Algoritmo euclideo di divisione

$\forall a \in \mathbb{N}_0,\ \forall b \in \mathbb{N},\ \exists!\ q, r \in \mathbb{N}_0$ tali che

$$a = q \cdot b + r \quad \text{con} \quad 0 \leq r < b$$

q = quoziente
r = resto

notazione: b è detto divisore di a se e solo se $r=0$.

Scriviamo $b \mid a \Leftrightarrow a = qb$

<u>dim</u>: Definiamo

$$S = \{ z \in \mathbb{N}_0 \mid z = a\cancel{q} - q \cdot b \text{ per qualche } q \in \mathbb{N}_0 \}$$

$S \subseteq \mathbb{N}_0$

$S \neq \emptyset$ perché: $a = a - 0 \cdot b \in S$, quindi per il buon ordinamento, S ha un primo elemento, che chiamo r.

$r \in S \Rightarrow \exists q \in \mathbb{N}_0$ t.c. $r = a - q \cdot b$

$$\Rightarrow \boxed{a = q \cdot b + r}$$

Rimane da dimostrare che $0 \leq r < b$

- $r \geq 0$ per costruzione, perché $r \in S \subseteq \mathbb{N}_0$
- Se per assurdo $r \geq b$, allora $r - b \geq 0$ e inoltre:

$$r - b = a - qb - b = a - \underbrace{(q+1)}_{\in \mathbb{N}_0} b, \text{ cioè } r - b \in S$$

e quindi sarebbe un elemento di S minore del primo elemento $\lightning$

$\Rightarrow$ Necessariamente $r < b$.

Per l'unicità di q ed r.

Se esistono q' ed r' tali che $a = qb + r = q'b + r'$ $\quad 0 \leq r, r' < b$

allora $(q - q') \cdot b = r' - r$

Senza perdere di generalità se $q \neq q'$ posso supporre $q > q' \Rightarrow q - q' > 0$

$b \leq b(q - q') = r' - r < b$ $\lightning$

Necessariamente $q = q'$ (e quindi $r = r'$).

Criterio per sottogruppi

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

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

$$\left\{ \begin{array}{l} \text{Notazione} \\ \text{additiva} \\ (G,+) \end{array} \iff \forall x,y \in H \quad x-y \in H \right\}$$

Dim:

$\Rightarrow$ H sottogruppo, $x,y \in H \Rightarrow y^{-1} \in H \Rightarrow x\cdot y^{-1} \in H$. ✓

$\Leftarrow$ Supponiamo valga $\boxed{\forall x,y \in H : x\cdot y^{-1} \in H}$

- Se $H = \emptyset$ non c'è niente da dimostrare
- Se $H \neq \emptyset$ esiste almeno un elemento $x \in H$.

Applico ✪ alla coppia x e $y=x$:

$$x\cdot x^{-1} \in H, \text{ cioè } 1_G = x\cdot x^{-1} \in H$$

Ora applico la condizione ✪ alla coppia $x=1_G$ e $y=x$:

$$1_G \cdot x^{-1} \in H, \text{ cioè } x^{-1} \in H \; ✓$$

Infine siano $x,y \in H$. Applico ✪ alla coppia $x=x$ e $y=y^{-1}$:

$$x(y^{-1})^{-1} = \text{ cioè } x\cdot y \in H \; ✓ \quad \#$$

Caratterizzazione del sottogruppo ciclico generato da un elemento

Def: Siano $(G,\cdot)$ un gruppo, e $x \in G$ un elemento.

Il sottogruppo ciclico generato da x è il più piccolo sottogruppo di G che contiene l'elemento x.

Si denota $\langle x \rangle$.

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

<u>Prop</u>: 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:

$$\langle x \rangle \underset{\subseteq}{\overset{\supseteq}{=}} \{x^n \mid n \in \mathbb{Z}\}$$

dim: doppio contenimento:

$\supseteq$ ovvio per la proprietà di sottogruppo

$\subseteq$ Siccome per def $\langle x \rangle$ è il più piccolo sottogruppo di G che contiene x, se mostriamo che $\{x^n \mid n \in \mathbb{Z}\}$ è sottogruppo e contiene x,

$$x = x^1 \in \{x^n \mid n \in \mathbb{Z}\} \checkmark$$

Usiamo il criterio: siano $a = x^n$ e $b = x^m$. Allora $ab^{-1} = x^n$

Allora $ab^{-1} = x^n \cdot (x^m)^{-1} = x^{n-m} \in \{x^n \mid \dots\} \checkmark$ #

oss. i sottogruppi ciclici sono commutativi: $x^n \cdot x^m = x^{n+m} = x^{m+n} = x^m \cdot x^n$.

Caratterizzazione dei sottogruppi di $(\mathbb{Z}, +)$

__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 $K\mathbb{Z} = \langle K \rangle$)

dim:

- $K\mathbb{Z}$ è un sottogruppo

Sia $H \leq \mathbb{Z}$ sottogruppo:

- Se $H = \{0\} \Rightarrow H = 0\mathbb{Z}$ ✓
- Se $H \neq \{0\} \Rightarrow \exists z \neq 0 \quad z \in H$

Poiché H è un sottogruppo, $-z \in H$.

