Algebra

Giacomo Dutto

Ottobre-Dicembre 2025

Indice

Capitolo 1

Introduzione

DEF. Sia dato un insieme A.L'**insieme delle parti** di A $\mathcal{P}(A)$, è l'unione dei sottoinsiemi di A.

1.1 Prodotto cartesiano

DEF. Dati due insiemi A,B il corpo **PRODOTTO CARTESIANO** $A \times B$ è l'insieme di tutte le coppie ordinate.

$$\{(a, b) : a \in A, b \in B\}$$

Data $\{A_1, \ldots, A_n\}$ collezione finita di insiemi il loro **prodotto cartesiano** è :

$$A_1 \times A_2 \times \ldots \times A_n = \{(x_1, \ldots, x_n,\ x_1 \in A_1, \ldots, x_n \in A_n\} = \prod_{i=1}^{n} A_i$$

Più in generale, data una famiglia di insiemi $\{A_\alpha\}_{\alpha \in I}$ indicizza con un insieme di indici I, assumendo l'assioma della scelta, si definisce il prodotto cartesiano di questa famiglia di insiemi:

$$\prod_{\alpha \in I} A_\alpha = \{f : I \to \bigcup_{\alpha \in I} A_\alpha : \forall A_\alpha \in I,\ f(\alpha) \in A_\alpha\}$$

Oss. Gli A_α possono essere anche tutti lo stesso insieme $\prod_{i \in \mathbb{Z}_+} \mathbb{R} = \mathbb{R}^\omega$ spazio delle successioni di elementi di $\mathbb{R}$.
In questo caso non serve assioma della scelta perché:

$$\prod_{i \in \mathbb{Z}_+} \mathbb{R} = \{x : \mathbb{Z}_+ \to \mathbb{R}\} \neq \varnothing$$

1.2 Funzioni ed Insiemi

Oss. Dati due insiemi X e Y, una **FUNZIONE** da X in Y; $f : X \to Y$, è un sottoinsieme $G \subseteq X \times Y$ t.c. $\forall x \in X\ \exists!\ y \in Y\ t.c.\ (x, y) \in G$
Tale $y \in Y$ viene indicato con $f(y)$

$X \rightsquigarrow$ **dominio** $\qquad Y \rightsquigarrow$ **codominio**

Notazione: $\qquad Y^X \rightsquigarrow$ funzioni da X $\to Y$

$Im(f) = f(x) = \{y \in Y : \exists\ x \in X\ t.c.\ f(x) = y\} \subseteq Y$

Oss. Oltre che della legge, f è determinata anche dal dominio e dal codominio.

Se $f : X \to Y$ e $X_0 \subseteq X$ definiamo la **restrizione di** f **ad** X_0 come la funzione $f|_{X_o} : X_0 \to Y$ data da $\{(x, f(x) : x \in X_0\}$ Date due funzioni $f : X \to Y,\ g : Y \to Z$ la **funzione composta** $g \circ f : X \to Z$ è definita da $\{(x, y) : \exists y \in Y\ t.c.\ f(x) = y\ e\ g(y) = z\}$

DEF. Una funzione $f : X \to Y$ è **INIETTIVA** (1-1) se:

$$\forall x_1, x_2 \in X con x_1 \neq x_2 \text{ si ha } f(x_1) \neq f(x_2)$$

Una funzione è **SURIETTIVA** (onto) se:

$$f(X) = Y$$

Se $f : X \to Y$ è iniettiva e suriettiva viene detta **biettiva**. In tal caso esiste la funzione inversa $f^{-1} : Y \to X$ definita ponendo $f^-1(y)$ l'unico $x \in X\ t.c.\ f(x) = y$

Dato X insieme definiamo $id_x : X \to X$ la **funzione identica** data dalla legge $id_x(x) = x\ \forall x \in X$

$$\{(x, x) : x \in X\}$$

Se una funzione $f : X \to Y$ è biettiva si

$$f^{-1} \circ f = id_x : X \to X$$

$$f \circ f^{-1} = id_y : Y \to Y$$

ATTENZIONE!!! Il concetto di inversa non è da confondere con quello di contronominale

DEF. Data $f : X \to Y$ è $Y_0 \subseteq$ la **controimmagine di** Y_0 è l'insieme $f^{-1}(Y_0) = \{x \in X : f(x) \in Y_0\}$

Oss. L'operazione di prendere la controimmagine si comporta bene rispetto a inclusioni, unioni, intersezioni e differenze d'insieme:

a) Se $A_1 \subseteq A_2 \subseteq Y \implies f^{-1}(A_1) \subseteq f^{-1}(A_2)$

b) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

c) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

d) Sia $A_1 \subseteq A_2 \subseteq Y \implies f^{-1}(A_2 \backslash A_1) = f^{-1}(A_2) \backslash f^{-1}(A_1)$

ATTENZIONE!!! L'operazione di prendere l'immagine preserva solo le inclusioni e le unioni.

Prop.

i) $A \subseteq f^{-1}(f(A))$ (= sse f è iniettiva).

ii) $f^{-1}(f(B)) \subseteq B$ (= sse $B \subseteq Im(f)$, in particolare se f è suriettiva).

1.3 Corrispondenze e Relazioni

DEF. Dati X, Y insiemi, una **Corrispondenza** F con dominio X e codominio Y è un sottoinsieme di $X \times Y$.

Oss. Rispetto alla definizione di funzione $f : X \to Y$ non richiediamo che ogni elemento di X compaia come prima coordinata di un elemento di F esattamente una volta.

DEF. Dato X un'insieme, una relazione su X è un sottoinsieme di R di $X \times X$. Se $a, b \in X$ sono in relazioni i.e. $(a, b) \in R$ scriveremo "aRb".

1.4 Relazione di equivalenza e d'ordine

DEF. Una relazione R su X si dice **RELAZIONE DI EQUIVALENZA** se per $a, b, c \in X$ si ha:

1) $aRa\ \forall a \in X$ (proprietà riflessiva)
2) $aRb\ \Rightarrow bRa$ (proprietà simmetrica)
3) $aRb,\ bRc \Rightarrow aRc$ (proprietà transitiva)

DEF. Una relazione di equivalenza R su X permette di definire la **classe di equivalenza** di un qualunque $x \in X$:

$$[x] = \{y \in X\ t.c\ xRy\}$$

NOTAZIONI COMUNI

$X/R \rightsquigarrow$ **insieme delle classi di equivalenza o insieme quoziente**

Prop. Due classi di equivalenza o sono disgiunte o coincidono.

Oss. La collezione delle classi di equivalenza di X rispetto a R forma quindi una partizione di X-

DEF. Sia X un insieme, una **PARTIZIONE di X** è una famiglia $\{X_i\}_{i \in I} \subseteq \mathcal{P}(X)$ di insiemmi non vuoti disgiunti t.c.

$$\bigcup_{i \in I} X_i = X$$

DEF. Una relazione R su X è detta **relazione d'ordine** se RIFLESSIVA, TRANSITIVA e per $\forall a, b \in X$ si ha aRb e $bRa \Rightarrow a = b$ (proprietà antisimmetrica).
(X, R) si dice **totalmente ordinato** se $\forall a, b, \in X$ vale che aRb oppure bRa altrimenti si dirà **parzialmente ordinato**.

Capitolo 2

Gruppi

2.1 Gruppi

DEF. Un gruppo (G, $\star$) è un insieme non vuoto G munito di un'operazione $\star$, cioè un'applicazione

$$G \times G \to G$$

$$(x, y) \to x \star y$$

che gode delle seguenti proprietà:

- **Associativa:** $\forall x, y, z \in G$

$$(x \star y) \star z = x \star (y \star z) = x \star y \star z$$

- **Esistenza dell'elemento neutro:**

$$\exists u \in G : u \star x = x \star u = x \qquad \forall x \in G$$

- **Esistenza dell'inverso**:

$$\forall x \in G,\ \exists\ x' \in G : x \star x' = x' \star x = u$$

Prop. In un gruppo, l'elemento neutro è unico.

Prop. In un gruppo, l'inverso di ogni elemento è unico.

