Algebra 1

Contents

Part I
Aritmetica

Definizioni

Insiemi dei numeri $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Operazioni di somma $+\colon (a,b) \mapsto a+b$ **e prodotto** $\times\colon (a,b) \mapsto a \times b = a \cdot b = ab$ **e proprietà**

Somma: associatività, commutatività, elemento neutro, inverso additivo (opposto),
Prodotto: associatività, commutatività, elemento neutro, inverso (moltiplicativo),
distributività.

Principio di buon ordinamento

Divisibilità $a \mid b$ **e Insieme dei multipli** $a\mathbb{Z} \coloneqq \{an \colon n \in \mathbb{Z}\}$

Massimo comun divisore $\operatorname{mcd}(a,b) \coloneqq \begin{cases} \max D(a,b) & \text{se } (a,b) \neq (0,0) \\ 0 & \text{se } (a,b) = (0,0) \end{cases}$, $D(a,b) \coloneqq \{n \in \mathbb{Z} \colon n \mid a, n \mid b\}$

Numeri coprimi $\operatorname{mcd}(a,b) = 1$

Minimo comune multiplo $\operatorname{mcm}(a,b) \coloneqq \begin{cases} \min\{n > 0 \colon a \mid n, b \mid n\} & \text{se } a \neq 0 \text{ e } b \neq 0 \\ 0 & \text{se } a = 0 \text{ o } b = 0 \end{cases}$

Numero primo

Algoritmo di Euclide

Equazioni diofantee lineari $ax + by = c$

Soluzione particolare: (x_0, y_0) $\left(\text{per es. } \left(m\frac{c}{d}, n\frac{c}{d}\right)\right)$
Soluzione generica: $(x,y) = \left(x_0 + \frac{bk}{d}, y_0 - \frac{ak}{d}\right)$
con $d = \operatorname{mcd}(a,b) = am + bn$

Congruenze modulari $a \equiv b \mod n \iff n \mid (a-b)$**, Classi di congruenza** $\overline{a}$, $[a]$, $[a]_n = a + n\mathbb{Z}$ **e Insieme quoziente** $\mathbb{Z}/n\mathbb{Z}$

Soluzioni di congruenze polinomiali e Sistemi di congruenze

Teoremi

Divisione con resto

Dati $a, b \in \mathbb{Z}$ con $b \neq 0 \implies \exists!\, q, r \in \mathbb{Z}$ tali che $a = b \cdot q + r$ e $0 \leq r < |b|$

Dimostrazione Se vale per (a, b) vale anche per $(a, -b)$ dato che $a = b \cdot q + r \Rightarrow a = (-b) \cdot (-q) + r$, quindi WLOG $b > 0$.

- **Esistenza:** Sia $A = \{n \in \mathbb{N} \mid \exists\, c \in \mathbb{Z} \text{ tale che } n = a - bc\} \subseteq \mathbb{N}$, ho $A \neq \emptyset$ (prendo $c = -|a|$), A ha un minimo r (principio di buon ordinamento) e tale che $r = a - qb \geq 0$, se per assurdo $r \geq b$ ho $r - b \in A$, quindi $0 \leq r < b$
- **Unicità:** Se per assurdo esistessero (q, r) e (q', r') avrei $r - r' = (q - q')\, b$ e $b \mid (r - r') \Rightarrow |b| \leq |r - r'|$, ma $-b < -r' \leq r - r' \leq r < b$, ↯. Quindi $0 = r - r' = (q - q')\, b \implies q = q'$

Formula di Bezout

$\forall\, a, b \in \mathbb{Z} \implies a\mathbb{Z} + b\mathbb{Z} = \overbrace{\operatorname{mcd}(a, b)}^{d}\mathbb{Z}$, in particolare se $(a, b) \neq (0, 0)$, d è il minimo intero positivo che si può scrivere come $an + bm$ per $m, n \in \mathbb{Z}$.

Dimostrazione Sia $(a, b) \neq (0, 0)$ (per = banale), sia $d' = \min\{c \in a\mathbb{Z} + b\mathbb{Z} \mid c > 0\}$ che esiste perchè $|a| > 0$ oppure $|b| > 0$. Dimostro ora che $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

- $\subseteq$: ho che $an + bm = (kd)\, n + (ld)\, m = d\,(kn + lm) \in d\mathbb{Z}$
- $\supseteq$: basta dimostrare che $d \in a\mathbb{Z} + b\mathbb{Z}$, ma dimostro direttamente che $d' = d$:
  - Ho che $d \leq d'$, siccome $d \mid d'$ in quanto $d' \in a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$
  - Ho che $d' \mid c \quad \forall\, c \in a\mathbb{Z} + b\mathbb{Z}$, siccome preso $c = qd' + r$ con $0 \leq r < d'$ ho che

    $$r = c - qd' = am + bn - q\,(am' + bn') = a\,(m - qm') + b\,(n - qn') \in a\mathbb{Z} + b\mathbb{Z}$$

    ed essendo d' minimo positivo di $a\mathbb{Z} + b\mathbb{Z}$, ho che $r = 0$, da cui $d' \mid c$, dunque $d' \mid a$ e $d' \mid b$ e quindi $d \geq d'$

Corollario

$$\forall\, a, b \in \mathbb{Z}, \quad d = \operatorname{mcd}(a, b) \quad \iff \quad \begin{array}{ll} (1) & d \mid a \text{ e } d \mid b \\ (2) & \text{se } c \mid a \text{ e } c \mid b \text{ allora } c \mid d \end{array}$$

Minimo comune multiplo

$\forall\, a, b \in \mathbb{Z} \implies a\mathbb{Z} \cap b\mathbb{Z} = \overbrace{\operatorname{mcm}(a, b)}^{m}\mathbb{Z}$

Dimostrazione Per $a = 0 \vee b = 0$ banale. Altrimenti

- $\supseteq$: se $c \in m\mathbb{Z}$, allora $a \mid c$ (siccome $a \mid m$ e $m \mid c$), qundi $c \in a\mathbb{Z}$, analogamente per $b\mathbb{Z}$ e dunque $c \in a\mathbb{Z} \cap b\mathbb{Z}$.
- $\subseteq$: se $c \in a\mathbb{Z} \cap b\mathbb{Z}$ ho che $\exists\, q, r \in \mathbb{Z}$ tali che $c = m \cdot q + r$ con $0 \leq r < m$, da cui $a | r = c - m \cdot q$ (siccome $a|c$ e $a|m$), analogamente per b, quindi per forza $r = 0$ siccome m minimo comune multiplo e $r < 0$

Corollario

$$\forall\, a, b \in \mathbb{Z}, \quad m = \operatorname{mcm}(a, b) \quad \iff \quad \begin{array}{ll} (1) & a \mid m \text{ e } b \mid m \\ (2) & \text{se } a \mid c \text{ e } b \mid c \text{ allora } m \mid c \end{array}$$

Teorema fondamentale dell'aritmetica

$\forall\, n \in \mathbb{Z}, n > 1 \quad \exists\, p_1, ..., p_k$ primi: $n = \prod_i p_i$ e inoltre se $q_1, ..., q_l$ primi: $n = \prod_i q_i \implies \exists\, \sigma$ permutazione: $q_i \xrightarrow{\sigma} p_{\sigma(i)}$

Dimostrazione

- **Esistenza:** $X = \{n > 1 \mid n \text{ non è prodotto di primi}\}$, per assurdo $X \neq \emptyset$ e quindi ammette un minimo n. n non è primo, ma esistono $1 < a, b < n$ tali che $a \cdot b = n$, ma n è minimo, quindi $a, b \notin X$, e $a \cdot b$ si può scrivere come prodotto di primi, $\lightning$.
- **Unicità:** Analogamente a prima, prendo per assurdo il più piccolo $n = \prod_i p_i = \prod_i q_i$ con fattorizzazioni diverse, ho che $q_l \mid n = p_1 \cdot \ldots \cdot p_k \Rightarrow \exists\, i$ tale che $q_l \mid p_i$, ma p_i primo quindi $q_l = p_i$. Prendo $n' = \frac{n'}{p_k} = \frac{n'}{q_l}$, ma $n' < n$ non avrà fattorizzazioni distinte, $\lightning$.

Soluzioni di sistema di congruenze

$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$ ha soluzione se e solo se $\operatorname{mcd}(m,n) \mid (b-a)$ e la soluzione è unica modulo $\operatorname{mcm}(m,n)$

Lemma $s \equiv t \mod m, s \equiv t \mod n \iff s \equiv t \mod \operatorname{mcm}(m,n)$, in quanto $(s-t) \in m\mathbb{Z} \wedge (s-t) \in n\mathbb{Z} \iff (s-t) \in \operatorname{mcm}(m,n)\,\mathbb{Z}$

Dimostrazione x soluzione se e solo se $\exists\, y, z \colon x = a + my = b - nz \implies a - b = my + nz \implies \operatorname{mcd}(m,n) \mid (b-a)$, unicità dal lemma precedente in quanto presa una soluzione particolare x_0 il sistema equivale a $x \equiv x_0 \mod m, x \equiv x_0 \mod n$.

Corollario (Teorema Cinese del Resto)

Se $\operatorname{mcd}(m,n) = 1$, il sistema ha soluzione per ogni $a, b \in \mathbb{Z}$, e la soluzione è unica modulo mn. Equivalentemente $[x]_{mn} \mapsto ([x]_m, [x]_n)$ è biunivoca se $\operatorname{mcd}(m,n) = 1$.

Part II
Gruppi, Sottogruppi, Omomorfismi

Definizioni

Gruppo $(G, \circ, e)$, con composizione $\circ \colon G \times G \longrightarrow G$ ed elemento neutro $e \in G$

(G1)	(*Associatività*)	$x \circ (y \circ z) = (x \circ y) \circ z$	(G3)	(*Inverso*)	$x \circ x^* = x^* \circ x = e$
(G2)	(*Elemento Neutro*)	$x \circ e = e \circ x = x$	*(G4)	(*Commutatività*)	$x \circ y = y \circ x$

Gruppo abeliano o commutativo (con G4)

Gruppi additivi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, Gruppi moltiplicativi $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$

Quaternioni di Hamilton $(\mathbb{H}, +), (\mathbb{H}^*, \cdot)$ e sottogruppo $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Vierergruppe $V_4 = \{e, a, b, c\}$ di Klein

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Gruppi delle classi di resto $(\mathbb{Z}/n\mathbb{Z}, +)$, $\left((\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \operatorname{mcd}(a,n) = 1\}, \cdot\right)$ $(\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*)$

Gruppo delle biiezioni $(S(X), \circ)$**, Gruppo Simmetrico** S_n per $X = \{1, 2, \dots, n\}$

Gruppo ortogonale $(O_2(\mathbb{R}))$ Isometrie di $\mathbb{R}^2$ che fissano $\mathbf{0}$, tra cui rotazioni R_α e riflessioni S_l

Gruppo diedrale $D_n = \{A \in O_2(\mathbb{R}) : A \text{ manda l'}n\text{-agono } \Delta_n \text{ in sé}\} = \begin{cases} R^k & \text{rotazioni di } \alpha = \frac{2\pi k}{n} \\ S_k & \text{riflessioni} \end{cases}$, $\#D_n = 2n$

Sottogruppo $H < G$

Omomorfismo, Isomorfismo, Endomorfismo, Automorfismo $f(ab) = f(a) f(b)$

Kernel $\ker(f) \coloneqq \{a \in G \colon f(a) = e'\}$ **e Immagine** $f(G) \coloneqq \{f(a) : a \in G\}$

Prodotto interno di gruppi $G_1 \times G_2$ con composizione $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$

Teoremi

Unicità dell'elemento neutro

Unicità dell'inverso

Dimostrazione Siano x^*, x^{**} inversi di x, ho che

$$x^* = e \circ x^* = (x^{**} \circ x) \circ x^* = x^{**} \circ (x \circ x^*) = x^{**} \circ e = x^{**}$$

Inverso dell'inverso

Inverso del prodotto

Struttura del gruppo diedrale

Sia R la rotazione di centro $\mathbf{0}$ e angolo $\alpha = 2\pi/n$ e sia S la riflessione rispetto alla retta $y = 0$. Allora

(i) $\#D_n = 2n$

(ii) $A \in D_n \Rightarrow \exists!\, i < n \colon A = R^i \vee A = R^i S$

(iii) $SR = R^{-1}S \rightarrow \begin{matrix} (R^i S) R^j = R^{i-j} S \\ (R^i S)(R^j S) = R^{i-j} \end{matrix}$

(iv) $R^i S = S_i$ riflessione rispetto a retta di angolo $\pi i/n$

Dimostrazione

(i), (ii) [...]

Caratterizzazione del sottogruppo

G gruppo, $H \subseteq G$, sono equivalenti

(i) H sottogruppo

(ii) $H \neq \emptyset$ e $\begin{cases} \forall\, a, b \in H & ab \in H \\ \forall\, a \in H & a^{-1} \in H \end{cases}$

(iii) $H \neq \emptyset$ e $\forall\, a, b \in H \quad ab^{-1} \in H$

Dimostrazione

(iii) $\Rightarrow$ (i) [...]

