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 $Im(f) = \{y \in Y : \exists x \in X \text{ tale che } f(x) = y\}$ 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 Xun 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
- $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$, $(\mathbb{C}\setminus\{0\}, \cdot)$ 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 $\langle S\rangle = \mathbb{N}$
- $S = \{0, 1\} \subseteq (\mathbb{N}, .)$. 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 σ 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.
  - $g \sim g : g \cdot e$, $\forall g \in G, e \in H$
  - $g_1 \sim g_2 \to g_2 \sim g_1 : g_1 = g_2 h \to g_1 h^{-1} = g_2$ $(h^{-1} \in H)$

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

In questo caso l'insieme quoziente lo indichiamo con G/H.

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

1.5.1 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* φ *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 φ *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* φ *è iniettivo. Dunque* φ *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* $\varphi(hk) = \varphi(\underbrace{k + k + \cdots + k}_{h \text{ volte}}) = \varphi(k)\varphi(k)\cdots\varphi(k) = [\varphi(k)]^h, \forall h \in \mathbb{Z}$. *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: $\{\{0\}, \langle \overline{29} \rangle, \langle \overline{31} \rangle, \mathbb{Z}_{899}\}$.

1.6 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 $xy = xz \to y = z, \forall y, z \in A$.*

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.

1.7 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.*

1.7.1 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 $\overline{am} = \overline{a}\overline{m} = \underbrace{\overline{m} + \overline{m} + \cdots + \overline{m}}_{a \text{ volte}} \in \langle \overline{m} \rangle$

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.

1.8 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:

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

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:

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

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

1.9 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 $\overline{365}^{-1} = \overline{-699} = \overline{1177}$.

1.10 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 Ψ 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* Ψ *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 $(2 mod 3, 5 mod 7, 4 mod 10) \in \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{10}$, questa terna corrisponde ad un elemento $x mod 210 \in \mathbb{Z}_{210}$ 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 $v_1 = 70b, v_2 = 30b = 30, v_3 = 21b$

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

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 Ψ 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 φ 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 φ 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:*

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