DEF. Un gruppo (G,$\star$) è detto **abeliano** (o commutativo) se $\star$ è commutativa:

$$\forall x, y \in G :\ x \star y = y \star x$$

NOTAZIONI COMUNI

Notazione additiva:

- Operazione $\star = +$

- Elemento neutro $= 0_G$
- Inverso $= -x$

Notazione moltiplicativa:

- Operazione $\star = \cdot$
- Elemento neutro $= 1_G$
- Inverso $= x^{-1}$

E.g. Gruppo simmetrico di ordine n
Prendiamo come X l'insieme $X = I_n\{1, 2, \ldots, n\}$
$(\mathcal{B}(I_n), \cdot) = S_n$ è detto gruppo simmetrico di ordine n.
(È il gruppo delle permutazioni di n elementi dotato dell'operazione di composizione).
$|S_n| = n!$

E.g. Gruppo diedrale
Sia P_n un poligono regolare di n lati nel piano $n \geq 3$.
L'insieme delle isometrie di P_n è un gruppo rispetto alla composizione, detto gruppo diedrale, viene denotato da D_n o Δ_n. $|\Delta_n| = 2n$

Prop. Sia $(G, \star)$ un gruppo, siano a,b,c $\in G$.
Valgono le **leggi di di semplificazione** o (di cancellazione):

- se $a \star b = a \star c \implies b = c$
- se $b \star a = c \star a \implies b = c$

Oss. Se $\star$ non è commutativa:

$$a \star b = c \star a \not\Rightarrow b = c$$

Oss.

$$\mathbb{Z}_n^* = \text{tutti gli elementi di } \mathbb{Z}_n \text{ che hanno un inverso moltiplicativo.}$$

Se n è primo, $\mathbb{Z}_n^* = \mathbb{Z}_n \backslash \{[0_n]\}$, cioè se n è primo $(\mathbb{Z}_n \backslash \{[0_n]\}, \cdot)$ è un gruppo; (vale anche il contrario, ma si vedrà in futuro).

Prop. (G, $\cdot$) gruppo (con notazione moltiplicativa) e a,b$\in G$. Allora:

- $(1_G)^{-1} = 1_G$
- $(a^{-1})^{-1} = a$
- $(ab)^{-1} = b^{-1} \cdot a^{-1}$

DEF. (G, $\cdot$) gruppo, $a \in G$ elemento. $\forall m \in \mathbb{Z}$ si dice **potenza m-esima di a** l'elemento:

$$a^m := \begin{cases} \text{se } m > 0 : a^m = a \cdot a \cdot a \cdot \ldots \cdot a \quad (m \text{ volte}) \\ \text{se } m = 0 : a^0 = 1_G \\ \text{se } m < 0 : a^m = (a^{-m})^{-1} \end{cases}$$

Oss. Se usiamo la notazione additiva (G,+), invece di potenza m-esima si parla di **multiplo m-esimo di a**:

$$ma := \begin{cases} \text{se } m > 0 : ma = a \cdot a \cdot a \cdot \ldots \cdot a \quad (m \text{ volte}) \\ \text{se } m = 0 : 0 \cdot a = 0_G \\ \text{se } m < 0 : ma = -((-m) \cdot a) \end{cases}$$

Prop. Sia $(G, \cdot)$ gruppo, $a, b \in G$ 2 elementi.

- $a^n \cdot a^m = a^{n+m} \quad \forall n, m \in \mathbb{Z}$
- $(a^n)^m = a^{nm} \quad \forall n, m \in \mathbb{Z}$

Se G è abeliano:

- $(ab)^m = a^m \cdot b^m \quad \forall m \in \mathbb{Z}$

Oss. $(ab)^m = (ab) \cdot (ab) = ab \cdot ab \neq aa \cdot bb$ (perché $\cdot$ non è commutativa per definizione.

2.2 OMOMORFISMI

DEF. Siano $(G, \star)$ e $(H, *)$ due gruppi. Una funzione $f : G \to H$ è detta **OMOMORFISMO** o (**morfismo di gruppi**) se $\forall x, y, \in G$:

$$f(x \star y) = f(x) * f(y)$$

DEF. Sia $f : (G, \star) \to (H, *)$ un omomorfismo. f è detto:

- **MONOMORFISMO** se è iniettivo
- **EPIMORFISMO** se è suriettivo
- **ISOMORFISMO** se è biettivo

Se $\exists$ un isomorfismo da G ad H, i gruppi si dicono **ISOMORFI** (e si scrive $G \cong H,\ G \simeq H$).
Un omomorfismo di un gruppo in se stesso è detto **ENDOMORFISMO**.
Un isomorfismo di un gruppo in se stesso è detto **AUTOMORFISMO**.

Prop. Sia $f : G \to H$ omomorfismo. Allora (usando la notazione moltiplicativa sia in G che in H):

- $f(1_G) = 1_H$
- $f(a^{-1}) = f(a)^{-1} \quad \forall a \in G,\ \forall m \in \mathbb{Z}$
- $f(a^m) = f(a)^m \quad \forall a \in G,\ \forall m \in \mathbb{Z}$

2.3 SOTTOGRUPPI

DEF. Sia $(G, \cdot)$ un gruppo. Un sottoinsieme $H \subseteq G$ è detto **SOTTOGRUPPO** se è un gruppo con la restrizione ad H dell'operazione di G. Si scrive $H < G$ o $H \leq G$.
I sottogruppi $\{1_G\}$ e G sono detti **sottogruppi impropri**.

Prop. Sia $(G, \cdot)$ un gruppo e sia $H < G$ un sottogruppo. Allora:

i) H è stabile

ii) se G è abeliano anche H è abeliano

iii) l'elemento neutro di H coincide con l'elemento neutro di G

iv) l'inverso in H di un elemento di H coincide con il suo inverso in G

Oss.

ii) il viceversa è falso: un gruppo non abeliano ammette sottogruppi abeliani

iii) in particolare, H sottogruppo $\implies 1_G \in H$

iv) in particolare, H sottogruppo implica: $x \in H \implies x^{-1} \in H$

Oss. Se $H \subseteq G$ è un sottoinsieme tale che:

- H è stabile
- $1_G \in H$
- Se $x \in H \implies x^{-1} \in H$

allora H è un sottogruppo

CRITERIO PER SOTTOGRUPPI

$(G, \cdot)$ gruppo. $H \subseteq G$ sottoinsieme.

H è sottogruppo $\iff \forall x, y \in H: \ x \cdot y^{-1} \in H$

Prop. $(G, \cdot)$ un gruppo e H,K sottogruppi.
Allora $H \cap K$ è un sottogruppo.

Oss. In generale l'unione di sottgruppi NON è un sottogruppo!!

DEF. G gruppo, H e K sottogruppi. Si dice **sottogruppi unione** di H e K, si denota $H \vee K$, il minimo sottogruppo di G che contiene sia H che K:

$$H \vee K = \bigcap_{\substack{L \leq G \\ L \supseteq H \cup K}} L$$

Prop. $(G, \cdot)$ gruppo, H e K sottogruppi. Allora:

$$H \vee K = \{h_1 \cdot k_1 \cdot h_2 \cdot k_2 \cdot h_2 \cdot k_2 \cdot ... \cdot h_n \cdot k_n \mid h_i \in H, k_i \in K\}$$

Corollario Se $(G, \cdot)$ è abeliano, allora

$$H \vee K = \{h \cdot k \mid h \in H, k \in K\}$$

Oss. è possibile vedere il sottogruppo unione anche come "il sottogruppo generato dall'insieme $H \cup K$".

DEF. Siano G un gruppo e A un suo sottoinsieme. Il **sottogruppo di G generato dell'insieme A** è il più piccolo sottogruppo di G che contiene A:

$$\langle A \rangle = \bigcap_{\substack{L \leq G \\ L \supseteq A}} L$$

Oss. $\langle \{x\} \rangle = \langle x \rangle$

2.4 Gruppi Ciclici

DEF. Siano $(G, \cdot)$ un gruppo, e $x \in G$ un elemento.
Il **sottogruppo ciclico da x** è il più piccolo sottogruppo G che contiene l'elemento x. Si denota $\langle x \rangle$

$$\langle x \rangle = \bigcap_{\substack{H \leq G \\ x \in H}} H$$

Prop. Siano $(G, \cdot)$ un gruppo e $x \in G$ un elemento.
Allora il sottogruppo ciclico generato da x coincide con le potenze intere di x:

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$$

Oss. I sottogruppi ciclici sono commutativi:

$$x^n \cdot x^m = x^{n+m} = x^{m+n} = x^m \cdot x^n$$

DEF. Un gruppo è detto **CICLICO** se $\exists$ un elemento $x \in G$ t.c. $\langle x \rangle = G$

Oss. Il generatore di un gruppo ciclico NON è unico:

es: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

Oss. Un gruppo ciclico è commutativo:
Se $G = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$
dati $a, b \in G$, $\exists s, t, \in \mathbb{Z}$ t.c. $a = x^s, b = x^t$ allora

$$a \cdot b = x^s \cdot x^t = x^{s+t} = x^{t+s} = x^t \cdot x^s = b \cdot a$$

Attenzione però che non tutti i gruppi commutativi sono ciclici!

Prop. Sia H un sottogruppo di $(\mathbb{Z}, +)$.
Allora $\exists k \in \mathbb{N}_0$ t.c. $H = k\mathbb{Z}$. (Cioè i sottogruppi di $\mathbb{Z}$ sono tutti e soli quelli del tipo $k\mathbb{Z} = \langle k \rangle$

DEF. In un gruppo $(G, \cdot)$ si dice **ORDINE** di un elemento $x \in G$ il minimo $n \in \mathbb{N}$ tale che $x^n = 1_G$.
Se tale n non esiste, diciamo che l'elemento x ha **ordine infinito**.