Altre (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii)

Sottogruppi di $\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$

(1) I sottogruppi di $\mathbb{Z}$ sono $d\mathbb{Z}$ e sono diversi tra loro.
(2) I sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono $H_d = \{\overline{d}, \overline{2d}, \dots, \overline{n-d}, \overline{0}\}$ con d divisore positivo di n.

Dimostrazione .

1. Sia $H < G \implies 0 \in H$. Se non ci sono altri elementi $H = \{0\}$ ok, altrimenti esiste $a \in H \implies -a \in H$ (essendo H chiuso per l'operazione) quindi ci sono per forza elementi positivi. Sia $\underline{d := \min\{h \in H : h > 0\}}$.

$d\mathbb{Z} \subseteq H$: poiché H sottogruppo $\implies$ ogni multiplo di d è in H (chiusura per addizione)

$d\mathbb{Z} \supseteq H$: ovvero ogni elemento $a \in H$ è divisibile (multiplo) di d. Facciamo **divisione con resto** e vediamo che $r = 0$: $a = qd + r \in H \quad \text{con } 0 \leq r < d \implies r = a - qd \in H$ ma d è definito come il minimo positivo in H e r è definito come $0 \leq r < d \implies r = 0$

I sottogruppi $d\mathbb{Z}$ sono diversi perché caratterizzati da d, che è il loro minimo intero positivo (ciò li distingue).

2. Sia $H < \mathbb{Z}/n\mathbb{Z}$. Definiamo $H' = \{a \in \mathbb{Z} : \overline{a} \in H\}$

$$\begin{aligned} \underbrace{\overline{0} \in H}_{\text{H sottogr.}} &\implies 0 \in H' \\ \overline{a}, \overline{b} \in H &\impliedby a, b \in H' \\ \underbrace{\overline{a-b} \in H}_{\text{H sottogr.}} &\implies a - b \in H' \qquad \implies H' < \mathbb{Z} \\ \overline{0} = \overline{n} \in H &\implies n \in H' \qquad \implies H' \neq \{0\} \end{aligned}$$

Quindi per (1) $H' = d\mathbb{Z}$. Inoltre $n \in H' \implies d | n$. Verificare che i gruppi H_d sono distinti.

Immagine dell'elemento neutro e dell'inverso attraverso un omomorfismo

(i) $f(e) = e'$ (ii) $f\left(a^{-1}\right) = f(a)^{-1}$

Dimostrazione

(i) Abbiamo che $f(e) = f(e \cdot e) = f(e) \cdot f(e)$

$$e' = f(e)^{-1} f(e) = f(e)^{-1} (f(e) f(e)) = \left(f(e)^{-1} f(e)\right) f(e) = e' f(e) = f(e)$$

(ii) Dalla parte (i) e dall'unicità dell'inverso

$$f\left(a^{-1}\right) f(a) = f\left(a^{-1} a\right) = f(e) = e'$$

Sottogruppi Kernel e Immagine

(i) $\ker(f)$ sottogruppo di G (ii) $f(G)$ sottogruppo di G (iii) f iniettiva $\iff \ker(G) = \{e\}$

Dimostrazione [...]

Composizione e Inverso di Isomorfismi

(i) f, g isomorfismi $\implies f \circ g$ isomorfismo (ii) f isomorfismo $\implies f^{-1}$ isomorfismo

Dimostrazione

(ii) Devo dimostrare che è omomorfismo

$$f\left(f^{-1}(ab)\right) = ab = f\left(f^{-1}(a)\right) f\left(f^{-1}(b)\right) = f\left(f^{-1}(a) f^{-1}(b)\right) \overset{\text{per iniettività di } f}{\longrightarrow} f^{-1}(ab) = f^{-1}(a) f^{-1}(b)$$

Teorema Cinese del Resto

$f(a \mod nm) = (a \mod n, a \mod m)$ con $\text{mcd}(n, m) = 1$ è un isomorfismo, ovvero

$$\boxed{\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}} \quad \text{se } n, m \text{ coprimi}$$

dove $\oplus$ è il prodotto cartesiano tra gruppi in cui l'operazione è il $+$ (indica che è abeliano))

Dimostrazione f è ben definita in quanto lo sono le due proiezioni (siccome $n \mid nm$ e $m \mid nm$), ed è un omomorfismo.

- **Iniettività**: Prendo $a \in \ker(f)$, ho che $a \equiv 0 \mod n$ e quindi $a = un$ (analogamente $a = vm$). In quanto m e n coprimi posso scrivere $1 = nx + my$ e quindi

$$a = a(nx + my) = anx + amy = (vm)nx + (un)my = (vx + uy)mn$$

  Da cui $mn \mid a \implies a \equiv 0 \mod mn$, e dunque f iniettivo.

- **Suriettività**: da $\#\mathbb{Z}/nm\mathbb{Z} = \#(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$

Part III
Permutazioni

Definizioni

Cicli $\sigma = (a_1\, a_2\, \dots\, a_k) \quad \sigma(a_i) = a_{i+1},\ \sigma(a_k) = a_1,\ \sigma(x) = x$ altrimenti

Cicli disgiunti $(a_1\, a_2\, \dots\, a_s), (b_1\, b_2\, \dots\, b_t)$ con $a_i \neq b_j$

Segno $\varepsilon(\sigma)$ Sia:

$$\Omega \coloneqq \{h : \mathbb{Z}^n \to \mathbb{Z}\} = \{\text{funzioni } h(X_1, \dots, X_n) \text{ di } n \text{ variabili intere}\}$$

Per $h \in \Omega$ e $\sigma \in S_n$ definiamo $\sigma(h) \in \Omega$:

$$(\sigma(h))(X_1, \dots, X_n) \coloneqq h(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

Usiamo la funzione $D \in \Omega$:

$$D(X_1, \dots, X_n) \coloneqq \prod_{1 \leq i < j \leq n} (X_i - X_j)$$
$$\sigma(D) = \pm D \coloneqq \varepsilon(\sigma) D \implies \varepsilon(\sigma) = \pm 1$$

In sostanza definiamo il segno di una permutazione (ovvero se il numero di trasposizioni, congiunte e disgiunte ma diverse, di cui è composta è in numero pari o dispari) attraverso sta funzione $D : \mathbb{Z}^n \to \mathbb{Z}$ che piglia gli n elementi $X_1, \dots, X_n$ e ci fa il prodotto delle differenze di tutte le coppie possibili a meno del segno come definito sopra. Quindi σ che agisce su tale D effettivamente per ogni trasposizione che fa ne cambia il segno, quindi per un numero pari avremo segno positivo perché si annullano, per un numero dispari rimarrà il meno.

Gruppo alterno $A_n \coloneqq \{\sigma \in S_n : \varepsilon(\sigma) = 1\}$

Teoremi

Scomponibilità di una permutazione in cicli disgiunti

Dimostrazione Per induzione, se $\sigma = (1)$ la tesi è dimostrata. Altrimenti, preso $x \in \{1, \dots, n\}$ consideriamo $Y \coloneqq \{x, \sigma(x), \sigma^2(x), \dots\}$ (che sarà finito), con k intero minimo per cui $x = \sigma^k(x)$, da cui $Y = \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$. Osserviamo che $\sigma(Y^C) = Y^C$, e dunque presa la restrizione $\sigma|_{Y^C}$ questa è prodotto di cicli disgiunti per ipotesi induttiva.

Segno del prodotto di permutazioni

$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)$, ovvero la funzione ε è un omomorfismo

Dimostrazione

$$\varepsilon(\sigma\tau)\,D = (\sigma\tau)(D) = \sigma(\tau(D)) = \sigma(\varepsilon(\tau)\,D) = \varepsilon(\tau)\,\sigma(D) = \varepsilon(\tau)\,\varepsilon(\sigma)\,D$$

Segno di trasposizioni, k-cicli e permutazioni

(i) Dato un k-ciclo ho che $(a_1\,a_2\,\ldots\,a_k) = (a_1\,a_2)(a_2\,a_3)\ldots(a_{k-1}\,a_k)$

(ii) $\forall\,\tau$ trasposizione $\rightarrow\ \varepsilon(\tau) = -1$, e dunque dato un k-ciclo τ ho che $\varepsilon(\tau) = (-1)^{k-1}$

(iii) Per una permutazione σ prodotto di k trasposizioni ho che $\varepsilon(\sigma) = (-1)^k$

Dimostrazione

(i) Verifica di $\sigma(a_i) = a_{i+1}$, $\sigma(a_k) = a_1$ e $\sigma(x) = x$ per $x \notin \{a_1, a_2, \ldots, a_k\}$

(ii) Per le trasposizioni $\tau = (a\,a+1)$ ovviamente $\varepsilon(\tau) = -1$, le per quelle generiche posso scrivere $(a\,b) = (b\,a+1)(a\,a+1)(b\,a+1)$, e avrà dunque segno $\varepsilon((a\,b)) = \varepsilon((b\,a+1))^2\,\varepsilon((a\,a+1)) = -1$.

Scomponibilità di una permutazione pari in 3-cicli

Dimostrazione Ogni permutazione pari è prodotto di un numero pari di trasposizioni. Basta dimostrare che il prodotto di due trasposizioni diverse è scomponibile in 3-cicli

$(a\,b)(b\,c) = (a\,b\,c)$ (trasposizioni non disgiunte) $\qquad (a\,b)(c\,d) = (c\,a\,d)(a\,b\,c)$ (trasposizioni disgiunte)

Teorema di Cayley

Ogni gruppo finito G è isomorfo a un sottogruppo di S_n per un certo intero positivo n.

Dimostrazione Devo costruire un isomorfismo tra G e un sotto gruppo di S_n

- Definisco
$$T_g : G \to G \quad h \mapsto gh$$
Verifico che essa è una **biezione**, ovvero una permutazione degli elementi di G, ovvero $T_g \in S(G)$.
Iniettiva:
$$h, h' \in G.\quad T_g(h) = T_g(h') \implies gh = gh' \implies h = h'$$
in quanto in un gruppo vale la legge di cancellazione.
Suriettiva:
$$\forall y \in G: \quad y = y(g^{-1}g) = (yg^{-1})g = T_g(yg^{-1})$$
Quidni T_g copre tutto G.

- Definisco
$$I : G \to S(G) \cong S_n \qquad I(g) = T_g \qquad n = \#G$$
(ovvero assegno ad ogni elemento la permutazione che esso fa su tutto G se moltiplicato per i suoi elementi).
Verifico che è un **omomorfismo iniettivo**.
Omomorfismo:
$$I(gg')(h) = T_{gg'}(h) = gg'h = T_g(g'h) = T_g(T_{g'}(h)) = I(g)(I(g')(h)) = (I(g) \circ I(g'))(h)$$
Iniettivo: $g \in \ker(I) \ \Rightarrow\ I(g) = \mathrm{Id}_G \ \Rightarrow\ g = e$.
Quindi (essendo omomorfismo) l'immagine $I(G) < S(G) \cong S_n$ e, essendo I iniettiva, la restrizione $I' : G \to I(G)$ è isomorfismo tra G e un sottogruppo di S_n.

Sostanzialmente vedo gli elementi di un gruppo come le permutazioni che ognuno fa sugli elementi del gruppo stesso tramite $g \mapsto xg$. Quindi effettivamente un gruppo finito è l'insieme di **alcune** permutazioni sui suoi oggetti definite proprio dai suoi stessi elementi. Peccato che è altamente inefficiente vedere un gruppo in tal modo poiché $\#G = n$ è molto minore di $\#S_n = n!$, ovvero le permutazioni degli n elementi rappresentate dagli elementi di G sono **molto meno** rispetto a tutte le possibili.
Teorema di Cayley generalizzato a p. 77 dell'Hernstein

Part IV
Generatori, Ordine, Indice, Coniugato e Centralizzante

Definizioni

Sottogruppo $\langle X \rangle$ generato da $X \subseteq G$, e Generatore X di un gruppo $G = \langle X \rangle$

Gruppo ciclico $G = \langle x \rangle$

Ordine di un gruppo $\#G$, ordine di un elemento $\operatorname{ord}(x) \coloneqq \min\{m > 0 \colon x^m = e\}$

Classi lateriali sinistre gH e destre Hg e Insieme delle classi laterali sinistre G/H e destre H/G
Dato $H \subseteq G$ sottogruppo, $gH \coloneqq \{gh \colon h \in H\}$ e $Hg \coloneqq \{hg \colon h \in H\}$

Indice $[G : H]$, Sistema di rappresentanti S $G = \bigcup_{s \in S} sH, \quad [G : H] = \#S$

Coniugato $b = c^{-1}ac$, Coniugio $a \sim b$, Classe di coniugio $\operatorname{Cl}(a) \coloneqq \{b \in G \colon b \sim a\}$

Sottogruppo del Centro $Z(G) = \{g \in G \colon gh = hg \quad \forall\, h \in G\}$ sottoinsieme di G che commuta con tutto G

Sottogruppo del Centralizzante $C(a) = \{g \in G \colon ga = ag\}$ sottoinsieme di G che commuta con $a \in G$
Vale che $Z(G) = \bigcap_{g \in G} C(g)$

