{gathered} f : K \to K' \\ a_0 + a_1 x \to a_0 + a_1(2Y + 1) \\ g : K \to K' \\ a_0 + a_1 x \to a_0 + a_1(Y + 2) \end{gathered}$$

$f(0) = 0$
$f(1) = 1$
$f(2) = 2$
$f(X) = 2Y + 1$
$f(1 + X) = f(1) + f(X) = 2Y + 2$
$f(2 + X) = f(2) + f(X) = 2Y$
$f(2X) = f(2)f(X) = 2f(X) = y + 2$
$f(1 + 2X) = f(1) + f(2X) = Y$
$f(2 + 2X) = f(2) + f(2X) = y + 1$

$g(0) = 0$
$g(1) = 1$
$g(2) = 2$
$g(X) = Y + 2$
$g(1 + X) = g(1) + g(X) = Y$
$g(2 + X) = g(2) + g(X) = Y + 1$
$g(2X) = g(2)g(X) = 2g(X) = 2Y + 1$
$g(1 + 2X) = g(1) + g(2X) = 2Y + 2$
$g(2 + 2X) = g(2) + g(2X) = 2Y$

***Osservazione:*** *$X \in K$ non è un generatore di $K \setminus \{0\}$.*
*infatti il sottogruppo del gruppo moltiplicativo $K \setminus \{0\}$ generato da $X$ è*
$< X >= \{X, 2, 2X, 1\} \subsetneq K \setminus \{0\}$

**Lemma:** se K è un anello commutativo di caratteristica prima p, allora

$$(X+Y)^{p^h} = X^{p^h} + Y^{p^h}$$

per ogni $x, y \in K, h \geq 1$.

***Dimostrazione:*** *sia $h = 1$. se $p > k > 0$, $p$ divide tutti i coefficienti binomiali $\binom{p}{k} := \frac{p!}{k!(p-k)!}$ perché non divide $k!(p-k)!$.*
*allora $(X+Y)^p = \sum_{k=0}^{p} \binom{p}{k} X^k Y^{p-k} = X^p + Y^p$.*
*la tesi segue per induzione.*

**Automorfismo di Frobenius:**
Dal lemma precedente segue che se K è un campo di caratteristica p, allora la funzione

$$\begin{gathered}\Phi : K \to K \\ x \to x^p\end{gathered}$$

è un morfismo di campi. infatti
$\Phi(x+y) = (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y)$
$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$
$\forall x, y \in K$.
se $K = \mathbb{F}_{p^n}, \Phi$ è un automorfismo
(essendo morfismo initettivo da un campo di cardinalità finita in se stesso)
detto **automorfismo di Frobenius**.

***Teorema:*** *il gruppo degli automorfismi di $\mathbb{F}_{p^n}, AUT(\mathbb{F}_p^n)$ è ciclico di cardinalità n, generato dall'automorfismo di Frobenius.*

***Dimostrazione:*** *vedi teorema 4.3.17 del libro di Stefania Gabelli.*

**Lemma:** sia F un campo. Il polinomio $X^d - 1$ divide il polinomio $X^n - 1$ s.s.e. d divide n.

***Dimostrazione:*** *se $n = qd + r, 0 \leq r \leq d$, in $\mathbb{F}[X]$ si ha:*

$$(x^n - 1) = (X^d - 1)(X^{n-d} + X^{n-2d} + ... + x^{n-(p-1)d} + X^r) + (X^r - 1).$$

*quindi $X^d - 1$ divide $X^n - 1$ s.s.e. $X^r - 1$ è il polinomio nullo, cioè s.s.e. $r = 0$*