Prop. Sia $(G, \cdot)$ gruppo, $x \in G$.
Se esistono $s, t \in \mathbb{Z}$ tali che $s \neq t$ ma $x^s = x^t$, allora:

i) $\exists$ minimo intero positivo n t.c. $x^n = 1_G$ (cioè ha ordine finito).

ii) Se m è intero, $x^m = 1_G \iff n \mid m$

iii) Gli elementi $x^0 = 1_G, x, x^2, ..., x^{n-1}$ sono tutti disgiunti. In particolare:

$$\langle x \rangle = \{1_G,\ x,\ x^2,\ ...,\ x^{n-1}\}$$

Corollario L'ordine di un elemento coincide con la cardinalità del sottogruppo ciclico da lui generato (spesso si usa il termine "ordine" al posto di "cardinalità".

$$\text{ord(x)} = |\langle x \rangle|$$

Prop. Ogni sottogruppo di un gruppo ciclico è ciclico.

Prop. Ogni gruppo ciclico è isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_n$ per qualche $n \in \mathbb{N}$.

2.5 Omomorfismi e sottogruppi

Prop. Sia $f : G \to H$ omomorfismo, $\{f(g_1 g_2) = f(g_1)f(g_2)\}$.
Sia $K \leq G$ sottogruppo.
Allora $f(K) \leq H$ è sottogruppo.

Corollario $f : G \to H$ omomorfismo, allora $Im(f) = f(G)$ è un sottogruppo di H.

Prop. $f : G \to H$ omomorfismo, sia $L \leq H$ sottogruppo. Allora $f^{-1}(L) \leq$ G è un sottogruppo.

DEF. Sia $f : G \to H$ un omomorfismo di gruppi.
Il **NUCLEO** di f, denotato $\mathbf{ker(}f\mathbf{)}$, è l'insieme delle retroimmagini dell'elemento neutro di H:

$$\ker(f) = \{g \in G \mid f(g) = 1_H\} = f^{-1}(\{1_H\})$$

Corollario $\ker(f)$ è un sottogruppo di G.

Prop. $f : G \to H$ omomorfismo. Allora:

i) f è epimorfismo $\iff Im(f) = H$;

ii) fè monomorfismo $\iff \ker(f) = \{1_G\}$.

2.6 Gruppo simmetrico

DEF.

$$S_n = \{\text{gruppo delle biezioni di } I_n, \text{ dotato della composizione}\}$$
$$I_n = \{1, 2, ..., n\}$$

DEF. Gli elementi di S_n si dicono "**permutazioni**".

Oss. La cardinalità di S_n è:
$$|S_n| = n!$$

DEF. Dati $a_1,\ a_2,\ ...,\ a_k \in I_n$, indichiamo con $(a_1 a_2 ... a_k)$ la permutazione σ tale che:

$$\begin{cases} \sigma(a_i) = a_{i+1} & \text{per } i = 1, \dots, k-1 \\ \sigma(a_k) = a_1 \end{cases}$$

e che lascia invariati tutti gli altri elementi di I_n.

Tale permutazione è detta **ciclo di lunghezza k**.
Un ciclo di lunghezza 2 e detto **trasposizione**.
Due cicli si dicono **disgiunti** se tali sono gli insiemi degli elementi da loro permutati.

Prop. Ogni permutazione può essere decomposta nel prodotto di un numero finito di cicli disgiunti. Tale decomposizione è unica a meno dell'ordine dei fattori.

Oss. $\gamma = (a_1 a_2 ... a_k)$ ciclo di lunghezza k.

$$\text{ord}(\gamma) = k$$

Corollario Sia $\sigma \in S_n$ e sia $\sigma = \gamma_1 \gamma_2 ... \gamma_t$ una decomposizione di σ in cicli disgiunti. Allora ord(σ)=mcm(ord(γ_1), ord(γ_2), ..., ord(γ_t)) e quindi il mcm delle lunghezze dei vari cicli.

$$\sigma = \gamma_1 \gamma_2 \gamma_3$$

Prop. Ogni permutazione può essere decomposta in un prodotto di trasposizioni.

TEOREMA Il numero di trasposizioni in cui si può decomporre una data permutazione o è sempre **pari** o è sempre **dispari**.

DEF. Una permutazione è detta **PARI** (rispettivamente **DISPARI**) se si decompone in un numero PARI (rispettivamente DISPARI) di trasposizioni.

DEF. Le permutazioni pari di S_n formano un gruppo, detto **gruppo ALTERNO** e denotato con A_n.

DEF. Possiamo definire **l'applicazione segno**:

$$\begin{aligned} \mathrm{sgn}\colon S_n &\longrightarrow \{\pm 1\} \\ \sigma &\longmapsto \begin{cases} +1 & \text{se } \sigma \text{ è pari} \\ -1 & \text{se } \sigma \text{ è dispari} \end{cases} \end{aligned}$$

Oss. sgn è un omomorfismo:

$$(S_n, \star) \longrightarrow (\{\pm 1, \cdot\})$$
$$sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$$

Inoltre A_n=Ker(sgn).

Teorema di Cailey Ogni gruppo è isomorfo a un gruppo di permutazioni sui suoi elementi.

Oss. G gruppo:

Sym(G)= gruppo delle permutazioni degli elementi dell'insieme G, dotato della composizione.

Corollario Se $|G| = n < \infty$, allora G è isomorfo a un sottogruppo di S_n

2.7 Classi laterali di un sottogruppo

Sia $(G, \cdot)$ un gruppo, e $H \leq G$ un sottogruppo. H induce una relazione sugli elementi di G:

$$\begin{aligned} \forall a, b \in G : a \sim_H b &\iff ba^{-1} \in H \\ &\iff \exists h \in H \text{ t.c. } b = ha \end{aligned}$$

$\sim_H$ è una relazione di equivalenza:

- riflessiva: $a \sim_H a$
- simmetrica: $a \sim_H b = b \sim_H a$
- transitiva: $a \sim_H b,\ b \sim_H c \implies a \sim_H c$

DEF. Le classi di equivalenza della relazione $\sim_H$ sono dette **CLASSI LATERALI DESTRE (o laterali sinistre)** del sottogruppo H e sono denotate:

$$[a]_{\sim_H} = \{b \in G \mid a \sim_H b\} = \{b \in G \mid \exists h \in H \text{ t.c. } b = ha\} = \{ha \mid h \in H\} =: Ha$$

Oss. Invece delle relazioni sopra, possiamo definire:

$$\begin{aligned} a \ {}_H\!\sim b &\iff a^{-1}b \in H \\ &\iff \exists h \in H \text{ t.c. } b = ah \end{aligned}$$

che si verifica essere di equivalenza.

DEF. Le classi di equivalenza rispetto alla relazione sono dette **classi laterali sinistre** e denotate con:

$$[a]_{H\sim} = aH = \{ah \mid h \in H\}$$

Oss. l'insieme delle classi laterali destre (rispettivamente sinistre) è l'insieme quoziente, denotato con $G/\sim_H$ (rispettivamente $G/{}_H\sim$).
Esiste un morfismo suriettivo naturale:

$$\begin{aligned} \pi : G &\longrightarrow G/\sim_H \\ a &\longrightarrow Ha \end{aligned}$$

detto proiezione.

Oss. Se usiamo la notazione additiva:

$$a \sim_H b \iff b - a \in H$$

e le classi laterali si denotano "H+a".

Oss. Se G è abeliano: ah=ha $\forall a \wedge \forall h$, quindi $\forall$ sottogruppo $H \leq G$ vale che:

$$aH = Ha \quad \forall a \in G$$

In generale $aH \neq Ha$ $\forall a \in G$ però:

- sono in ugual numero
- hanno lo stesso numero di elementi

Prop. Nelle notazioni precedenti, esiste una biezione:

$$\begin{aligned} f : G/{}_H\sim &\longrightarrow G/\sim_H \\ aH &\longrightarrow Ha^{-1} \end{aligned}$$

DEF. G gruppo, $H \leq G$ sottogruppo. **L'indice** di H in G il numero di classi laterali di H in G (destre o sinistre è uguale, perché $|G/{}_H\sim| = |G/\sim_H|$). Tale numero di denota **[G:H]**.

Oss.

i) se $|G| < \infty \implies$ l'indice di ogni $H \leq G$ è un numero naturale

ii) $|G| = \infty \implies$ l'indice di $H \leq G$ può essere un numero naturale, o infinito.

iii) $[G : \{1_G\}] = |G|$

iv) $[G : G] = 1$
$a \sim b \iff ba^{-1} \in G$

Teorema di Lagrange
G gruppo finito, $H \leq G$ sottogruppo, allora:

$$[G : H] = \frac{|G|}{|H|} (\iff |G| = |H|[G : H])$$

In particolare, l'ordine di H divide l'ordine di G: $|H|/|G|$.