Teoremi

Isomorfismo dei gruppi ciclici

Se $\operatorname{ord}(x) = \begin{cases} \infty & \text{allora } \langle x \rangle \cong \mathbb{Z} \quad \text{(i)} \\ m & \text{allora } \langle x \rangle \cong \mathbb{Z}/m\mathbb{Z} \quad \text{(ii)} \end{cases}$. Quindi se G ciclico allora $G \cong \mathbb{Z}$ oppure $G \cong \mathbb{Z}/m\mathbb{Z}$

Dimostrazione

(i) Considero $f \colon \mathbb{Z} \longrightarrow G$ tale che $f(n) = x^n$, è ovviamente un omomorfismo ed è iniettiva in quanto $x^m = 1$ vale solo per $m = 0$, quindi è un isomorfismo

(ii) Considero $f \colon \mathbb{Z}/m\mathbb{Z} \to G$ tale che $f(\overline{a}) = x^a$, è ben definita, è un omomorfismo suriettivo, ed è iniettiva in quanto $x^m = 1$ vale solo per $\overline{m} = \overline{0}$, quindi è un isomorfismo

Corollario

$\operatorname{ord}(x) = \#\langle x \rangle$

Proprietà delle classi laterali sinistre

Dati a, b valgono

(i) $aH = bH \Leftrightarrow a^{-1}b \in H$ (ii) $aH = bH \vee aH \cap bH = \emptyset$ (iii) $\forall x \in G\, \exists a \in G \colon x \in aH$

Dimostrazione

(i) $\Rightarrow$: ho che $ah = be$ per un certo $h \in H$, da cui $a^{-1}b = h \in H$.
$\Leftarrow$: ho che $a^{-1}b = h \in H$, ovvero $b = ah, a = bh^{-1}$, quindi $x \in aH \Rightarrow x = ah_1 = bh^{-1}h_1 \in bH$ e viceversa

(ii) Se $z \in aH \cap bH \neq \emptyset$ ho che $z = ah_1 = bh_2$ da cui $a^{-1}b = h_1h_2^{-1} \in H$ in quanto H gruppo, la tesi segue da (i)

(iii) $x = xe \in xH$

Cardinalità delle classi laterali sinistre

Dato $H \subseteq G$ sottogruppo, $f \colon H \to aH$ tale che $f(h) = ah$ è una biiezione (ma non un omomorfismo), e quindi $\#H = \#aH$

Teorema di Lagrange

Dato G gruppo e $H \subseteq G$ sottogruppo, $\#G = \#H \cdot [G : H]$

Dimostrazione Data S sistema di rappresentanti, siccome $\#H = \#sH$ ho che $\#G = \sum_{s \in S} \#(sH) = \#S \cdot \#H = \#H \cdot [G : H]$

Corollario

Dato G gruppo finito

(i) Se H sottogruppo di G, allora $\#H \mid \#G$

(ii) Se $x \in G$, allora $\operatorname{ord}(x) \mid \#G$

(iii) Sia G' gruppo e sia $f \colon G \longrightarrow G'$ omomorfismo, allora $\#\ker(f) \mid \#G$ e, se il gruppo G' è finito, $\#f(G) \mid \#G'$.

Corollario

Dato p primo e G gruppo di ordine p ho che $G \cong \mathbb{Z}/p\mathbb{Z}$

Dimostrazione Prendo $x \neq e$ in G, ho che $\operatorname{ord}(x) \mid \#G$ e dunque $\operatorname{ord}(x) = p$, ma quindi G gruppo ciclico di ordine p, quindi la tesi

Teorema di Fermat

p primo e $x \in \mathbb{Z}$ tale che $p \nmid x$, allora $x^{p-1} \equiv 1 \mod p$

Dimostrazione Siccome $p \nmid x$, la classe $\overline{x}$ è in $(\mathbb{Z}/p\mathbb{Z})^*$, ma dunque $\operatorname{ord}(x) \mid \#(\mathbb{Z}/p\mathbb{Z})^* = p - 1$

Teorema di Eulero

n intero positivo e $x \in \mathbb{Z}$ tale che $\operatorname{mcd}(x, n) = 1$, allora $x^{\varphi(n)} \equiv 1 \mod n$

Dimostrazione Analogamente a prima, ma con $\#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$

Numero di elementi coniugati ad a

$c_a = \#\mathrm{Cl}(a) = \#G/\#C(a) = [G : C(a)]$

Dimostrazione Ho una corrispondenza biunivoca tra gli elementi di $\mathrm{Cl}(a)$ e le classi laterali destre di $C(a)$ siccome x, y nella stessa classe implica $y = cx$ con $c \in C(a)$, da cui

$$y^{-1}ay = \left(x^{-1}c^{-1}\right) a\,(cx) = x^{-1}\left(c^{-1}ac\right) x = x^{-1}\left(c^{-1}ca\right) x = x^{-1}ax$$

L'implicazione inversa procedendo in senso opposto

Corollario (Equazione delle classi)

$\#G = \sum \frac{\#G}{\#C(a)}$, sommatoria su un a per ogni classe di coniugio

Centro di un gruppo di ordine p^n

Se $\#G = p^n$ con p primo, allora $Z(G) \neq \{e\}$

Dimostrazione [...]

Corollario

Se $\#G = p^2$ con p primo, allora G è abeliano

Part V
Sottogruppi normali e Gruppi quoziente

Definizioni

Elemento coniugato Il coniugato di $h \in G$ da $g \in G$ è ${}^g h \coloneqq ghg^{-1}$

Sottogruppo coniugato Il coniugato di $H < G$ è l'inisieme degli elementi coniugati degli elementi di H, ovvero ${}^g H = \{ghg^{-1} :\ h \in H\} = gHg^{-1}$. È sempre un sottogruppo.

Sottogruppo normale $H \lhd G$ sottogruppo tale che $ghg^{-1} \in H \quad \forall\, h \in H, g \in G$. Tre definizioni equivalenti (dim. sotto):

- $gH = Hg\ \forall g \in G$ (classi destre sono uguali alle sinistre)
- $gHg^{-1} = H\ \forall g \in G$ (H coincide cin il suo coniugato)
- $ghg^{-1} \in H\ \forall h \in H, g \in G$ (H chiuso rispetto alla coniugazione)

Gruppo quoziente $G/N \coloneqq \{gN \colon g \in G\}$ Elementi $\overline{g} = gN = Ng$, $\overline{a} = \overline{b} \iff a^{-1}b \in N$, composizione $\overline{a} \cdot \overline{b} = \overline{ab}$

Applicazione canonica $\pi \colon G \longrightarrow G/N, \quad \pi(g) = \overline{g}$

Commutatori The commutator gives an indication of the extent to which a certain binary operation fails to be commutative.
In gruppi: $[a, b] \coloneqq aba^{-1}b^{-1}$, ovvero $ab = [a, b]ba$. Quindi $[a, b] = 1 \iff ab = ba$, ovvero se commutano.
In anelli: $[a, b] = ab - ba$, discorso analogo a sopra.

Sottogruppo generato dai commutatori $[G,G] := < C >$ con $C = \{[g,h] : g,h \in G\} = \{ghg^{-1}h^{-1} : g,h \in G\}$. È sottogruppo normale

Teoremi

Caratterizzazione dei sottogruppi normali

Dato $H \subseteq G$ sottogruppo, sono equivalenti

(i) H sottogruppo normale di G (ii) $gH = Hg \quad \forall g \in G$ (iii) $gHg^{-1} = H \quad \forall g \in G$

Dimostrazione

(i) $\Rightarrow$ (ii) Prendo $x = gh \in gH$, quindi $x = gh = \left(ghg^{-1}\right) g = h'g \in Hg$, da cui $gH \subseteq Hg$, analogo l'inverso

(ii) $\Rightarrow$ (i) Presi $h \in H$ e $g \in G$ ho che $gh \in gH = Hg$, quindi $gh = h'g \;\Rightarrow\; h' = ghg^{-1} \in H$

(ii) $\Leftrightarrow$ (iii) Preso $g \in G$ vale che

$$\overbrace{\{gh \colon h \in H\}}^{gH} = \overbrace{\{hg \colon h \in H\}}^{Hg} \iff \overbrace{\left\{ghg^{-1} \colon h \in H\right\}}^{gHg^{-1}} = \overbrace{\{h \colon h \in H\}}^{H}$$

Insieme delle classi è gruppo solo se H è normale

$H \lhd G \implies G/H = \{$insieme delle classi laterali sinistre di $H\}$ è un gruppo con l'operazione definita da

$$\overline{a} \cdot \overline{b} = \overline{ab} \qquad \text{ovvero} \qquad aH \cdot bH = abH$$

Dimostrazione Due passi:

- L'operazione è ben definita: se $a_1H = a_2H$ e $b_1H = b_2H$ allora

$$a_1H \cdot b_1H = a_1b_1H = a_1(b_2H) \overset{\star}{=} (a_1H)b_2 = (a_2H)b_2 \overset{\star}{=} a_2b_2H = a_1H \cdot a_2H$$

  in $\star$ abbiamo usato l'ipotesi che H è normale, ovvero le classi laterali commutano.

- G/H verifica le proprietà di gruppo (identità con $e = eH = H$, chiusura e inverso)

Normalità dei sottogruppi di indice 2

$H \subseteq G$ sottogruppo di indice $[G : H] = 2 \implies H$ sottogruppo normale

Dimostrazione Una delle due classi laterali sinistre sarà H, e l'altra di conseguenza $G - H$. Analogamente per le classi destre, da cui le uguaglianze

$$gH = Hg = H \quad \text{per } g \in H \qquad\qquad gH = Hg = G - H \quad \text{per } g \notin H$$

Normalità del ker di una funzione

$f \colon G \longrightarrow G'$ omomorfismo, allora $\ker(f)$ sottogruppo normale di G

Dimostrazione Dato $h \in \ker(f)$ ho che $f\left(ghg^{-1}\right) = f(g)\, f(h)\, f\left(g^{-1}\right) = f(g)\, f\left(g^{-1}\right) = e'$, da cui $ghg^{-1} \in \ker(f)$

Buona definizione della composizione nel gruppo quoziente

Dimostrazione Dati $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$ ho che $a' = an_1$ e $b' = bn_2$, da cui $a'b' = an_1bn_2 = ab\left(b^{-1}n_1b\right)n_2$ e quindi $\overline{a'b'} = \overline{ab}$

Commutatività del gruppo quoziente

N sottogruppo normale di G. Allora G/N commutativo $\iff [G,G] \subseteq N$

Dimostrazione

G/N commutativo $\Leftrightarrow \forall \overline{g}, \overline{h} \in G/N \quad \overline{g} \cdot \overline{h} = \overline{h} \cdot \overline{g} \Leftrightarrow \overline{ghg^{-1}h^{-1}} = \overline{e} \Leftrightarrow ghg^{-1}h^{-1} \in N \Leftrightarrow [G, G] \subseteq N$

Part VI
Teoremi di Isomorfismo

Teoremi

Teorema di omomorfismo

$f\colon G \longrightarrow G'$ omomorfismo, $N \subseteq G$ sottogruppo normale con $N \subseteq \ker(f)$, allora, $\exists!\, h\colon G/N \longrightarrow G'$ tale che $h \circ \pi = f$, ovvero $h(\underbrace{xN}_{\text{classe di } x}) = f(x)$. Alternativamente, il diagramma è commutativo (π applicazione canonica).

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\searrow & & \nearrow{\scriptstyle h} \\ & G/N & \end{array}$$

Dimostrazione Definisco $h(\overline{x}) = f(x)$, ben definita in quanto

$\overline{x} = \overline{y} \longrightarrow x^{-1}y \in N$, dunque $f(x^{-1}y) = e' = f(x)^{-1}f(y) \iff f(x) = f(y) \longrightarrow h(\overline{x}) = f(x) = f(y) = h(\overline{y})$

Ed omomorfismo in quanto $h(\overline{xy}) = f(xy) = f(x)\, f(y) = h(\overline{x})\, h(\overline{y})$

Primo teorema di isomorfismo

$f\colon G \longrightarrow G'$ omomorfismo, allora $G/\ker(f) \cong \mathrm{Im} f$

Dimostrazione Devo trovare un **omomorfismo iniettivo**

$$G/\ker f \to G$$

in modo che poi la restrizione all'immagine sia anche suriettiva e quindi isomorfismo. Vediamo che

$$\begin{cases} h : G/N \to G, \quad h(\overline{x}) = f(x) \quad \text{dal teo omo.} \\ N = \ker f \end{cases}$$

soddisfa la richiesta.

- f **e** h **hanno stessa immagine**: Vediamo dalla def. di h che $h(x\ker(f)) = f(x)$, quindi l'immagine di h è uguale all'immagine di f (poiché anche $f(x \cdot k) = f(x)f(k) = f(x)$ con $k \in \ker f$)
- h **iniettiva**:

  $$\overline{x} \in \ker(h) \implies h(\overline{x}) = f(x) = e' \implies x \in \ker(f) \implies \overline{x} = \overline{1}$$

  dove $\overline{1}$ è l'elemento neutro di $G/\ker(f)$. Allora è iniettiva

Quindi h isomorfismo sull'immagine.

Corollario

Se f omomorfismo suriettivo, allora $G/\ker(f) \cong G'$

Corollario

Se $G' = A$ abeliano, allora, $\exists!\, f\colon G/[G,G] \longrightarrow A$ tale che $h(x[G,G]) = f(x)$.