Corollario L'ordine di ogni elemento di un gruppo finito G divide $|G|$.

Corollario G gruppo finito, allora $\forall x \in G : x^{|G|} = 1_G$

Corollario Un gruppo finito il cui ordine è un numero primo è necessariamente ciclico.

Oss. Il teorema di Lagrange dice che se $H \leq G \implies |H| \mid |G|$.
Il viceversa è falso, cioè non è vero che per ogni divisore d di $|G| \exists H \leq G$ t.c. $|H| = d$
È vero solo per i gruppi ciclici.

DEF. Un sottogruppo N di un gruppo G è detto **SOTTOGRUPPO NORMALE** (e denotato $N \trianglelefteq G,\ N \triangleleft G$) Se $\forall a \in G$:

$$aN = Na$$

In tal caso i due insiemi quozienti $G/\sim_N = G/\ _N\sim$ e si denota l'insieme quoziente semplice G/N (G "modulo" N).

Oss. attenzione che $aN = Na \nRightarrow an = na\ \forall n \in N$

$$aN = Na \text{ significa } an = n'a$$

Oss. in un gruppo abeliano, tutti i sottogruppi sono normali.

CRITERIO DI NORMALITÀ G gruppo, $N \leq G$ sottogruppo.
N è normale se e solo se:

$$\forall a \in G,\ \forall h \in N : aha^{-1} \in N$$

Oss. G gruppo finito, $H \leq G$ t.c [G:H]=2.
Allora H è normale.

2.8 Gruppo Quoziente

$N \leq G$ sottogruppo:
$aN = \{an \mid n \in N\}$
$Na = na \mid n \in N$
$|aN| = |Na| = |N|$ Numero di classi laterali $= \frac{|G|}{|N|}$ Se N è un sottoruppo normale G/N= insieme quoziente.

Prop. Siano G un gruppo e $N \triangleleft G$ sottogruppo normale. Allora è possibile definire un'operazione sull'insieme quoziente G/N rispetto alla quale G/N è un gruppo e la proiezione canonica:

$$\begin{aligned} \pi : G &\longrightarrow G/N \\ a &\longrightarrow aN \end{aligned}$$

è un omomorfismo di gruppi, che ha come nucleo $Ker(\pi) = N$.

Oss. Dalla proposizione segue che un sottogruppo normale coincide con nucleo di π, cioè col nucleo di un omomorfismo.
Viceversa:

Prop. Sia $f : G \to G'$ omomorfismo di gruppi.
Allora $ker(f) \lhd G$ è un sottogruppo normale.

TEOREMA FONDAMENTALE DI OMOMORFISMO PER GRUPPI
Sia $\varphi : G \to G'$ omomorfismo di gruppi e sia $K = Ker(\varphi)$. Siano inoltre $\pi : G \to G/k$ la proiezione sul gruppo quoziente. Allora $\exists$ un omomorfismo iniettivo $\overline{\varphi} : G/K \to G'$ tale che $\overline{\varphi} \circ \pi = \varphi$, cioè tale che il seguente diagramma è commutativo:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\ G/K \arrow[ur, "\overline{\varphi}"] & \end{tikzcd}$$

In particolare, esiste un isomorfismo $G/K \cong Im(\varphi)$.

Capitolo 3

Teoria dei numeri

3.1 Regola di Bezout

Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Allora:

i) il minimo intero $d > 0$ che si può scrivere nella forma:

$$d = \alpha \cdot a + \beta \cdot b$$

per qualche α e $\beta \in \mathbb{Z}$ è un MCD di a e b.

ii) Esistono esattamente 2 MCD di a e b, che sono: d e -d.

Corollario Due interi a e b non entrambi nulli sono coprimi $\iff \exists\, \alpha, \beta \in \mathbb{Z}\ t.c.\ 1 = a \cdot \alpha + b \cdot \beta$.

Lemma Siano a e b interi non nulli, sia r il resto della divisione di a per b.
Allora MCD(a,b)=MCD(b,r)

3.2 Algoritmo euclideo per il calcolo del MCD

Siano $a, b \in \mathbb{Z};\ a, b \neq 0$
Siccome $MCD(a, b) = MCD(|a|, |b|)$, possiamo supporre che a,b¿0.

$$a_1 = a; a_2 = b$$

Dividiamo a_1 per a_2:

$$a_1 = q_1 \cdot a_2 + a_3$$

ora dividiamo a_2 per a_3

$$a_2 = q_2 \cdot a_3 + a_4$$

si itera il processo seguendo questo schema:

$$a_{i-1} = q_{i-1} \cdot a_i + a_{i+1}$$

dove a_{i+1} =resto della divisione di a_{i-1} per a_i. Stiamo costruendo una sequenza $\{a_i\}$ con le proprietà

- $a_i \geq 0$

- $a_2 > a_3 > a_4 > \ldots > a_n = 0$

Dopo un numero finito di passi, arrivo ad $a_n = 0$. Sia a_{n-1} l'ultimo resto non nullo.

$$a_{n-1} = MCD(a_{n-2}, a_{n-1}) = MCD(a_{n-3}, a_{n-2}) = \ldots = MCD(a_1, a_2) = MCD(a, b)$$

Prop. Siano $a, b, n \in \mathbb{Z}$ tali che $n|ab$.
Se MCD(a,n)=1 $\implies n|b$

Corollario Siano $a, b, p \in \mathbb{Z}$, con p primo.
Se $p|ab \implies p|a$ oppure $p|b$. Nota: vale anche il viceversa.

3.3 Teorema cinese dei resti

Questo teorema ha 2 formulazioni: una più astratta, che riguarda le classi di resto modulo un intero, e una che è una applicazione diretta alle congruenze diofantee $\rightarrow$ dove cerco soluzioni intere.

TEOREMA Formulazione astratta:
Siano $m_1, m_2, m_3, \ldots, m_s \in \mathbb{N}$ a due a due coprimi e sia $n = m_1 \cdot m_2 \cdot \ldots \cdot m_s$ il loro prodotto.
Allora l'applicazione :

$$\begin{aligned} \Gamma : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_s} \\ [a]_n &\longrightarrow ([a]_{m_1}, [a]_{m_2}, \ldots, [a]_{m_s}) \end{aligned}$$

è biettiva!

TEOREMA Siano m_1 e $m_2 \geq 1$ due interi coprimi.
Allora per ogni coppia $a, b \in \mathbb{Z}$, il sistema di congruenze

$$\begin{cases} x \equiv a (\text{mod } m_1) \\ x \equiv b (\text{mod } m_2) \end{cases}$$

ammette sempre soluzioni.

3.4 Piccolo teorema di Fermat

Prop. In $\mathbb{Z}_n$ un elemento $[a]_n$ è invertibile $\iff MCD(a, n) = 1$. In altre parole: $\mathbb{Z}_n^* = \{[a]_n | MCD(a, n) = 1\}$

Corollario $\mathbb{Z}_p$ è un campo $\iff$ p è primo

$$\mathbb{Z}_p = \mathbb{Z}_p \{[0]_p\} \text{ sse p è primo}$$

TEOREMA Piccolo teorema di Fermat Sia p un primo e sia $a \in \mathbb{Z}$ un intero non divisibile per p. Allora:

$$a^{p-1} \equiv 1 (\text{mod p})$$

Capitolo 4

Anelli

4.1 Anelli e Campi

DEF. Un' anello (A, +, ·) è un insieme non vuoto A dotato di 2 operazioni somma (+) e prodottto (·) che godono delle seguenti proprietà:

I) (A, +) è un gruppo abeliano (il cui elemento neutro è 0_A)

II) · è associativa

III) Valgono le proprietà distributive $\forall a, b, c \in A$:
$a \cdot (b + c) = a \cdot b + a \cdot c$
$(a + b) \cdot c = a \cdot c + b \cdot c$

Oss. I) A è detto anello unitario (o anello con unità) se $\exists$ l'elementoa neutro 1_A del prodotto.

II) Gli elementi di A che hanno inverso moltiplicativo sono detti "invertibili".

III) A è detto commutativo se il prodotto è commutativo.

IV) Un anello dove ogni elemento $\neq 0_A$ è invertibile è detto **CORPO**.

V) Un corpo commutativo è detto **CAMPO**.

Prop. A anello:

- 0_A e -a sono unici $\forall a \in A$.
- se $\exists$, 1_A e a^{-1} sono unici $\forall a \in A$ invertibile.
- $-(-a) = a$ e $-(a + b) = -a - b \quad \forall a, b \in A$.
- Vale la legge di semplificazione per la somma:
$a + b = a + c \implies b = c$.
- L'equazione $a + x = b$ ha sempre un'unica soluzione.

Oss. Le ultime 2 proprietà non valgono in generale per il PRODOTTO!!!

Prop. In un anelo A esistono i multipli interi di ciascun elemento, che godono delle seguenti proprietà $\forall n, m \in \mathbb{N}_0, \forall a, b \in A$:

- $(a^n)^m = a^{nm}$
- $a^n \cdot a^m = a^{n+m}$

se A è commutativo:

- $(ab)^n = a^n \cdot b^n$

Prop. In un anello A:

- $a * 0_A = 0_A * a = 0_A \quad \forall a \in A.$

Prop. In un anello A, $1_A \neq 0_A$.

Prop. In un anello A, $\forall a, b \in A$, vale:

- $(-a) \cdot b = -(ab)$
- $a \cdot (-b) = -(ab)$
- $(-a) \cdot (-b) = ab$
- $(-1_A) \cdot a = -a$

Prop. In un anello A, $\forall a, b \in A, \forall n \in \mathbb{Z}$ vale:

- $n(a \cdot b) = (na) \cdot b = a \cdot (nb)$

Prop. In un anello A, $\forall a, b \in A, \forall n \in \mathbb{N}_0$:

- $(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$

DEF. Due elementi a,b di un anello A si dicono **divisori dello zero** (zero-divisore) se $a \neq 0_A, b \neq 0_A$ ma o $a \cdot b = 0_A$ oppure $b \cdot a = 0_A$.

- Un anello commutativo privo di divisori dello zero è detto **dominio di integrabilità**.

Prop. Un anello commutativo A è un dominio di integrabilità $\iff$ vale la legge di semplificazione per il prodotto:

- se $a \neq 0_A$ è t.c. $a \cdot b = a \cdot c \implies b = c$.

Prop/Oss. In un anello A, gli elementi invertibili (che si denotano A^* formano un gruppo rispetto al prodotto:

- $(A, +, \cdot)$ anello $\implies (A^*, \cdot)$ gruppo.
- Se A è un campo $A^* = A - \{0_A\}$.

Corollario ogni campo è un dominio di integrabilità.

DEF. Si dice **CARATTERISTICA**, "Char(A)" di un anello A il minimo intero positivo n tale che $na = 0_A \quad \forall a \in A$.
Se tale n non esiste, si dice che l'anello ha caratteristica 0.

Oss. Se A possiede l'unità, la sua caratteristica coincide con l'ordine additivo di 1_A:

- ord(1_A)=min$\{n \in \mathbb{N} \mid n \cdot 1_A = 0_A\}$

Se il minimo esiste, cioè quando la caratteristica è positiva. Altrimenti, se ord(1_A)=inf, char(A)=0.

Prop. La caratteristica di un dominio di integrità (e quindi in particolare di un campo) o è 0, oppure è un numero primo.

Oss. $\mathbb{Z}_n$ è un campo se e solo se n è primo.

4.2 Morfismi di anelli

DEF. Siano A e A' due anelli. Un'applicazione $\varphi : A \to A'$ è detta **omomorfismo** (o morfismo di anelli) se $\forall a, b \in A$:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

N.B. La prima addizione/prodotto e la seconda addizione/prodotto sono due operazioni differenti, definite nei relativi due anelli A e A'.

- Un omomorfismo **iniettivo** si dice **monomorfismo**
- Un omomorfismo **suriettivo** si dice **epimorfismo**
- Un omomorfismo **biettivo** si dice **isomorfismo**

Oss. Un morfismo di anelli è t.c. $\varphi(0_A) = 0_{A'}$.
Se però entrambi gli anelli possiedono l'unità, non è automatico che $\varphi(1_A) = 1_{A'}$.

DEF. Un omo-mono-epi-isomorfismo di anelli con unità è detto omo-mono-epi-isomorfismo se oltre alle condizioni della definizione precedente vale anche $\varphi(1_A) = 1_{A'}$.

Prop. Se $\varphi : A \to A'$ è un omomorfismo, $\forall n \in \mathbb{Z}$,∀k$\in \mathbb{N}_0$, $\forall a \in A$:

- $\varphi(0_A) = 0_{A'}$
- $\varphi(-a) = -\varphi(a)$
- $\varphi(na) = \text{n}\varphi(a)$

- $\varphi(a^k) = \varphi(a)^k$

DEF. $\varphi : A \to A'$ morfismo di anelli. Il nucle ker(φ) è il nucle di φ come morfismo di gruppi additivi, cioè:

- ker(φ)= $\{a \to A \mid \varphi(a) = 0_{A'}\}$

Oss. φ è iniettivo $\iff$ ker(φ)=$\{0_A\}$.

Prop. Se A è un anello con char(A)=0, allora l'omomorfismo unitario μ è iniettivo.
Se invece char(A)=$K > 0$, allora ker(μ)=k$\mathbb{Z}$.

DEF. Un sottoinsieme non vuoto S di un anello A è detto **sottoanello** se è un anello rispetto alla restrizione delle 2 operazioni.

Oss. S è un sottoanello se:

- S è un sottogruppo additivo
- S è stabile (chiuso) rispetto al prodotto:
  a,b $\in A \implies a \cdot b \in S$

CRITERIO PER SOTTOANELLI Un sottoinsieme non vuoto S di un anello A è un sottoanello se e solo se $\forall a, b \in S$:

- a-b $\in$ S
- a $\cdot$ b $\in$S

4.3 Ideali

DEF. Un sottoinsieme I di un anello A si dice **IDEALE (o un ideale bilatero)** di A se valgono le seguenti proprietà:

- $\forall x, y, \in I : x - y \in I$
  (cioè I è sottogruppo additivo)
- $\forall x \in I$ e $\forall a \in A : a \cdot x \in I$ e $x \cdot a \in I$
  (cioè I "ingloba" per moltiplicazione tutti gli elementi di A)

Oss.
- ogni ideale è un sottoanello
- $\{0_A\}$ e A sono ideali impropri

Oss. A anello con 1_A, I ideale.
Se $1_A \in I \implies I = A$
Infatti, $\forall a \in A : a \cdot 1_A \in I$

Prop. Siano A e A' anelli con unità e $\varphi : A \to A'$ omomorfismi. Allora:

I) Im(φ)è un sottoanello di A'

II) Ker(φ) è un ideale di A

Prop. Un campo non ha ideali propri.
(Gli unici ideali di un campo K sono $\{0_K\}$ e K stesso).

Corollario Tutti gli omomorfismi di campi sono iniettivi.

Prop. A, A' sono anelli unitari, $\varphi : A \to A'$ omomorfismi.

I) L'immagine è la restroimmagine di un sottoanello sono **sottoanelli**.

II) La retroimmagine di un ideale è un **ideale**.

III) Se φ è suriettivo, l'immagine di un ideale è un **ideale**.

DEF. A anello con unità. Dato un elemento $x \in A$, **l'ideale principale generato da x** (denotato con "(x)") è il più piccolo ideale di A che contiene x, cioè:

$$(x) = \bigcap_{\substack{I \subseteq A \text{ ideale} \\ I \ni x}} I$$

Prop. Se A è commutativo, allora:

$$(x) = \{a \cdot x \mid a \in A\}$$

DEF. Un anello A è detto **anello a ideali principali** se tutti i suoi ideali sono principali.
Un domio di integrabilità a ideali principali si denota con la sigla **PID** (Principal Ideal Domain).

DEF. A anello con unità, $S \subseteq A$ sottoinsiemi.
L'ideale generato da S è il più piccolo ideale di A che contiene S, e si denota con (S):

$$(S) = \bigcap_{\substack{I \subseteq A \text{ ideale} \\ I \supseteq S}} I$$

Prop. I, J ideali di un anello A. Allora l'intersezione I∩J è un'ideale.
In generale, l'intersezione di una famiglia qualsiasi di ideali è un ideale.

Def/Prop. Siano I,J ideali di un anello A. **L'ideale somma** I+J è per definizione il più piccolo ideale di A che contiene I∪J, cioè l'ideale generato da I∪J.
Inoltre:

$$I + J = \{i + j \mid i \in I, j \in J\}$$

Oss. Se A è commutativo, l'ideale somma di I=(x) e J=(y) è:

$$I + J = \{i + j \mid i \in I, j \in J\} = \{ax + by \mid a, b \in A\} = (\{x, y\})$$

4.4 Anello quoziente

A anello, $I \subseteq A$ ideale.
In particolare, $I \lhd (A, +)$, quindi possiamo definire:

- le classi laterali $I + a = \{i + a \mid i \in I\}$
- l'insieme quoziente A/I
- una struttura di gruppo abeliano su A/I tramite l'operazione:

$$(I + a) + (I + b) = I + (a + b)$$

- inoltre la proiezione:

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ a &\longrightarrow I + a \end{aligned}$$

  è un omomorfismo di gruppi, con nucleo $Ker(\pi) = I$.