Dimostrazione Siccome $G/\ker(f) \cong f(G)$ è un sottogruppo di A, è abeliano, e quindi $[G,G] \subseteq \ker(f)$

Secondo teorema di isomorfismo

$H \subseteq G$ sottogruppo, $N \subseteq G$ sottogruppo normale, $HN \coloneqq \{hn\colon h \in H, n \in N\}$, allora:

(i) $H \cap N$ sottogruppo normale di H (ii) $\begin{matrix} HN & \text{sottogruppo di} & G \\ N & \text{sottogr. normale di} & HN \end{matrix}$ (iii) $H/(H \cap N) \cong HN/N$

Dimostrazione

(i) $n \in H \cap N, g \in H$, ho che $gng^{-1} \in H$ in quanto H gruppo, e $gng^{-1} \in N$ in quanto N normale.

(ii) Di certo $e = e \cdot e \in HN$. Prendo $a = h_1 n_1$ e $b = h_2 n_2$, ho che

$$ab^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = \overbrace{h_1 h_2^{-1}}^{h'} \overbrace{h_2 n_1 n_2^{-1} h_2^{-1}}^{n',\, N \text{ normale}} = h'n' \in HN$$

quindi HN sottogruppo di G. N sottogruppo normale di HN in quanto N sottogruppo normale di $G \supseteq HN$

(iii) Prendo $f\colon H \longrightarrow HN/N$ tale che $f(h) = hN$, omomorf. suriett. di $\ker(f) = \{h \in H\colon hN = N\} = H \cap N$

Terzo teorema di isomorfismo

N, N' sottogruppi normali di G tali che $N \subseteq N' \subseteq G$, allora N'/N sottogruppo normale di G/N, ogni sottogruppo normale di G/N ha la forma M/N con $N \subseteq M \subseteq G$, e inoltre $(G/N)/(N'/N) \cong G/N'$

Dimostrazione [...]
Data l'applicazione canonica $\pi\colon G \longrightarrow G/N'$, trovo per il teorema di omomorfismo $h\colon G/N \longrightarrow G/N'$ tale che $h(gN) = \pi(g) = gN'$, suriettiva dato che lo è π. Adesso, so che $gN \in \ker(h) \Leftrightarrow gN' = N'$, ovvero $g \in N'$, da cui

$$\ker(h) = \{gN\colon g \in N'\} = N'/N \qquad \longrightarrow \qquad G/N' \cong (G/N)/\ker(h) = (G/N)/(N'/N)$$

Part VII
Anelli

Definizioni

Anello $(R, +, \cdot, 0, 1)$, con addizione $+$, moltiplicazione $\cdot$, ed elementi $0, 1$

(R1)	(*Gruppo additivo*)	$(R, +, 0)$ gruppo abeliano	(R4)	(*Distributività*)	$x \cdot (y+z) = x \cdot y + x \cdot z$ $(y+z) \cdot x = y \cdot x + z \cdot x$
(R2)	(*Associatività*)	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	*(R5)	(*Commutatività*)	$x \cdot y = y \cdot x$
(R3)	(*Identità*)	$1 \cdot x = x \cdot 1 = x$	*(R6)	(*Inverso moltipl.*)	$x \cdot x^* = x^* \cdot x = 1$ $(x \neq 0)$

Anello commutativo (R5), Anello con divisione (R6), Campo o Corpo (R5 e R6)

Anelli $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ commutativi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, con divisione $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$, campi $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Anello banale È l'insieme $\{0\}$ in cui 0=1: i due elementi neutri coincidono. Si può anche dare come caratteristica unica il fatto che gli elementi neutri coincidono e ricavare che è solo l'insieme $\{0\}$, infatti:

$$0 = 1 \implies x = 1 \cdot x = 0 \cdot x = 0 \quad \forall x$$

la prima uguaglianza per def. di elem. neutro prodotto, nella seconda perché 1=0, nella terza perché in un anello valgono

$$\begin{cases} x + 0 = x & \text{(def. elem. neutro somma)} \\ x(y+z) = xy + zy & \text{(proprietà distributiva)} \end{cases}$$

(usiamo la proprietà distributiva proprio come ponte tra le due operazioni, infatti vogliamo capire cosa fa il **prodotto** per l'elemento neutro della **somma**) quindi

$$\begin{aligned} x + 0 &= x \\ (x+0)y &= xy \\ xy + 0y = xy &\iff 0y = 0 \end{aligned}$$

NB: $\{0\}$ NON È UN CAMPO

Anello delle classi di resto $\mathbb{Z}/n\mathbb{Z}$ commutativo

Anello degli interi di Gauss $\mathbb{Z}[i]$ $\mathbb{C} \supset \mathbb{Z}[i] \coloneqq \{a + bi \in \mathbb{C} \colon a, b \in \mathbb{Z}\}$, commutativo

Unità di R **e insieme delle unità** R^* $x \mid \exists\, x^{-1} \colon x \cdot x^{-1} = x^{-1} \cdot x = 1$

Divisori di zero $a \neq 0 \mid \exists\, b \neq 0$ tale che $ab = 0$ (divisore sinistro) / $ba = 0$ (divisore destro)

Dominio di integrità Anello *non banale*, *commutativo* e *senza divisori di zero*

Sottoanelli $S \subseteq R$ tale che $(S, +, \cdot, 0, 1)$ anello $[(S, +, 0)$ sottogruppo di $(R, +, 0)$, e $a, b \in S \implies ab \in S]$

Prodotto di anelli $R_1 \times R_2$ con addizione $(r, s) + (r', s') = (r + r', s + s')$ e moltiplicazione $(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$

Se $R_1, R_2 \neq \{0\}$, ha divisori di zero in quanto $(r, 0) \cdot (0, r) = (0, 0)$

Anello dei polinomi $R[X]$ $R[X] = \left\{\sum_{i=0}^{\infty} a_i X^i : a_i \in R\right\}$, con

$$\boxed{+} \quad \left(\sum_{i=0}^{\infty} a_i X^i\right) + \left(\sum_{i=0}^{\infty} b_i X^i\right) = \sum_{i=0}^{\infty} (a_i + b_i) X^i \qquad \boxed{\cdot} \quad \left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i\right) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^i$$

$R[X]$ commutativo $\Leftrightarrow$ R commutativo, R dominio $\Rightarrow$ $R[X]$ dominio e $\deg(fg) = \deg(f) + \deg(g)$

Anello dei polinomi in n **variabili** $R[X_1, X_2, \ldots, X_n] = (R[X_1, X_2, \ldots, X_{n-1}])[X_n]$

Campo quoziente $Q(R)$ R *dominio*, $\Omega \coloneqq \{(a, r) \in R \times (R - \{0\})\}$, $(a, r) \sim (b, s) \Leftrightarrow as = br$ relazione d'equivalenza, $Q(R) = \Omega/\!\sim = \left\{\frac{a}{r} \text{ classe di } (a, r)\right\}$, addizione $\frac{a}{r} + \frac{b}{s} = \frac{as+br}{rs}$ e moltiplicazione $\frac{a}{r} \cdot \frac{b}{s} = \frac{ab}{rs}$

Campo delle funzioni razionali $K(X) = Q(K[X])$

Anello degli endomorfismi $\mathbf{End}(A)$ A gruppo *additivo*, addizione $(f + g)(a) = f(a) + g(a)$, prodotto $(fg)(a) = f(g(a))$

Anello delle funzioni $R^X \coloneqq \{f \colon X \longrightarrow R\}$ X insieme, R anello, addizione $(f + g)(x) = f(x) + g(x)$, prodotto $(f \cdot g)(x) = f(x) \cdot g(x)$

Anelli $C^0([0, 1])$, $C^1([0, 1])$, $C^\infty([0, 1])$

Teoremi

Gruppo moltiplicativo dell'insieme delle unità

Dimostrazione Vale associatività, 1 è elemento neutro, inverso $a \in R^* \Rightarrow a^{-1} \in R^*$, e chiusura $a, b \in R^* \Rightarrow ab \in R^*$ siccome

$$(ab)\left(b^{-1}a^{-1}\right) = \left(b^{-1}a^{-1}\right)(ab) = 1$$

Campo $\mathbb{Z}/p\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ campo $\iff$ n primo

Dimostrazione $\forall\, a \in (\mathbb{Z}/n\mathbb{Z} - \{0\})$ ha inverso moltipl. $\Leftrightarrow \forall\, a \in \mathbb{Z}\colon 0 < a < n$ si ha $\operatorname{mcd}(a, n) = 1 \Leftrightarrow n$ primo

Indivisibilità dello zero per le unità

Un'unità di R non può essere divisore di zero

Dimostrazione Per assurdo, a, b, c tali che $ab = 1$, $ca = 0$, $c \neq 0$, allora

$$0 = 0 \cdot b = (ca) \cdot b = c \cdot (ab) = c \cdot 1 = c \quad \lightning$$

Campo quoziente è campo

Il campo quoziente come definito sopra è un campo.

Dimostrazione Prima buone def. delle operazioni:

- Buona def. del $+$: abbiamo

$$\frac{a}{r} = \frac{a'}{r'} \iff ar' = a'r, \qquad \frac{b}{s} = \frac{b'}{s'} \iff bs' = b's$$

allora

$$(a's' + b'r')rs = a's'rs + b'r'rs = (a'r)s's + (b's)r'r = ar's's + bs'r'r = (as + br)r's'$$

che per def.

$$\frac{a's' + b'r'}{r's'} = \frac{as + br}{rs} \longrightarrow \frac{a'}{r'} + \frac{b'}{s'} = \frac{a}{r} + \frac{b}{s}$$

Part VIII
Omomorfismi di anelli e Ideali

Definizioni

Omomorfismo di anelli $f(a + b) = f(a) + f(b)$ $\quad f(a \cdot b) = f(a) \cdot f(b)$ $\quad f(1) = 1$

Ideale sinistro, destro, bilaterale $I \subseteq R$ sottogruppo additivo, $ra \in I$ $\quad \forall\, r \in R$, $\forall\, a \in I$ (destro se $ar \in I$) $\longrightarrow$ sottogruppo additivo (normale) + **assorbe** R in I

Ideale principale sinistro $Rx \coloneqq \{rx \colon r \in R\}$ e destro $xR \coloneqq \{xr \colon r \in R\}$, ideali (x) generati da x

Ideale generato da $a_1, a_2, \ldots, a_n$ $(a_1, \ldots, a_n) = a_1R + \cdots + a_nR \coloneqq \{a_1x_1 + \cdots + a_nx_n \colon x_1, \ldots, x_n \in R\}$

Intersezioni, Prodotti, Somme di ideali Dati I, J ideali bilaterali, sono ideali $I \cap J$, $I + J \coloneqq \{x + y \colon x \in I, y \in J\}$ e $IJ \coloneqq \{\sum_{k=1}^{m} x_k y_k \colon x_k \in I, y_k \in J\}$

$$\begin{array}{ccccccc} & & & \subset & I & \subset & \\ IJ & \subset & I \cap J & & & & I + J \subset R \\ & & & \subset & J & \subset & \end{array}$$

Ideali coprimi $I + J = R$

Anelli quoziente $R/I \coloneqq \{x + I \colon x \in R\}$ NB è con il $+$
Elementi $\overline{x} = x + I = I + x$, $\overline{x} = \overline{y} \Leftrightarrow x - y \in I$, addizione $\overline{x} + \overline{y} = \overline{x + y}$, moltiplicazione $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

Omomorfismo canonico $\pi \colon R \longrightarrow R/I$, $\pi(x) = \overline{x}$ suriettivo, di nucleo $\ker(\pi) = I$

Teoremi

Ideale del Nucleo di omomorfismi

f omomorfismo, allora $\ker(f)$ ideale

Dimostrazione Presi $r \in R$ e $x \in \ker(f)$ ho che $f(rx) = f(r) f(x) = f(r) \cdot 0 = 0$, e quindi $rx \in \ker(f)$. Analogamente $xr \in \ker(f)$

Ideali contenenti un'unità

$I \subseteq R$ ideale che contiene un'unità $a \in R^*$, allora $I = R$

Dimostrazione Vale che $a \in I \Rightarrow a \cdot a^{-1} \in I \Rightarrow \forall x \in R \quad x = x \cdot 1 \in I$

Corollario

Dato R anello con divisione

(i) R ha solo ideali banali

(ii) Dato R' anello non banale, $f \colon R \to R'$ omomorfismo è sempre iniettivo

Dimostrazione

(ii) Vale che $f(1) = 1$, quindi $1 \notin \ker(f)$, ma quindi $\ker(f) \neq R \Rightarrow \ker(f) = \{0\}$

Teorema di omomorfismo

$f \colon R \longrightarrow R'$ omomorfismo di anelli, $I \subseteq R$ ideale con $I \subseteq \ker(f)$, allora, $\exists!\, h \colon R/I \longrightarrow R'$ tale che $h \circ \pi = f$, ovvero $h(x + N) = f(x)$. Alternativamente, il diagramma è commutativo.