Ora volgiamo dare all'insieme quoziente una struttura di anello. Definiamo quindi il prodotto di 2 classi laterali:

$$(I + a) \cdot (I + b) := I + a \cdot b$$

Prop. Nelle ipotesi precedenti, l'insieme quoziente A/I è un anello se dotato delle operazioni di somma e prodotto definite sopra, detto **anello quoziente di A modulo l'ideale I**.
La proiezione $\pi : A \to A/I$ è un morfismo di anelli.
Lo $0_{A/I}$ è la classe laterale di 0_A, cioè $0_{A/I} = I + 0_A = I$.
Se $\exists\ 1_A$, allora A/I è un anello unitario e $1_{A/I} = I + 1_A$.
Infine, se A è commutativo, anche A/I è commutativo.

Teorema fondamentale dei morfismi di anelli
Siano A e A' 2 anelli, e sia $\varphi : A \to A'$ un morfismo di anelli, con $I = Ker(\varphi)$.
Allora esiste un morfismo iniettivo $\overline{\varphi} : A/I \to A'$ che rende commutativo il seguente diagramma.

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\pi"'] & A' \\ A/I \arrow[ur, "\overline{\varphi}"] & \end{tikzcd}$$

cioè t.c. $\overline{\varphi} \circ \pi = \varphi$.
In particolare $Im(\varphi) \cong A/I$.

4.5 Ideali primi e ideali massimali

Sia A un anello commutativo con unità.

DEF.

i) Un ideale $M \subseteq A$ è detto **MASSIMALE** se non è contenuto in nessun ideale proprio di A. In altre parole, se $I \subseteq A$ è un ideale tale che:

$$M \subseteq I \subseteq A$$

allora o I=M, oppure I=A

ii) Un ideale $P \subseteq A$ è detto **PRIMO** se vale la seguente condizione:

$$\forall ab \in P \implies a \in P \text{ oppure } b \in P$$

Prop. Ogni ideale MASSIMALE è PRIMO.

Esempio Ideali primi e massimali in $\mathbb{Z}$ $\mathbb{Z}$ è un PID, dominio a ideali principali, quindi tutti i suoi ideali sono della forma $(n) = n\mathbb{Z}$
Poiché $(n) = (-n)$ possiamo guardare solo gli $n \geq 0$. $(0) = \{0\}$è un ideale primo, poiché $\mathbb{Z}$ è un dominio di integrità:
Siano $a, b \in \mathbb{Z}$ t.c. $ab \in (0)$
Cioè $ab = 0 \implies a = 0$ (cioè $a \in (0)$) oppure b=0 (cioè $b \in (0)$) Perché $\mathbb{Z}$ è un dominio di integrità.
Però (0) non è massimale ad esempio $(0) \subseteq (4) \subseteq \mathbb{Z}$

- (n), $n > 0$
- (n) è un ideale primo $\iff$ n è primo.

Ricordiamo:

$$\boxed{\text{n è primo} \iff [\text{se } n|ab \Rightarrow n|a \text{ oppure } n|b]}$$

Sia (n) con n primo, siano $a, b \in \mathbb{Z}$ tali che
$a \cdot b \in (n) = \{nz | z \in \mathbb{Z}\}$ Cioè tali che $n|ab \implies n|a$ (cioè $a \in (n)$) oppure $n|b$ (cioè $b \in (n)$)
Quindi (n) è primo.

Viceversa, mostriamo che se l'ideale (n) è primo, allora n è un numero primo.
Siano $a, b \in \mathbb{Z}$ tali che $n|ab$ allora $a, b \in (n) \implies a \in (n)$ (cioè $n|a$) oppure $b \in (n)$ (cioè $n|b$)
Conclusione:

$$\begin{aligned} &\text{in } \mathbb{Z} : (0) \text{ è primo ma non massimale} \\ &\quad (n) \text{ è primo} \iff \text{n è un numero primo} \end{aligned}$$

Tra poco vedremo che in $\mathbb{Z}$: primo $\iff$ massimale.

Oss. Se A è un PID, gli ideali primi $\neq (0) = \{0\}$ sono anche massimali.

Prop. A anello commutativo con unità. $I \subseteq A$ ideale proprio.

1. I è primo $\iff$ A/I è un dominio di integrità
2. I è massimale $\iff$ A/I è un campo

Oss.

1) Questo fornisce una seconda dimostrazione del fatto che massimale $\implies$ primo.
2) è un corollario quasi immediato il fatto che:
A dominio di integralità $\iff$ (0) è primo.

Capitolo 5

Polinomi

5.1 Anelli polinomiali

DEF. Sia A un anello commutativo con unità:

- Un polinomio a coefficienti in A in una indeterminata x è una scrittura formale:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_i x^i + \ldots = \sum_{i \in \mathbb{N}_0} a_i x^i$$

  con $a_i \in A$ tutti nulli tranne un numero finito.

- L'insieme di tutti i polinomi a coefficienti in A è denotato con $A[x]$.

- Il massimo intero n tale che $a_n \neq 0$ è detto grado di $p(x)$ e viene indicato con $deg(p(x))$; a_n viene detto **coefficiente direttivo**.
  (Usualmente si scrive $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ omettendo i termini successivi).

- Un polinomio **monico** se il suo coefficiente direttivo è 1.

- I polinomi costanti, cioè del tipo $p(x) = a_0$ hanno grado zero se $a_0 \neq 0$. Per convenzione il polinomio p(x)=0 ha grado $-\infty$.

Oss. Due polinomi $p(x) = \sum_{i=0}^{n} a_i x^i$ e $q(x) = \sum_{i=0}^{m} b_i x^i$ sono uguali se e solo se hanno gli stessi coefficienti, cioè se per ogni $i : a_i = b_i$

Oss. All'insieme A[x] possiamo dare una struttura di anello con le seguenti operazioni di somma e prodotto nel modo seguente:
dati $p(x) = \sum_{i=0}^{n} a_i x^i$ e $q(x) = \sum_{i=0}^{m} b_i x^i$ di gradi n ed m con $m \geq n$,

$$p(x) + q(x) = \sum_{i=0}^{m} (a_i + b_i) x^i$$

$$p(x) \cdot q(x) = \sum_{h=0}^{n+m} \left(\sum_{i+j=h} (a_i + b_j) x^h \right)$$

Osserviamo che per i gradi di somma e prodotto valgono le relazioni:

$$deg(p(x)+q(x)) \leq \max\{\deg(p(x)), \deg(q(x))\}$$

$$deg(p(x)\cdot q(x)) \leq \deg(p(x)) + \deg(q(x))$$

Nota: nel grado del prodotto si mette $\leq$ perché se è un anello polinomiale in "modulo" allora il termine con ordine massimo si può annullare.
Con tali operazioni, A[x] è un anello commutativo con unità.

Prop. A dominio di integrità $\implies A[x]$ dominio di integrità.

Corollario Se K campo, K[x] è un dominio di integrità.

Prop. Se k è un campo, gli elementi invertibili dell'anello k[x] sono le costanti non nulle.

5.2 Divisione tra polinomi

DEF. Sia A[x] anello di polinomi. Si dice che il polinomio g(x) divide il polinomio f(x) in A[x] (e si scrive $g(x)|f(x)$ o anche $g|f$) se esiste un polinomio $q(x) \in A[x]$ tale che:

$$f(x) = g(x) \cdot q(x)$$

TEOREMA Siano K campo, $g(x) \in k[x]$ un polinomio. Allora per ogni $f(x) \in k[x]$ esistono unici q(x) (quoziente) e r(x) (resto) elementi di K[x] tali che:

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

dove o $r(x) = 0$, oppure $\deg(r(x)) < \deg(g(x))$. Inoltre, q(x) ed r(x) sono univocamente determinati da queste condizioni.

Prop. K campo $\implies K[x]$ PID.

Oss. Il teorema è falso se k non è un campo.