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ {\scriptstyle \pi}\searrow & & \nearrow{\scriptstyle h} \\ & R/I & \end{array}$$

Dimostrazione Definisco $h(\overline{x}) = f(x)$, ben definita in quanto

$$\overline{x} = \overline{y} \longrightarrow x - y = a \quad \text{con } a \in I \subseteq \ker(f), \quad \text{dunque } f(x) = f(y + a) = f(y) + f(a) = f(y)$$

Per costruzione vale $h(\pi(x)) = f(x)$, ed omomorfismo in quanto $h(\overline{1_R}) = f(1_R) = 1_{R'}$

$$h(\overline{x + y}) = f(x + y) = f(x) + f(y) = h(\overline{x}) + h(\overline{y}) \qquad h(\overline{xy}) = f(xy) = f(x) f(y) = h(\overline{x})\, h(\overline{y})$$

Primo teorema di isomorfismo

$f\colon R \longrightarrow R'$ omomorfismo di anelli, allora $R/\ker(f) \cong f(R)$

Dimostrazione Dal Teorema di omomorfismo, con $I = \ker(f)$, ottengo $h(\overline{x}) = f(x)$. Preso ora $\overline{x} \in \ker(h)$, ho che $h(\overline{x}) = f(x) = e'$, dunque $x \in \ker(f)$, ovvero $\overline{x} = \overline{0}$ e perciò h è inettiva, quindi isomorfismo.

Secondo teorema di isomorfismo

$R' \subseteq R$ sottoanello, $I \subseteq R$ ideale, allora:

(i) $R' \cap I$ ideale di R' (ii) $R' + I$ sottoanello di R (iii) $R'/(R' \cap I) \cong (R' + I)/I$

Terzo teorema di isomorfismo

I ideale di R, ogni ideale di R/I ha la forma J/I con J ideale di R tale che $I \subseteq J \subseteq R$, e inoltre $(R/I)/(J/I) \cong R/J$

Teorema Cinese del Resto

I, J ideali coprimi di R anello commutativo ($I + J = R$). Allora vale che

(i) $IJ = I \cap J$ (ii) $R/(IJ) \cong (R/I) \times (R/J)$

Dimostrazione

(i) $\subseteq$) Vale sempre che $IJ \subseteq I \cap J$ (in quanto sia I che J sono chiusi rispetto al prodotto esterno).
$\supseteq$) Siccome $I + J = R$, ho che $\exists\, x \in I, y \in J$ tali che $x + y = 1$, prendo allora $z \in I \cap J$ e osservo $z = z \cdot 1 = zx + zy$, dove

$$\begin{cases} zx \in (I \cap J)I \subseteq JI \\ zy \in (I \cap J)J \subseteq IJ = JI \text{ essendo commutativo} \end{cases} \implies z = zx + zy \in IJ + IJ = IJ$$

che dimostra $z \in IJ$, ovvero $IJ \supseteq I \cap J$

(ii) Prendo $\Psi\colon R \to (R/I) \times (R/J)$ tale che $\Psi(x) = (x \mod I, x \mod J)$, ovvero la proiezione standard ai due quozienti, che è dunque **omomorfismo** con $\ker(\Psi) = I \cap J = IJ$ (per punto (i)). Ψ è **suriettivo** in quanto ogni (a, b) nel codominio ha preimmagine definita da $z = ay + bx$ con $x \in I, y \in J$ tali che $x + y = 1$. Infatti:

$$\begin{cases} z = ay + bx \equiv ay = a(1 - x) = a - ax \equiv a \mod I \\ z = ay + bx \equiv bx = b(1 - y) = b - by \equiv b \mod J \end{cases} \implies \Psi(z) = (a, b)$$

Quindi, per il primo teo. di isomorfismo $R/\ker\Psi \cong \Psi(R) \implies$ tesi

Corollario

Dati m, n interi coprimi vale

(i) Isomorfismo tra anelli $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

(ii) Isomorfismo tra gruppi $(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$

(iii) Se m, n coprimi e positivi, allora $\varphi(nm) = \varphi(n)\varphi(m)$

Corollario

n intero positivo, allora $\varphi(n) = \prod_{p \in P}\left(1 - \frac{1}{p}\right)$ con $P \coloneqq \{p \text{ primo}\colon p \mid n\}$

Dimostrazione [...]

Part IX
Zeri di Polinomi

Definizioni

Zero di un polinomio $f(\alpha)=0$ e zeri doppi $f_1(\alpha)=0$ per $f=f_1\cdot(X-\alpha)$

Polinomio derivato f' Dato $f\in R[X]$ con R anello commutativo, $f'=na_nX^{n-1}+(n-1)a_{n-1}X^{n-2}+\cdots+a_1$

Teoremi

Divisione con resto

Sia R anello, dati $f,g\in R[X]$ con $g=b_mX^m+\cdots+b_1X+b_0$ e $b_m\in R^*$, allora $\exists!\, q,r\in R[X]$ tali che

$$f=qg+r,\qquad r=0 \text{ oppure } \deg(r)<\deg(g)$$

Dimostrazione

- **Esistenza:** Di $f_1(\alpha)=0$ mostro per $\deg(f)\geq\deg(g)$, altrimenti banale. Dimostro per induzione sul grado di f: sia $f=a_nX^n+\cdots+a_1X+a_0$ con $n\geq m$, e considero

  $$f_1=f-a_nb_m^{-1}X^{n-m}g=\left(a_{n-1}-a_nb_m^{-1}b_{m-1}\right)X^n+\ldots$$

  Siccome $\deg(f_1)<\deg(f)$ per induzione ho $f_1=q_1g+r_1$ con $r_1=0$ oppure $\deg(r_1)<\deg(g)$, da cui

  $$f=f_1+a_nb_m^{-1}X^{n-m}g=\left(q_1+a_nb_m^{-1}X^{n-m}\right)g+r_1$$

- **Unicità:** Considero $f=qg+r=q'g+r'$, avrei $(q-q')g=r'-r$. Se per assurdo $q\neq q'$, siccome $b_m\in R^*$ ho che $\deg(q-q')g\geq\deg(g)$, ma vale che $\deg(r-r')<\deg(g)$ oppure $r-r'=0$, ↯.

Principalità degli ideali dei polinomi a coefficienti in un campo

Dato K campo, gli ideali di $K[X]$ sono principali

Dimostrazione Sia I un ideale di $K[X]$. Se $I=\{0\}$, è principale, altrimenti prendo $g\in I$ non nullo di grado minimale, e dimostro che $I=(g)$. Prendo $f\in I$, posso scrivere $f=qg+r$ e noto che $r=f-qg\in I$, ma non può essere $\deg(r)<\deg(g)$ quindi $r=0$, quindi $f=qg$ da cui la tesi.

Struttura di $R[X]/(X-\alpha)$

Dato R anello commutativo e $\alpha\in R$ vale che:

(i) Per ogni polinomio $f\in R[X]$ esiste $q\in R[X]$ tale che $f=q\cdot(X-\alpha)+f(\alpha)$

(ii) $\Psi: R[X]\longrightarrow R,\quad f\mapsto f(\alpha)$ è un omomorfismo suriettivo di nucleo $(X-\alpha)$

(iii) C'è un isomorfismo indotto da Ψ tra $R[X]/(X-\alpha)\cong R,\quad \overline{f}\mapsto f(\alpha)$

Dimostrazione

(i) Ho che $f = q \cdot (X - \alpha) + r$, e ottengo r da $f(\alpha) = q(\alpha)(\alpha - \alpha) + r$

(ii) Ψ omomorfismo suriettivo (grazie alla commutatività), per (i) $f \in \ker(\Psi)$ se e solo se f è divisibile per $X - \alpha$

(iii) Primo Teorema di Isomorfismo applicato a Ψ

Isomorfismo tra $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$

Dimostrazione Considero $\Phi(f) = f(i)$, ovviamente omomorfismo suriettivo, per il nucleo osservo che $(X^2+1) \subseteq \ker(\Phi)$. Viceversa, per $f \in \ker(\Phi)$ ho $f = q \cdot (X^2+1) + r$, da cui $r(i) = 0$, ma vale $\deg(r) \leq 1$, quindi $r(i) = ai + b = 0$, quindi $r \equiv 0$, da cui $X^2 + 1 \mid f$, $(X^2+1) \supseteq \ker(\Phi)$. La tesi dal Primo Teorema di Isomorfismo.

Struttura di $\mathbb{R}[X]/(g)$

R anello commutativo e $g = b_n X^n + \cdots + b_1 X + b_0 \in R[X]$ e $b_n \in R^*$, allora $\forall \overline{f} \in R[X]/(g)$ esiste unico $r \in R[X]$ con $\deg(r) < n$ oppure $r = 0$ tale che $\overline{f} = \overline{r}$, ovvero $R[X]/(g) = \{r : r = a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[X]\}$

Dimostrazione Preso $\overline{f} \in R[X]/(g)$ ho $\overline{f} = \overline{qg + r} = \overline{r}$ siccome $(qg + r) - r = qg \in (g)$. L'unicità dalla divisione col resto.

Scomponibilità di un polinomio in un dominio di integrità

R dominio di integrità e $f \in R[X]$ polinomio di zeri distinti $\alpha_1, \alpha_2, \ldots, \alpha_n$, allora $\exists\, q \in R[X]$ tale che

$$f = q \cdot (X - \alpha_1)(X - \alpha_2) \cdot \cdots \cdot (X - \alpha_n)$$

Dimostrazione Per induzione su n, $n = 0$ banale, dato n per $n+1$ posso scrivere $f = f_1 \cdot (X - \alpha_{n+1}) + f(\alpha_{n+1}) = f_1 \cdot (X - \alpha_{n+1})$, ma $\alpha_1, \alpha_2, \ldots, \alpha_n$ sono anche zeri di $f_1$in quanto $\forall\, 1 \leq i \leq n$ ho $0 = f_1(\alpha_i)(\alpha_i - \alpha_{n+1})$ con $\alpha_i - \alpha_{n+1} \neq 0$ per ipotesi e R dominio di integrità, quindi $f_1(\alpha_i) = 0$

Corollario

Un polinomio di grado d in un dominio di integrità ha al più d zeri distinti.

Proprietà del polinomio derivato

$$\alpha' = 0 \quad \text{per } \alpha \text{ costante} \qquad (f+g)' = f' + g' \qquad (f \cdot g)' = f'g + fg'$$

Caratterizzazione degli zeri doppi

α zero doppio per $f \iff f'(\alpha) = 0$

Dimostrazione

$$f = f_1 \cdot (X - \alpha) \quad \longrightarrow \quad f' = f_1' \cdot (X - \alpha) + f_1 \quad \longrightarrow \quad f'(\alpha) = \cancel{f_1'(\alpha) \cdot (\alpha - \alpha)} + f_1(\alpha) = 0$$

Prodotto di tutti i polinomi di grado 1 di $\mathbb{Z}/p\mathbb{Z}[X]$

Dato p primo, in $\mathbb{Z}/p\mathbb{Z}[X]$ vale

$$\prod_{\overline{a} \in \mathbb{Z}/p\mathbb{Z}} (X - \overline{a}) = X^p - X$$

Dimostrazione Per il Teorema di Fermat vale $\overline{a}^{p-1} = \overline{1}$ per $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, ovvero $\forall\, \overline{a} \in \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$ è uno zero di $X^{p-1} - 1$, moltiplicando il polinomio per $X = X - \overline{0}$ ho la tesi.

Teorema di Wilson

p primo $\iff (p-1)! \equiv -1 \mod p$

Dimostrazione

$\Rightarrow$ Per $p = 2$ verifica diretta. Per p dispari, ho che $\prod_{i=1}^{p-1} \left(X - \overline{i}\right) = X^{p-1} - \overline{1}$, che valutato in $X = \overline{0}$ dà

$$\left(\overline{-1}\right) \cdot \left(\overline{-2}\right) \cdot \cdots \cdot \left(\overline{-(p-1)}\right) = -\overline{1} \quad \longrightarrow \quad \overline{(p-1)!} = -\overline{1}$$

Proprietà dei numeri primi

$p > 2$ primo, sono equivalenti

(i) $\exists\, x \in \mathbb{Z} \mid x^2 \equiv -1 \mod p$ (ii) $X^2 - 1$ ha uno zero in $\mathbb{Z}/p\mathbb{Z}$ (iii) $p \equiv 1 \mod 4$

Dimostrazione

(i) $\Rightarrow$ (iii) $x^2 \equiv -1 \mod p \Rightarrow \operatorname{ord}(\overline{x}) = 4$, quindi $4 \mid \#\left(\mathbb{Z}/p\mathbb{Z}\right)^* = p - 1 \Rightarrow p \equiv 1 \mod 4$

(iii) $\Rightarrow$ (i) Posso prendere $x = \left(\frac{p-1}{2}\right)!$ che soddisfa $x^2 \equiv -1 \mod p$

Part X
Ideali primi e massimali

Definizioni

SIAMO IN ANELLI COMMUTATIVI

Ideale primo $I \subsetneq R$ ideale primo di un anello commutativo R se $\forall\, x, y \in R \quad xy \in I \implies x \in I \ \vee \ y \in I$

Ideale massimale $I \subsetneq R$ ideale massimale di un anello commutativo R se $\forall\, J$ ideale tale che $I \subseteq J \subseteq R$ vale $J = I$ oppure $J = R$

SIAMO IN DOMINI DI INT:

Irriducibile $\alpha \in R$ irriducibile in R dominio di integrità se $\alpha \neq 0$, $\alpha \notin R^*$ e $\alpha = \beta\gamma \implies \beta \in R^* \ \vee \ \gamma \in R^*$

Implicazioni tra ideali primi, ideali massimali e irriducibili Dato R dominio di integrità ho che

$$(\alpha) \text{ massimale} \implies (\alpha) \text{ primo} \implies \alpha \text{ irriducibile}$$

Teoremi

Caratterizzazione degli ideali primi

$I \subsetneq R$ ideale è primo in un anello commutativo $R \iff R/I$ è un dominio di integrità

Dimostrazione Per definizione $R/I \neq \{0\}$. Siano $x, y \in R$ tali che $\overline{x} \cdot \overline{y} = \overline{0}$ in R/I, significa che $xy \in I$, ovvero $x \in I \ \vee y \in I$, cioè $x = \overline{0} \ \vee y = \overline{0}$, quindi R/I è un dominio di integrità. L'implicazione inversa è la dimostrazione nel senso opposto.

Corollario (riformulazione def. dominio

$\{0\}$ ideale banale è primo $\iff$ R dominio di integrità

Caratterizzazione degli ideali massimali

$I \subsetneqq R$ ideale è massimale in un anello commutativo $R \iff R/I$ è un campo

Dimostrazione

$\Rightarrow$ Per definizione $R/I \neq \{0\}$. Prendo $\overline{x} \in R/I$ non nullo (ovvero $x \in R$ ma $x \notin I$) e cerco l'inverso. L'ideale $I + (x)$ è tale che $I \subsetneqq I + (x) \subseteq R$ e quindi $I + (x) = R$ (in quanto per ipotesi I è massimale), e in paricolare $1 = y + rx$ per certi $y \in I$ e $r \in R$. Modulo I ottengo $\overline{1} = \cancel{\overline{y}} + \overline{rx} = \overline{r} \cdot \overline{x}$ da cui $\overline{x}^{-1} = \overline{r}$, R/I campo.

$\Leftarrow$ Prendo J ideale di R tale che $I \subseteq J \subseteq R$, ho che J/I è ideale di R/I, ma siccome R/I campo (e quindi anello con divisione) possiede solo ideali banali, da cui

$$\begin{cases} J/I = \{0\} \iff J = I \\ \quad \text{oppure} \\ J/I = R/I \iff J = R \end{cases}$$

Corollario

Ogni ideale massimale di un anello commutativo R è anche un ideale primo

Dimostrazione Ogni campo è dominio di integrità

Irriducibilità dei generatori di ideali primi principali

R dominio di integrità, $\alpha \in R$ non zero, allora (α) primo $\implies \alpha$ irriducibile

Dimostrazione Siccome $(\alpha) \neq R$ per definizione, ho $\alpha \notin R^*$. Prendo $\beta\gamma = \alpha$, ho che $\beta\gamma \in (\alpha)$, da cui $\beta \in (\alpha) \ \vee \ \gamma \in (\alpha)$. Prendo WLOG $\beta \in (\alpha)$ ovvero $\beta = r\alpha = r\beta\gamma$, da cui $\beta\,(1 - r\gamma) = 0$, e siccome R dominio di integrità e $\beta \neq 0$ ho che $1 = r\gamma$.

Esistenza di ideali massimali

R anello commutativo, allora

(i) Se $R \neq \{0\}$, allora R contiene un ideale massimale

(ii) Sia $I \neq R$ un ideale di R, allora $\exists\, J$ ideale massimale di R tale che $J \supseteq I$

Dimostrazione

(i) Dal Lemma di Zorn.

(ii) Applicando la parte (i) a R/I ottengo un ideale massimale per R/I della forma J/I con $J \supseteq I$ ideale di R. Ho quindi che $R/J \cong (R/I)\,/\,(J/I)$ è un campo, dunque J massimale.

Part XI
Fattorizzazione

Definizioni

Anello a ideali principali R dominio di integrità, è anello a ideali principali se ogni ideale di R è principale

Anello Euclideo R dominio di integrità, è anello euclideo se $\exists\, N\colon R-\{0\}\to\mathbb{Z}_{\geq 0}$ tale che $\forall\, x,y\in R$ posso scrivere $x=qy+r$ con $r=0$ oppure $N(r)<N(y)$

K campo $\Longrightarrow$ K anello Euclideo rispetto alla funzione $N\equiv 0$

Elementi associati α,β associati $\Longleftrightarrow$ $\exists\,\varepsilon\in R^*$ tale che $\alpha=\varepsilon\beta$. Si ha che $\forall\,\gamma\in R$ vale che $\alpha\mid\gamma\ \Leftrightarrow\ \beta\mid\gamma$

Anello a Fattorizzazione unica R dominio di integrità, è anello a fattorizzazione unica se $\forall\, x\in R, x\neq 0$ posso scrivere $x=u\cdot\pi_1\cdot\dots\cdot\pi_t$ con $u\in R^*$ e π_i irriducibili, unica a meno di ordine e fattori associati

Teoremi

Proprietà degli anelli a ideali principali

Sia R anello a ideali principali e $\alpha\in R$, $\alpha\neq 0$, allora sono equivalenti

(i) (α) massimale (ii) (α) primo (iii) α irriducibile

Dimostrazione Basta dimostrare (iii) $\Rightarrow$ (i). Per definizione, ho $\alpha\notin R^*$, prendo J ideale tale che $(\alpha)\subseteq J\subseteq R$, ma siccome R a ideali principali ho $J=(\beta)$, e vale che $\alpha=r\beta$. Ma siccome α irriducibile $\beta\in R^*$ oppure $r\in R^*$, nel primo caso $J=R$ e nel secondo $J=(\alpha)$

Corollario

In un anello a ideali principali ogni ideale primo è massimale.

Anello Euclideo $\Longrightarrow$ Anello a ideali principali

Dimostrazione Per definizione R dominio di integrità, preso $I\neq\{0\}$ ideale di R (per $\{0\}$ banale) osservo che questo è principale in quanto se prendo $y\in I$ tale che $N(y)$ minimale, ho che $\forall\, x\in I$ posso scrivere $x=qy+r$, ma $r=x-qy\in I$ quindi $r=0$ (impossibile $N(r)<N(y)$), da cui $I=(y)$

Anello Euclideo degli interi di Gauss

$\mathbb{Z}[i]$ è un anello Euclideo rispetto alla funzione $N(a+bi)=a^2+b^2$

Dimostrazione [...]

Corollario

Sia $p\neq 2$ primo, allora $p=a^2+b^2$ per certi interi a,b se e soltanto se $p\equiv 1 \mod 4$.

Dimostrazione [...]

Proprietà degli anelli a fattorizzazione unica

Sia R anello a fattorizzazione unica, allora π irriducibile $\Longleftrightarrow$ (π) primo

Dimostrazione Basta dimostrare $\Rightarrow$. Prendo $\beta,\gamma\in R$ con $\beta\gamma\in(\pi)$, fattorizzo β e γ come prodotto di irriducibili, π dovrà comparire nella fattorizzazione di β o in quella di γ, ovvero $\beta\in(\pi)$ o $\gamma\in(\pi)$.

Anello a ideali principali $\Longrightarrow$ Anello a fattorizzazione unica

Dimostrazione [...]

Part XII
Fattorizzazione di Polinomi

Definizioni

Numero di fattori π $\quad \operatorname{ord}_\pi(x)$ per $x \neq 0$ e π irriducibile

Massimo comun divisore

$$\operatorname{mcd}(x,y) \coloneqq \prod_{\pi \text{ irriducibile}} \pi^{\min(\operatorname{ord}_\pi(x),\operatorname{ord}_\pi(y))}, \quad x,y \neq (0,0), \text{ altrimenti } \operatorname{mcd}(x,0) = \operatorname{mcd}(0,x) \coloneqq x$$

Contenuto e Polinomio primitivo R dominio a fattorizzazione unica, $f = a_n X^n + \cdots + a_0 \in R[X]$ non nullo, allora contenuto $\operatorname{cont}(f) = \operatorname{mcd}(a_n, \ldots, a_0)$, e f primitivo $\Leftrightarrow \operatorname{cont}(f) = 1$

Teoremi

Proprietà del massimo comun divisore

Sia R dominio a fattorizzazione unica e $x, y \in R$ non nulli, allora:

(i) $x \mid y \iff \operatorname{ord}_\pi(x) < \operatorname{ord}_\pi(y) \quad \forall\, \pi$ irriducibile

(ii) $\forall\, z \in R, z \neq 0$ vale che $\operatorname{mcd}(zx, zy) = z \cdot \operatorname{mcd}(x,y)$

(iii) $\operatorname{mcd}(x,y)$ divide x e y, e ogni divisore comune di x e y divide $\operatorname{mcd}(x,y)$

Dimostrazione [...]

Unicità di fattorizzazione dei polinomi a coefficienti in un anello a fattorizzazione unica

R dominio a fattorizzazione unica $\Longrightarrow R[X]$ a fattorizzazione unica

Lemma Sia K il campo quoziente di R, allora ogni $g \in K[X], g \neq 0$ si può scrivere $g = c \cdot g_0$ con $c \in K^*$ e $g_0 \in R[X]$ primitivo, unici a meno di moltiplicazione per unità di R.
Posso trovare infatti $\gamma \in R, \gamma \neq 0$ per cui $h = \gamma \cdot g \in R[X]$ e preso $\delta = \operatorname{cont}(h)$ ho che $h = \delta \cdot g_0$ con g_0 primitivo

Lemma Dati due polinomi $f, g \in R[X]$ primitivi, $f \cdot g$ è primitivo.
Se $f \cdot g$ non fosse primitivo, $\exists\, \pi$ che divide tutti i sui coiefficienti, ovvero $f \cdot g \equiv 0$ in $R/(\pi)[X]$, ma siccome l'ideale (π) è primo, ho che l'anello $R/(\pi)[X]$ è un dominio di integrità, da cui $f \equiv 0 \vee g \equiv 0$, ovvero $\pi \mid \operatorname{cont}(f)$ oppure $\pi \mid \operatorname{cont}(g)$, ↯

Dimostrazione Considero $f \in R[X]$, dimostro dapprima che si può scrivere come $f = u \cdot \pi_1 \cdot \ldots \cdot \pi_s \cdot g_1 \cdot \ldots \cdot g_t$ con $u \in R^*$, π_i irriducibili di R e g_i polinomi primitivi in $R[X]$ irriducibili in $K[X]$. [...]
Concludo dimostrando che gli irriducibili di $R[X]$ sono gli irriducibili di R e i polinomi primitivi di $R[X]$ che sono irriducibili in $K[X]$.

Corollario

(i) L'anello $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ è un anello a fattorizzazione unica

(ii) K campo $\Rightarrow K[X_1, X_2, \ldots, X_n]$ anello a fattorizzazione unica.

Proprietà degli zeri di un polinomio

R dominio a fattorizzazione unica, K campo quoziente associato, e $f = a_n X^n + \cdots + a_0 \in R[X]$ con $a_n, a_0 \neq 0$, allora ogni $\alpha \in K$ zero di f ha la forma $\alpha = u/v$ con $u \mid a_0$ e $v \mid a_n$. Se f monico, ogni zero sta in R e divide a_0

Dimostrazione [...]

Irriducibilità di un polinomio di grado 2 o 3 in un campo

K campo, $f \in K[X]$ di grado 2 o 3 è irriducibile $\iff$ non ha zeri in K

Dimostrazione Per assurdo $f = g \cdot h$ con $g, h \in K[X]$ non costanti, allora almeno uno fra g e h avrebbe grado 1, $\lightning$.

Lemma di Gauss

R dominio a fattorizzazione unica, K campo quoziente associato, $f \in R[X]$ primitivo è irriducibile in $R[X]$ $\iff$ è irriducibile in $K[X]$

Dimostrazione Posso scomporre $f = u \cdot g_1 \cdot \cdots \cdot g_t$ con $u \in R^*$, $g_i \in R[X]$ primitivi e irriducibili in $K[X]$ con $t \geq 1$ (f primitivo $\Rightarrow \deg(f) > 0$), allora f è irriducibile in $R[X] \iff t = 1 \iff$ è irriducibile in $K[X]$

Corollario

$f \in \mathbb{Z}[X]$ monico, se $\exists\, p$ primo tale che $f \mod p \in \mathbb{Z}/p\mathbb{Z}[X]$ è irriducibile allora f è irriducibile in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$

Criterio di Eisenstein

R dominio a fattorizzazione unica, $f = a_n X^n + \cdots + a_0 \in R[X]$ primitivo, π elemento irriducibile di R , allora f è irriducibile in $R[X]$ se

$$\pi \text{ non divide } a_n \qquad \pi \text{ divide } a_k \text{ con } k = 0, \ldots, n-1 \qquad \pi^2 \text{ non divide } a_0$$

Dimostrazione Per assurdo $f = g \cdot h$ fattorizzazione non banale in $R[X]$, allora $\deg(g), \deg(h) > 0$ e vale che

$$\overline{a_n} X^n = \overline{g} \cdot \overline{h} \quad \text{in } R/(\pi)[X] \quad \longrightarrow \quad g \equiv bX^k, \quad h \equiv aX^{n-k} \mod \pi$$

Ma ciò vuol dire che i termini noti di g e h sono divisibili per π, da cui $\pi^2 \mid a_0$, $\lightning$.