DEF. Un dominio di integrità A si dice **dominio euclideo** se esiste una applicazione:

$$\delta : A\backslash\{0_A\} \to \mathbb{N}_0$$

(detta **valutazione euclidea** con la seguente proprietà:

i) $\forall a, b \in A$, con $b \neq 0_A$, $\exists\ q, r \in A$ t.c. $a = qb + r$

ii) o $r = 0_A$ oppure $\delta(r) < \delta(b)$

5.3 Polinomi irriducibili

DEF.

i) Due polinomi in A[x], A anello commutativo con 1_A, si dicono **associati** se differiscono per un fattore costante non nullo.
(e.g. $2x + 4$ e $x + 2$ sono associati)

ii) Un polinomio è detto **irriducibile** se i suoi divisori sono solo i polinomi costanti non nulli e i suoi polinomi associati (detti anche divisoti impropri).
(e.g. $2x + 4 = 2(x + 2)$)

Oss. Ricordiamo che $p \in \mathbb{Z}$ è primo se e solo se ha la proprietà:

$$p|ab \implies \text{o } p|a \text{ oppure } p|b$$

DEF. Dati $f(x),\ g(x) \in K[x]$ polinomi non nulli, si definisce massimo comune divisore di $f(x)$ e di $g(x)$ un polinomio $d(x) \in K[x]$ tale che:

- $d(x)|f(x)$ e $d(x)|g(x)$
- se $\exists\ \alpha(x) \in K[x]$ t.c. $\alpha(x)|f(x)$ e $\alpha(x)|g(x)$, allora $\alpha(x)|d(x)$

Oss. il MCD di 2 polinomi si può trovare con l'algoritmo euclideo, e vale la formula di Bezout: Se $f(x), g(x) \in K[x]$ non nulli, e $d(x) = \text{MCD}(f, g)$, allora $\exists\ \alpha(x),\ \beta(x) \in K[x]$ t.c.

$$d(x) = \alpha(x) \cdot f(x) + \beta(x) \cdot g(x)$$

$$t.f.a.e. \quad d = \alpha \cdot f + \beta \cdot g$$

Oss. Se $\text{MCD}(f, g) =$ costante, f e g si dicono polinomi coprimi.

Prop. Sia $f(x) \in K[x]$ un polinomio irriducibile, siano $a(x),\ b(x) \in K[x]$ tali che $f|ab$. Allora:

$$f(x)|a(x) \text{ oppure } f(x)|b(x)$$

Teorema di fattorizzazione unica
Ogni polinomio $f(x) \in K[x]$, K[x] campo, $\deg(f(x)) \geq 1$, si fattorizza in un prodotto di polinomi irriducibili. Tale fattorizzazione è unica nel senso che se

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_s(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_t(x)$$

Sono 2 diverse fattorizzazioni irriducibili, allora s=t ed esiste una corrispondenza biunivoca tra gli insiemi $\{p_i\}$ e $\{q_i\}$ tale che i polinomi corrispondenti sono associati.

Oss. Se K non è un campo, l'unicità non vale:

$$e.g. \text{ siamo in } \mathbb{Z}_{15}[x] : x^2 - \overline{1} = (x - \overline{1})(x - \overline{14}) = (x - \overline{4})(x - \overline{11})$$

DEF. Sia $f(x) \in A[x]$. Un elemento $a \in A$ si dice **radice** di f (o anche zero di f) se $f(a) = 0_A$, cioè se sostituendo l'elemento a all'incognita x si trova l'elemento 0_A.

Teorema di Ruffini
Sia $f(x) \in K[x]$. Un elemento $a \in A$ è radice di f se e solo se $(x-a)$ divide $f(x)$.

$$f(a) = 0 \iff (x-a)|f(x)$$

DEF. Una radice a di un polinomio $f(x) \in K[x]$ è detta **semplice** se

$$(x-a)|f(x) \ \text{ ma } \ (x-a)^2 \nmid f(x)$$

Si dice **molteplicità** della radice a il massimo intero **m** t.c. $(x-a)^m|f(x)$.
(radice semplice = molteplicità 1).

Prop. Un polinomio non nullo $f(x) \in K[x]$ di grado n ha al più n radici in K, contate con la loro molteplicità.

Oss. se K non è un campo, la proposizione è **falsa**:
e.g in $\mathbb{Z}_{15}[x]$ il polinomio $x^2 - 1$ ha 4 radici: $\overline{1}$, $-\overline{1} = \overline{14}$, $\overline{4}$, $-\overline{4} = \overline{11}$

Oss. Dato $f(x) \in K[x]$ posso costruire l'ideale principale $I = (f(x))$ e considerare il quoziente $\frac{K[x]}{(f(x))}$, cioè l'anello delle classi laterali modulo $(f(x))$.

Due polinomi $a(x)$ e $b(x)$ appartengono alla stessa classe laterale $\iff$ $a(x) - b(x)$ è un multiplo di $f(x)$.

DEF. In questo caso $a(x)$ e $b(x)$ si dicono congrui modulo $f(x)$

DEF. Siano $p(x) \in K[x]$ polinomio fissato, $I = (p(x))$ ideale principale. Due polinomi $a(x), b(x) \in K[x]$ si dicono **congrui modulo p(x)** se appartengono alla stessa classe laterale in $\frac{K[x]}{(p(x))}$.

Classe laterale di

$$\begin{aligned} a(x): \quad & a(x) + (p(x)) \\ & a(x) + I \end{aligned}$$

Oss. Ogni classe laterale può essere rappresentata in un unico da un polinomio di grado $<$ $\deg(p(x))$, che il resto della divisione per p(x) di un qualsiasi elemento della classe laterale.

Oss. $\mathbb{Z}$ PID $\implies$ gli ideali primi sono (0) e (p), p numero primo, è poiché in un PID gli ideali primi non nulli sono anche massimali, gli ideali max sono del tipo (p), p primo.

$$\mathbb{Z}_p \text{ campo} \iff (p) \iff p \text{ è primo}$$

TEOREMA Se $p(x) \in K[x]$ è irriducibile, allora il quoziete $\frac{K[x]}{(p(x))}$ è un campo.

(equivalentemente, (p) è massimale)

Prop. Siano $f(x) \in K[x]$ e $a, s \in K$. Allora $f(x)$ congruo ad a modulo ad a modulo il polinomio $x - s \iff f(s) = a$.

Oss. $\exists$ una versione del teorema cinese dei resti per la congruenza modulo un polinomio.

Oss. $f(x) \in K[x]$ polinomio di grado ≥ 2
Se $f(x)$ ammette radici in K $\implies f(x)$ non è irriducibile (è riducibile).
Quindi deg ≥ 2, irriducibile $\implies \nexists$ radici.

DEF. Un campo K e detto **algebricamente chiuso** se ogni polinomio di $K[x]$ di grado ≥ 1 ha almeno una radice in K.

Teorema fondamentale dell'algebra
I numeri complessi $\mathbb{C}$ sono un campo algebricamente chiuso.

Prop. I polinomi irriducibili di $\mathbb{C}[x]$ sono tutti e soli i polinomi di grado 1.

Prop. Ogni polinomio $f(x) \in \mathbb{C}[x]$ di grado deg ≥ 1.
Si decompone in $\mathbb{C}[x]$ come:

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

con $a_1,\ \alpha_i \in \mathbb{C}$.

Prop. Gli elementi riducibili di $\mathbb{R}[x]$ sono:

i) i polinomi di grado 1

ii) i polinomi $ax^2 + bx + c$ con $a \neq 0$ e $b^2 - 4ac < 0$.

Lemma Se $\alpha = a + ib$ è una radice complessa di un polinomio $f(x) \in \mathbb{R}[x]$, allora anche il suo coniugato $\overline{\alpha} = a - ib$ è radice di $f(x)$.

5.4 Polinomi irriducibili su $\mathbb{K}$

DEF. Sia $f(x) \in \mathbb{Z}[x]$, $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ polinomio non nullo.
$f(x)$ si dice **primitivo** se MCD($a_0, a_1, \ldots,\ a_n$)=1.

Oss. (Raccoglimento a fattore comune)
Un qualsiasi polinomio $g(x) = b_0 + b_1 x + \ldots + b_m x^m$ in $\mathbb{Z}[x]$, si può scrivere nella forma $g(x) = d \cdot g_0(x)$ dove: $d = MCD(b_0,\ b_1, \ldots,\ b_m)$ e $g_0(x)$ è un polinomio primitivo.

Prop. Sia $g(x) = \mathbb{Z}[x],\ g(x) \neq 0$. Allora la scrittura $g(x) = d \cdot g_0(x)$ con $d \in \mathbb{Z}$ e $g_0(x)$ primitivo è unica a meno di segno.

Prop. Sia $f(x) \in \mathbb{Q}[x],\ f(x) \neq 0$. Allora $f(x) = \gamma \cdot f_0(x)$ con $\gamma \in \mathbb{Q}$ e $f_0(x) \in \mathbb{Z}[x]$ primitivo.
Tale scrittura è unica a meno del segno.

DEF. La **riduzione modulo p** di un polinomio $f(x) \in \mathbb{Z}[x]$ è la sua immagine tramite il seguente omomorfismo di anelli:

$$\begin{aligned} \underline{Q}_p : \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_p[x] \\ f(x) &\longrightarrow \overline{f(x)} \end{aligned}$$

dove se $f(x) = a_0 + a_1x + \ldots + a_nx^n$, con $\overline{f(x)}$ denotiamo il polinomio:

$$\overline{f(x)} = \overline{a}_0 + \overline{a}_1x + \ldots + \overline{a}_nx^n$$

e $\overline{a}_i = [a_i]_p$

Lemma Di Gauss:
Il prodotto di polinomi primitivi è primitivo.