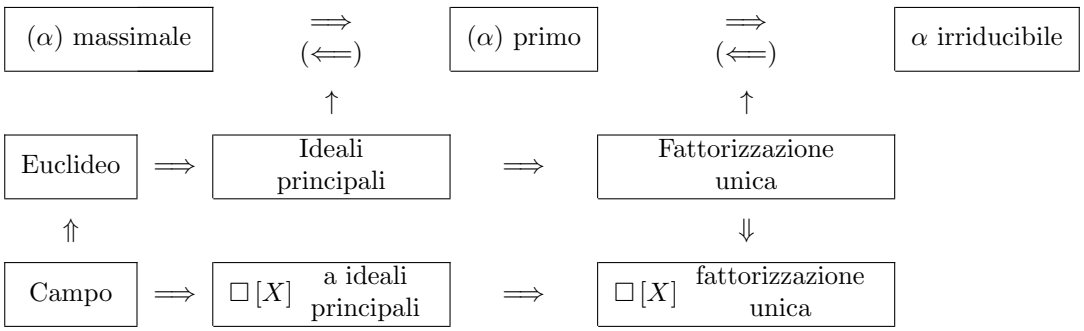
	Commutativi			Non commutativi		
1	$\{e\}$ $=C_1=S_1=A_1$					
2	C_2 $=S_2$					
3	C_3 $=A_3$					
4	C_4	$C_2 \times C_2$ $=D_2=V_4$				
5	C_5					
6	C_6			D_3 $=S_3$		
7	C_7					
8	C_8	$C_4 \times C_2$	$C_2 \times C_2 \times C_2$	D_4	Q_8	
9	C_9	$C_3 \times C_3$				
10	C_{10}			D_5		
11	C_{11}					
12	C_{12}	$C_6 \times C_2$		D_6	A_4	B
13	C_{13}					
14	C_{14}			D_7		
15	C_{15}					

C_n	$(C_2)^n$	$C_4 \times C_2$	$C_3 \times C_3$	$C_6 \times C_2$

A_4

D_3	D_4	D_5

Q_8	B



Part XIII
Riassunto gruppi

1 Commutatività e normalità

- G non ha sottogruppi (non banali) $\iff$ $G \cong C_p$ con p primo, ovvero G è ciclico di ordine un numero primo.
  Dim: $\implies$) $< g >$ è sottogruppo, ed è il più piccolo sottogruppo che contiene g (quindi non è neanche banale), ma G non ha sottogruppi propri non banali quindi $< g >= G$. $\impliedby$) ovvio, in quanto i sottogruppi di un gruppo ciclico sono solo ciclici, quindi generati da un solo elemento e dato che p non ha divisori, ogni elemento genera tutto il gruppo.
- Ogni gruppo G ha almeno due sottogruppi normali: G e $\{0\}$.
- **Gruppo semplice**: se ha solo G e $\{0\}$ come sottogruppi normali.
  Esempi: **gruppi semplici abeliani** sono **solo** i C_p con p primo; **gruppi semplici non abeliani**: il più piccolo è A_5 che ha 60 elementi.
- Qualunque sottogruppo che contiene $[G, G]$ è normale in G

2 Gruppo simmetrico S_n

2.1 Generalità

- Sottogruppi **normali** di S_n: per $n = 3$ o $n \geq 5$ S_n ha solo A_n come sottogruppo normale, il quale per tali n è semplice, ovvero a sua volta non ha sottogruppi normali.

Gruppo	**Cosa rappresenta**	**Sottogr.**	**Sottogr. normali**	**Cosa rappresentano**
S_1	Identità		/	
S_2	$\cong C_2$		/	
S_3	$\cong D_3$ (rotaz.+rifl. triangolo)	Sono 6	$A_3 \cong < r >$	Rotaz. triangolo
S_4	Rotaz. cubo/ottaedro	Sono 30	A_4, V_4	Rotaz tetraedro, rotaz.+rifl. rettangolo
S_5			A_5	Rotaz icosaedro/dodecaedro

Diagramma sottogruppi di S_4: `https://people.maths.bris.ac.uk/~matyd/GroupNames/1/S4.html`
Diagramma ciclico di S_4: `https://en.wikiversity.org/wiki/Symmetric_group_S4#/media/File:Symmetric_group_4;_cycle_graph.svg`

Part XIV
Riassunto anelli

3 Implicazioni tra strutture

Anelli $\supset$ Anelli commutativi $\supset$ Domini di integrità $\supset$ A fattorizzazione unica $\supset$ A ideali principali $\supset$ Euclideo $\supset$ Campi

Campo $\implies$ euclideo

Euclideo $\implies$ a ideali principali

(p. 106) Per definizione R dominio di integrità, preso $I \neq \{0\}$ ideale di R (per $\{0\}$ banale) osservo che questo è principale in quanto se prendo $y \in I$ tale che $N(y)$ minimale, ho che $\forall\, x \in I$ posso scrivere $x = qy + r$, ma $r = x - qy \in I$ quindi $r = 0$ (impossibile $N(r) < N(y)$), da cui $I = (y)$

A ideali principali $\implies$ a fattorizzazione unica

p. 109

A fattorizzazione unica $\implies$ Dominio di int.

Dominio di int. $\implies$ anello commutativo

Anello commutativo $\implies$ anello

4 Esempi

Anelli: $\mathbb{H}$ (ma non contiene divisori di zero)
Anelli commutativi: $R_1 \times R_2$ (se entrambi anelli commutativi) contiene divisori di zero
Domini di integrità: $\mathbb{Z}[\sqrt{-5}]$
A fattorizzazione unica: $K[X_1, X_2]$ con K campo
A ideali principali: roba strana, tipo $R[X,Y]/(X^2+Y^2+1)$
Euclideo: $\mathbb{Z}$, $K[X]$ con K campo (rispetto alla funzione grado), $\mathbb{Z}[i]$ rispetto alla funzione $N(a+bi) = a^2+b^2$
Campi: $\mathbb{Z}/p\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, Q(R)$ (campo dei quozienti se R dominio)

5 Omomorfismi

Proprietà omomorfismi:

- $f(0_A) = 0_B$
- $f(-a) = -f(a)$ (f è omom. di gruppi additivi)
- a unità, allora $f(a^{-1}) = f(a)^{-1}$ (f induce un omom. di gruppi moltiplicativi se ristretto alle unità)
- $im(f)$ sottoanello di B
- $\ker(f)$ ideale di A
- f iniettivo $\iff \ker(f) = \{0\}$
- A campo, B non banale $\implies f$ iniettivo
- $\#A = \#(\ker(f))\#(\mathrm{im}(f))$
- I ideale di $B \implies f^{-1}(I)$ ideale di A
- per ogni anello R, esiste un **unico** omomorfismo $\mathbb{Z} \to R$ (per dim. basta vedere che $f(1) = 1_R$, quindi $f(n) = f(\underbrace{1+1+\cdots+1}_{n \text{ volte}}) = f(1)+\cdots+f(1) = 1_R+\cdots+1_R = n \cdot 1_R = n$, per numeri negativi fare ragionamento analogo ricordando $f(-1) = -f(1) = -1_R$. Quindi $f(n) = n\ \forall n \in \mathbb{Z}$ per forza.)

6 Ideali ed elementi

Esempi:
Ideali primi: $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$ con p primo
Ideali massimali: $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$ con p primo

Struttura	Elem.	Teo/prop.
Anelli		Unità $\implies$ non divisore di zero Le unità formano un gruppo moltiplicativo $f : R_1 \to R_2$ omom. $\implies$ $ker(f)$ è ideale di R_1 I ideale continiene un'unità $\implies$ $I = R$ I, J ideali $\implies$ $I \cap J, I + J$ ideali di R
Anelli commutativi	Associati	Teo. cinese resto: $I + J = R$ (ideali coprimi) $\implies$ $IJ = I \cap J$ $\implies$ $R/IJ \cong (R/I) \times (R/J)$ $I \subset R$ ideale primo $\iff$ R/I dominio di integrità $I \subset R$ ideale massimale $\iff$ R/I campo ...quindi massimale $\implies$ primo Ogni anello $\neq \{0\}$ contiene un ideale massimale Ogni ideale $\neq R$ è contenuto in un ideale massimale
(Anelli con divisione)		Ideali sono solo quelli banali R' non banale $\implies$ $f : R \to R'$ omom. è iniettivo
Domini di integrità	Irriducibili	$\alpha \neq 0$ allora (α) primo $\implies$ α irriducibile $(f) = (g)$ $\iff$ f e g sono associati
Anelli a fattorizzazione unica		α irriducibile $\iff$ (α) primo
Anelli a ideali principali		(α) massimale $\iff$ (α) primo $\iff$ α irriducibile
Anelli euclidei		
Campi		$\{0\}$ ideale massimale $\iff$ R campo

Attenzione alle definizioni:

- Campo: si richiede che $\forall x \neq 0$ esiste x^*, e 0 non deve avere inversi, ovvero divisori di zero. Quindi un campo è un dominio di integrità.
- se $g, f \neq 0$, allora $\deg(fg) = \deg(f) + \deg(g)$
- α in un dominio di integrità si dice **irriducibile** se $\alpha \neq 0, \alpha \notin R^*$ ...

7 Polinomi

Polinomi a coefficienti in:

Anelli	
Anelli commutativi	$f \in R[X]$ ha zeri $\implies$ f riducibile (p. 89) Le calssi di $R[X]/(g)$ hanno grado minore di g (p. 90) J/I primo in $A/I \iff J$ primo in A (per terzo teo.iso.)
(Anelli con divisione)	
Domini di integrità	R dominio $\implies$ $R[X]$ dominio (non ha divisori di zero) $(f) = (g) \iff f$ e g sono associati se $g, f \neq 0$, allora $\deg(fg) = \deg(f) + \deg(g)$ $f \in R[X]$ con R dominio $\implies f = q \cdot \prod(X - \alpha_i)$ con α_i gli zeri del pol. R dominio $\implies f \in R[X]$ di grado d ha al più d zeri distinti in R R dominio, allora $\alpha \in R$ è zero doppio di $f \in R[X] \iff f'(\alpha) = 0$
Anelli a fattorizzazione unica	Lemmi p. 117 R a fattorizzazione unica $\implies$ $R[X]$ a fattorizzazione unica $\mathbb{Z}[X_1, \ldots, X_n]$ è a fattorizzazione unica. $f \in R[X] \implies$ zeri: $\alpha = u/v$ con $u, v \in R$ e $u \mid a_0, v \mid a_n$ (Lemma Gauss) $f \in R[X]$ primitivo. Allora: f irriducibile in $R[X] \iff f$ irriducibile in $K[X]$ campo quoziente $f \in \mathbb{Z}[X]$ monico. $f \mod p \in \mathbb{Z}/p\mathbb{Z}$ irriducibile $\implies f$ irriduc. in $\mathbb{Z}[X]$ e $\mathbb{Q}[X]$ Criterio Eisenstein $\implies f$ irriducibile in $R[X]$
Anelli a ideali principali	$(f) + (g) = (f, g) = (mcd(f, g))$. Quindi: $(f) + (g) = \mathbb{Q}[X] \iff mcd(f, g) = 1$ (non hanno divisori comuni)
Anelli euclidei	
Campi	K campo $\implies$ $K[X]$ euclideo K campo $\implies$ $K[X_1, \ldots, X_n]$ anello a fattorizzazione unica $f \in K[X]$ di grado 2 o 3. f irriducibile in $K[X] \iff f$ non ha zeri in K

8 Concetti e generalizzazioni

Concetto	**Generalizzazione**
$\mathbb{Z}$	Anello euclideo
Fattorizzazione di interi	Fattorizzazione di polinomi
Numero primo	Ideale primo
Interi coprimi: $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$	Ideali coprimi: $I + J = R$

Part XV
Esame

9 Scritto

9.1 Gruppi

Miscellaneo

- Classe del prodotto è prodotto delle classi
- Per dimostrare uguaglianze tra insiemi/sottoinsiemi (come ideali, intersezioni, ecc) si può dim. $\subseteq$ e poi $\supseteq$
- Per dimostrare che una cosa divide un'altra posso far divisione con resto e dimostrare che $r = 0$
- Dimostrare che **due gruppi non sono isomorfi**: per esempio vedere che hanno cardinalità diversa, o (forse più utile) vedere che in un gruppo c'è un elemento con ordine "grande" t.c. non ci possono essere elementi con tale ordine nel secondo gruppo

Permutazioni:

- Ordine di un k-ciclo è k
- Prodotto di 3-cicli (non disgiunti) può avere ordine 2. Prodotto di due trasposizioni (non disgiunte) può generare 3-ciclo.
- Il numero di k-cicli in S_n è
$$\frac{n!}{(n-k)!} \cdot \frac{1}{k}$$
(il primo fattore sono le permutazione di k oggetti in n, mentre il secondo fattore c'è perché un ciclo non dipende dall'elemento da cui parto, quindi devo dividere per il numero di elementi del ciclo)
- Gruppo alternante: ogni elemento si può scrivere come prodotto di 3-cicli o come prodotto di un numero pari di trasposizioni (a due a due se sono congiunte danno luogo a un 3-ciclo, se sono disgiunte danno luogo a un 2-ciclo)

Sottogruppi, sottogruppi normali

- Verifica di sottogruppo: $e \in G$, $ab \in G \implies ab^{-1} \in G$. Delle volte è più comodo verificare $ab \in G$, $a^{-1} \in G$
- In $S_3 \cong D_3$ l'unico sottogruppo normale è $A_3 \cong < r >$ sottogruppo delle rotazioni. In generale in D_n i sottogruppi normali sono $< r^d > \ \forall d|n$ (per tutti), $< r^2, rf >$ (se n pari)
- Il massimo ordine di un elemento in A_4 è 3 (poiché A_4 è fatto solo dai cyle-type $[3^1]$ e $[2^2]$)
- $gH \in H \iff g \in H$, ovvero le classi ripartiscono il gruppo, quindi per forza g deve stare in H
- Se nelle ip. c'è che un sottogruppo è normale probabilmente nella dimo si deve usare un quoziente
- A sempre sottogruppo normale di $A \times B$ e $(A \times B)/A = B$
- Per dimostrare che un sottogruppo è normale si può trovare un omom. t.c. il sottogruppo = ker
- Sottogruppi e quozienti di un gruppo ciclico sono ciclici

Ordine

- Per dim. che un elemento ha ordine infinito devo dim che $a^k = e \iff k = 0$. Se devo dim. che l'ordine è k, devo verificare sia che $a^k = 0$, ma anche che k sia il minimo intero t.c. avvenga ciò.
- $\text{ord}(\overline{a}) \mid \text{ord}(a)$ (ordine della classe divide l'ordine del rappresentante)

- Formula che si usa:
$$\text{ord}(a^k) = \frac{\text{ord}(a)}{\text{mcd}(\text{ord}(a), k)}$$
Dimo: sia $n = \text{ord}(a)$. Voglio trovare il minimo c t.c. $(a^k)^c = a^{kc} = 1 \iff kc$ multiplo di n. Voglio che kc sia il più piccolo multiplo sia di k (così lo posso scrivere come kc per un qualche c) che di n (così fa l'elemento neutro). Allora:
$$\begin{aligned} kc = \text{mcm}(k,n) \implies c &= \frac{\text{mcm}(k,n)}{k} \\ &= \frac{\text{mcm}(k,n)\cdot n}{k\cdot n} \\ &= \frac{\text{mcm}(k,n)\cdot n}{\text{mcm}(k,n)\text{mcd}(k,n)} \quad \text{NB: } ab = \text{mcm}(a,b)\text{mcd}(a,b) \\ &= \frac{n}{\text{mcd}(k,n)} \end{aligned}$$

Omomorfismi

- f omomorfismo di gruppi $\implies f(< A >) =< f(A) >$ con A sottogruppo
- Per dim. che omomorf. è iniettivo: $\ker(f) = \{0\}$
- Isomorfismo di gruppi comodo: automorfismo interno $\gamma_a(g) = gag^{-1}$
- Omomorfismo iniettivo: **inclusione**
- Omomorfismo suriettivo: **proiezione al quoziente**
- $\#A = \#(\ker(f))\#(\text{im}(f))$

9.2 Anelli

- Verifica di sottonaello: deve essere sottogruppo additivo, avere l'1 ed essere chiuso nel prodotto
- **Verifica di ideale**: o si usano le proprietà (sottogruppo additivo+assorbe nel prodotto esterno) o si trova omomorf. di anelli di cui è il ker
- Ricorda: un ideale non banale non è un sottoanello (infatti non contiene l'1, se lo congenesse sarebbe tutto l'anello)
- Schemone anelli e anelli di polinomi
- per studiare l'irriducibilità di un polinomio monico con il lemma usare numeri primi p piccoli (tipo 2), che è più facile
- se devo dim. $A \cong B \times C$ con tutti anelli probabilmente c'è di mezzo teo. cinese resto
- Polinomi irriducibili si comportano come numeri primi: c'è nozione di mcm, essere coprimi (il loro prodotto genera tutto l'anello)
- G dominio $\iff \{0\}$ primo
- Anello commutativo $\neq \{0\}$ è **semplice** (solo ideali banali) $\iff$ campo
- $A \neq \{0\} \implies \exists$ un ideale massimale.
Infatti se $A = \{0\}$ l'unico suo ideale è $\{0\}$, che non è massimale in quanto uguale ad A. Se $A \neq \{0\}$ allora, se ha ideali $\neq \{0\}$ basta pigliare un massimale, se non ne ha allora $\{0\}$, che è sempre ideale, è un suo ideale massimale.
- Omomorfismo (suriettivo) di anelli comodo: valutazione dei polinomi in un α fissato. Per esempio $\psi_\alpha : \mathbb{Q}[X] \to \mathbb{Q} : \quad \psi_\alpha(f) = f(\alpha)$. È suriettivo poiché basta prendere come input i polinomi costanti e si ha l'identità.
- Omomorfismo iniettivo: **inclusione**. Ad esempio la mappa inclusione nel proprio campo quoziente $a \mapsto (a,1) = \frac{a}{1}$
- Omomorfismo suriettivo: **proiezione al quoziente**

- verificare che un **polinomio di grado alto** non è riducibile: per esempio verifichiamo che $X^4 + X^3 + X^2 + X + 1$ non è riducibile in $\mathbb{Z}/2\mathbb{Z}[X]$
  - **Radici**: vediamo che non ha radici in $\mathbb{Z}/2\mathbb{Z}$ (neanche a meno del segno, infatti le radici vanno cercate tra $\pm 0, \pm 1$, anche se $-1 \notin \mathbb{Z}/2\mathbb{Z}$, poiché se ci fosse -1 potrei dividere per $(X - (-1)) = (X + 1) \in \mathbb{Z}/2\mathbb{Z}[X]$) $\implies$ non lo posso dividere in un polinomio di primo grado $\implies$ quindi neanche di terzo grado (altrimenti avrei $f =$(terzo grado)$\cdot$(primo grado) per averlo di quarto)
  - allora ciò che rimane è provare a dividerlo per un polinomio di secondo grado, che sono: X^2, $X^2 + 1$, $X^2 + X$, $X^2 + X + 1$. Sicuramente non è divisibile per i primi tre perché essi sono riducibili, quindi divisibili per un polin. di primo grado e se f fosse divisibile per uno di quei tre sarebbe anche divisibile per un polin. di primo grado, cosa che abbiamo appena detto essere impossibile.
    L'unico che rimane è $X^2 + X + 1$: facciamo divisione con resto e vediamo che non è divisibile $\implies$ irriducibile

- Ricorda che in un dominio di integrità gli ideali $(f) = (g) \iff f$ e g sono associati

- Se vogliamo dimostrare $(f) + (g) = \mathbb{Z}[X]$, dato che quest'ultimo non è a id. princ. non possiamo usare $(f) + (g) = K[X] \iff mcd(f, g) = 1$. Allora un modo è dimostrare che $1 \in (f) + (g)$: infatti somma di id. è id. e se un $1 \in I \implies I = A$.
  Un modo è fare divisione con resto di g per f: così $g = qf + r \implies r = g - qf \implies r \in (g) + (f)$. Se siamo fortunati e $r = 1$ siamo apposto.

- È utile la seguente applicazione del **terzo teo. di isomorfismo**:
  in generale
  $$R/(a, b) \cong [R/(a)]/[(a, b)/(a)] = [R/(a)]/(\overline{b})$$
  In particolare (molto utile):
  $$\mathbb{Z}[X]/(n, f) \cong (\mathbb{Z}[X]/(n))/(\overline{f}) \cong \mathbb{Z}/n\mathbb{Z}[X]/(\overline{f})$$
  dove $\overline{f} \in \mathbb{Z}/n\mathbb{Z}[X]$

10 Orale

10.1 Esempi e controesempi

- Classi laterali diverse tra loro: in D_3 $r < f > \neq < f > r$

- Automorfismo $G \to G$ con G abeliano: lo è sempre la negazione $A(g) = -g$ (se $+$ è l'operazione). Non lo è per anelli o campi.
  In particolare $\mathbb{Z}$ ha solo questo come **unico automorfismo non banale** (deve mantenere la struttura additiva e ricoprire tutto $\mathbb{Z}$). Invece, considerando l'automorfismo di anelli, $\mathbb{Q}$ ed $\mathbb{R}$ hanno solo l'identità (banale) in quanto si deve mantenere sia la struttura additiva che moltiplicatima. $\mathbb{C}$ invece ha un solo automorfismo non banale, che è la coniugazione complessa (infatti lascia i numeri reali fermi).

- Omomorfismo $G \to \mathrm{Aut}(G)$ con nucleo il centro $Z(G)$. Come prima cosa devo trovare un automorfismo $G \to G$ (ovvero un **isomorfismo** che ha G stesso come immagine, in quanto omom. mantiene la sua struttura) che dipenda da un elemento, così assegno ad ogni elemento tale automorfismo e sono a posto. Ad esempio
  $$\gamma_g : G \to G \qquad \gamma_g(x) \coloneqq {}^g x = g^{-1}xg$$
  è un automorfismo (in quanto ha come nucleo $\ker \gamma_g = \{0\}$, infatti $g^{-1}hg = 1 \iff hg = 1 \iff h = 1$) chiamato **automorfismo interno**; assegna ad ogni elemento il proprio coniugato per g. Allora
  $$f : G \to \mathrm{Aut}(G) \qquad f(g) \coloneqq \gamma_g$$
  è omomorfismo (verificare) con nucleo $\ker f = Z(G)$ il centro di G. Infatti il nucleo è l'insieme degli elementi di G che vengono mappati nell'elemento neutro di $\mathrm{Aut}(G)$, ovvero l'**identità**: per ogni γ_g si ha l'identità per gli elementi che commutano con g, in modo che scambio h, g nella def. e ottengo l'identità, ovvero gli elementi del centralizzante $C(g)$ di g. Quindi l'insieme dei centralizzanti di tutti i $g \in G$ è il centro $C(Z)$ di G.

- Gruppo di Klein V_4: 4 elementi (neutro + 3), ogni elemento è l'inverso di se stesso e il prodotto di due elementi dà il terzo (non neutro). Può essere visto come gruppo delle simmetrie di un rettangolo non quadrato (le due riflessioni e rotazione di 180^o) oppure come $\mathbb{Z}_2 \times \mathbb{Z}_2$. É sottogruppo normale di S_4

- Anello in cui ci sono ideali tali che il prodotto non è un ideale:
- Omomorfismo di anelli $R \to \mathrm{End}(R)$:
- Sottoanello di $\mathbb{Q} \neq \mathbb{Z}$: $R = \{\frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{N}_0\}$. Si dimostra che ogni sottoanello di $\mathbb{Q}$ contiene $\mathbb{Z}$
- Ideali primi di $\mathbb{Z}/n\mathbb{Z}$: ogni ideale ha la forma $m\mathbb{Z}/n\mathbb{Z}$ con $m|n$ (per il terzo teo. iso). Per essere ideale primo m deve essere un numero primo, quindi sono $p\mathbb{Z}/n\mathbb{Z}$ con $p|n$, p primo.
- Ideale primo ma non massimale di $\mathbb{Z}[X]$: (in realtà vale per qualsiasi $R[X]$, R dominio di integrità) (X), in quanto $R[X]/(X) \cong R$ non è un campo (non essendolo R) $\iff$ (X) non è massimale. È primo in quanto R è un dominio di integrità, quindi non ha divisori di 0, quindi se il prodotto di due elementi sta in (X) (ovvero $a_0 b_0 = 0$) allora almeno uno dei due deve stare in (X) ($a_0 = 0$ oppure $b_0 = 0$)

10.2 Dimostrazioni

- Ideale massimale $\implies$ non principale in $\mathbb{Z}[X]$: dimostriamo il contrario, ovvero principale $\implies$ non massimale.
  Se $f \in \mathbb{Z}[X] = n \neq \pm 1$ (ovvero $f \in \mathbb{Z} \setminus \mathbb{Z}^*$) allora (X, n) contiene (f), in quanto contiene tutti i polinomi con coefficienti multipli di n, ma diverso da (f) poiché abbiamo anche tutti i polinomi di primo grado, con qualsiasi coeff., ed è diverso da tutto l'anello, in quanto per esempio non ha l'1.
  Se $f \in \mathbb{Z}[X]$ ha grado > 0, allora se p è un primo che non divide il coefficiente di grado massimo, (f, p) contiene (f) ed è diverso da tutto l'anello, dal momento che (terzo teo. iso.)

  $$\mathbb{Z}[X]/(f, p) \cong (\mathbb{Z}[X]/(p))/(\overline{f}) \cong \mathbb{Z}/p\mathbb{Z}[X]/(\overline{f})$$

  non può essere banale ($= \{0\}$, ovvero (f, p) deve essere diverso da tutto $\mathbb{Z}[X]$) poiché altrimenti

  $$(\overline{f}) = \mathbb{Z}/p\mathbb{Z}[X], \text{ ovvero } \overline{f} \in \mathbb{Z}/p\mathbb{Z}[X]^* = \mathbb{Z}/p\mathbb{Z}^*$$

  il che è impossibile dato che f ha grado > 0 e p non divide il coeff. di grado max.