Prop. Sia $f(x) \in \mathbb{Q}[x], f \neq 0$ e fattorizziamo

$$f(x) = \gamma \cdot f_o(x)$$

con $\gamma \in \mathbb{Q}$ e $f_0(x) \in \mathbb{Z}[x]$ primitivo allora:

$$f(x) \text{ è irriducibile su } \mathbb{Q}\,(\text{in } \mathbb{Q}[x]) \iff f_0(x) \text{ è irriducibile su } \mathbb{Z}\,(\text{in } \mathbb{Z}[x])$$

Oss. Sia $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Q}[x]$
Sia $u \in Q, u = \frac{a}{b}$ con $a, b \in \mathbb{Z}, b \geq 1$ e $MCD(a, b) = 1$. Se u è una radice di $f(x)$ allora $a|a_0$ e $b|a_n$.
In particolare, se $f(x)$ è un polinomio monico a coefficienti interi, allora ogni sua radice razionale è un numero intero che divide il termine noto.

CRITERIO DI IRRIDUCIBILITÀ 1
Sia $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo, e sia p un primo che non divide il coefficiente direttivo di f(x).

$$f(x) = a_0 + a_1x + \ldots + a_nx^n, \quad p \nmid a_n$$

Sia $\overline{f(x)}$ la riduzione modulo p di $f(x)$. Se $\overline{f(x)}$ è irriducibile in $\mathbb{Z}_p[x]$, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ (e quindi anche in $\mathbb{Q}[x]$)

CRITERIO DI IRRIDUCIBILITÀ 2
Sia $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ in $\mathbb{Z}[x],\ n \geq 1,\ a_n \neq 0$, supponiamo che esista un primo p tale che:

i) $p \nmid a_n$

ii) $p|a_i$ per $i = 0, \ldots,\ n - 1$

iii) $p^2 \nmid a_0$

Allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$,e, se è primitivo, lo è anche in $\mathbb{Z}[x]$.

Oss. In generale char(A[x])=char(A) ma char($\frac{A}{I}$)≠char(A)

5.5 Estensione di campi

DEF. Siano E e F due campi. E si dice **ESTENSIONE** di F (e si scrive $E \mid F$) se esiste un omomorfismo iniettivo di campi $\varphi : F \hookrightarrow E$ (detto **immersione**).

Oss. $F \cong \varphi(F) \subseteq E$
(Nota: "$\cong$" significa isomorfo).

E.g. $\mathbb{R} \mid \mathbb{Q}$, $\mathbb{C} \mid \mathbb{R}$, $\mathbb{C} \mid \mathbb{Q}$

Prop. Sia $E \mid F$ un'estensione di campi. È possibile rendere in modo naturale E come uno spazio vettoriale su F (ovvero su $\varphi(F)$, con $\varphi : F \hookrightarrow E$ immersione).

DEF. Sia $E \mid F$ un'estensione di campi. La dimensione di E visto come spazio vettoriale su F è detta **grado dell'estensione**, e denota con **[E:F]**.

E.g. $[\mathbb{C} : \mathbb{R}] = 2$ ($\mathbb{C}$ spazio vettoriale su $\mathbb{R}$ con base $\{1, i\}$).

Oss. $[E : F] = 1 \implies E \cong F$

DEF. Siano $K \subseteq F$ due campi e sia $s \in F$. Definiamo **estensione semplice di K mediante s** il più piccolo sottocampo di F che contiene sia K che s. SI denota con "K(s)". Quindi:

$$K(s) = \bigcap_{\substack{L \subseteq F \text{ sottocampo} \\ K \cup \{s\} \subseteq L}} L$$

Oss. Se $s \in K \implies K(s) = K$.

Vogliamo descrivere queste estensioni semplici in maniera più esplicita:

Prop. Nelle notazioni precedenti, l'estensione semplice K(s) è data salle espressioni razionali fratte in s a coefficienti in K:

$$K(s) = \left\{ \frac{\alpha(s)}{\beta(s)} \;\middle|\; \begin{matrix} \alpha(s) = a_0 + a_1 s + \cdots + a_n s^n \\ \beta(s) = b_0 + b_1 s + \cdots + b_m s^m \end{matrix} \quad \text{con } a_i, b_j \in K,\ \beta(s) \neq 0 \right\}$$

Nota: $\frac{\alpha(s)}{\beta(s)}$ è il quoziente di combinazione lineari a coefficienti in K degli elementi $1, s, s^2, s^3, \ldots$ che si chiamano espressioni razionali intere.

Def/Prop. Nelle notazioni precedenti, l'insieme delle espressioni razionali intere, si denota con "K[s]", coincide con il più piccolo sottoanello di F che contiene K e s.

$$K \subseteq F \quad s \in F \backslash K$$

$$\text{espr. razionali intere, anello} \quad K[s] \subseteq K(s) \quad \text{espr. razionali fratte, campo}$$

DEF. Nelle notazioni precedenti, l'elemento s si dice **algebrico su K** se è radice di un polinomio non nullo a coefficienti in K. In caso contrario, si dice **trascendente su K**.

E.g.
$\sqrt{2}, \sqrt{3}$ sono algebrici in $\mathbb{Q}$
i è algebrico in $\mathbb{R}$
π è trascendente su $\mathbb{Q}$

Oss. Tutti gli elementi $t \in K$ sono algebrici su K, in quanto radici del polinomio di grado 1 $p(x) = x - t$.

Oss. s algebrico su K. L'insieme

$$I = \{f(x) \in K[x] \mid f(s) = 0\} \quad \text{L'insieme di tutti i polinomi che si annullano in s}$$

è un ideale di K[x].

- $f(x), g(x) \in I \implies f(x) - g(x) \in I$
- $f(x) \in I$, $p(x) \in K[x] \implies f(x) \cdot p(x) \in I$

DEF. Nelle notazioni precedenti, sia s algebrico su K. Allora:

$$I = \{f(x) \in K[x] \mid f(s) = 0\}$$

è un ideale in K[x] PID, quindi è della forma $I = (p(x))$. Il polinomio generatore p(x) è detto **polinomio minimo** di s su K.

Prop. Nelle ipotesi precedenti, p(x) è irriducibile su K.

Prop. Sia $F|K$ estensione finita (cioè $[F : K] = \dim_K(F) < \infty$).
Allora F è un'estensione algebrica, cioè tutti gli elementi di F sono algebrici su K.

TEOREMA Sia $F|K$ un'estensione di campi, e $s \in F$ un elemento.

i) L'elemento s è algebrico $\iff K[s] = K(s)$

ii) Se s è algebrico su K, ogni elemento di $K(s) = K[s]$ può essere scritto in modo unico come un'espressione razionale intera in s a coefficienti in K di grado inferiore al grado del polinomio minimo di s su K.

Corollario Sia $K \subseteq K(s) = K[s]$ un'estensione semplice con s algebrico. Sia $p(x)$ il polinomio minimo di s su K. Allora:

$$[K(s) : K] = \deg(p(x))$$

Oss.

K campo	s elemento algebrico
$p(x)$ polinomio minimo	$I = (p(x))$ ideale massimale

Allora $\frac{K[x]}{I}$ è un campo. Sia Φ_s un omomorfismo di anelli così definito:

$$\begin{aligned} \Phi_s : K[x] &\longrightarrow F \\ f(x) &\longrightarrow f(s) \end{aligned}$$

Allora sappiamo che:

$$\text{Im}(\Phi_s)\text{=K[s]}$$
$$\text{Ker}(\Phi_s)\text{=I}$$
$$\frac{K[x]}{I} = K[s]$$

5.6 Campi finiti

DEF. Se K è un campo finito, allora char(K)=p primo.
K contiene un sottocampo isomorfo a $\mathbb{Z}_p$:

$$\mathbb{Z}_p \hookrightarrow K : \quad K|\mathbb{Z}_p$$

Prop. Se K è un campo finito di caratteristica p e il grado dell'estensione $[K : \mathbb{Z}_p] = n$, allora K contiene p^n elementi.

Prop. Se K campo finito, char(K)=p, $[K : \mathbb{Z}_p] = n$, allora gli elementi di K sono tutte e sole le soluzioni dell'equazione a coefficienti in $\mathbb{Z}_p$:

$$x^{p^n} - x = 0$$

Prop. K campo finito. il gruppo moltiplicativo $G = K^* = K\backslash\{0\}$ è ciclico.

Lemma A gruppo commutativo. Se $a_1, a_2, \ldots, a_h \in A$ hanno ordine ord$(a_i) = m_i$, e se m=mcm$(m_1, \ldots, m_h)$, allora esiste un elemento $b \in A$ t.c. ord(b)=m.

Prop. In ogni campo finito K di caratteristica p esiste un automorfismo, detto **automorfismo di Frobenius**, definito da:

$$\begin{aligned} f : K &\longrightarrow K \\ a &\longrightarrow a^p \end{aligned}$$

Prop. Se K è un campo finito di caratteristica p, allora K è un'estensione semplice di $\mathbb{Z}_p$