Uno tra z e $-z$ è positivo e quindi l'insieme

$$S = \{m \in H \mid m > 0\} \neq \emptyset$$

$$\left.\begin{array}{l} S \subseteq \mathbb{N} \\ S \neq \emptyset \end{array}\right\} \Rightarrow$$ per il buon ordinamento esiste un primo elemento

Sia $K = \min(S)$ il primo elemento. Voglio dim:

$$H \overset{\supseteq}{\underset{\subseteq}{=}} K\mathbb{Z}$$

$(\supseteq)$ $K \in H$, H sottogruppo, quindi tutti i multipli interi di K devono essere elementi di H. ✓

($\subseteq$) Sia $b \in H$. Poichè $K \neq 0$, possiamo usare la divisione euclidea e dividere b per K:

$\exists\, q, r$ tali che:

$$b = K \cdot q + r, \qquad 0 \leq r < K$$

$$r = \underset{H}{\underset{\cap}{b}} - \underset{H}{\underset{\cap}{Kq}} \in H$$

Siccome $r \in H$, se fosse $r \neq 0$ sarebbe un elemento di S più piccolo del primo elemento: assurdo $\lightning$

L'unica possibilità è $b = Kq \in K\mathbb{Z}$ ✓ #

Ogni gruppo ciclico è isomorfo a $\mathbb{Z}$ (se infinito) o a $\mathbb{Z}_n$ (se è finito) per qualche $n \in \mathbb{N}$

dim: CASO 1 $|G| = \infty$, $G = \langle x \rangle$

definiamo l'applicazione

$$\varphi : \mathbb{Z} \longrightarrow G$$
$$s \longmapsto x^s$$

- φ è omo: $\varphi(s+t) = x^{s+t} = x^s \cdot x^t = \varphi(s) \cdot \varphi(t)$
- φ è suriettivo per definizione di un gruppo ciclico
- φ è iniettivo. ($\Leftrightarrow Ker(\varphi) = \{0\}$)

$Ker(\varphi) = \{ s \in \mathbb{Z} \mid \varphi(s) = 1_G \} = \{ s \in \mathbb{Z} \mid x^s = 1_G \}$

Se esiste $m \neq 0$, $m \in Ker(\varphi)$, allora avrei $ord(x) = |G| < \infty$ ASSURDO $\Rightarrow Ker(\varphi) = \{0\}$ ✓

CASO 2: $|G| = n < \infty$, cioè $G = \{x^0, \dots, x^{n-1}\}$ $ord(x) = n$

Definiamo l'applicazione $\psi : \mathbb{Z}_n \to G$ $\quad [s]_n = \bar{s}$

$$\bar{s} \to x^s$$

- ψ è ben definita: $t \in \bar{s}$, allora $t = qn + s$ e quindi

$$\psi(\bar{t}) = x^t = x^{qn+s} = \underbrace{(x^n)^q}_{1_G} \cdot x^s = x^s = \psi(\bar{s})$$

- ψ è omo per la proprietà delle potenze come prima
- ψ è suriettivo per definizione di G.

• Ψ è iniettivo:

$$\mathrm{Ker}(\Psi) = \{\bar{s} \in \mathbb{Z}_n \mid \Psi(\bar{s}) = 1_G\} = \{\bar{s} \in \mathbb{Z}_n \mid x^s = 1_G\}$$

$$= \{\bar{s} \in \mathbb{Z}_n \mid s = q \cdot n\} = \{\bar{0}\}$$

↳ Per quanto visto prima: $x^s = 1_G \Leftrightarrow s = q \cdot n,\ q \in \mathbb{Z}$.

#

Gruppo simmetrico: decomposizione delle permutazioni in cicli e trasposizioni

Ogni permutazione può essere decomposta in un prodotto di trasposizioni

dim: è sufficiente dimostrarlo per i cicli:

$$(a_1 a_2 a_3 \dots a_{k-1} a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_3)(a_1 a_2).$$

Continua sul foglio 4

Teorema di Cailey

Ogni gruppo è isomorfo a un gruppo di permutazioni sui ~~soi~~ suoi elementi.

<u>oss.</u> G gruppo

$\mathrm{Sym}(G)$ = gruppo delle permutazioni degli elementi dell'insieme G, dotato della composizione.

dim: vogliamo dimostrare che G è isomorfo a un sottogruppo di $\mathrm{Sym}(G)$

Sia $(G, \cdot)$ un gruppo. Costruiamo esplicitamente un monomorfismo

$\lambda: G \hookrightarrow \mathrm{Sym}(G)$, in modo che $G \cong \mathrm{Im}(\lambda) \leq \mathrm{Sym}(G)$ ✓

$\forall\, a \in G$ definiamo $\lambda_a: G \to G$

$g \to ag$

e osserviamo che λ_a è una biezione, cioè un elemento di $\mathrm{Sym}(G)$, perché ha un'inversa:

$(\lambda_a)^{-1} = \lambda_{a^{-1}}$

$(\lambda_a \circ \lambda_{a^{-1}})(g) = \lambda_a(\lambda_{a^{-1}}(g)) = \lambda_a \cdot a^{-1} \cdot g = a \cdot a^{-1} \cdot g = g$

Quindi l'applicazione $\lambda: G \to \mathrm{Sym}(G)$

$a \to \lambda_a = \lambda(a)$

è ben definita

• λ è omomorfismo: $\lambda_{ab} = \lambda_a \circ \lambda_b \quad \lambda(ab) = \lambda(a) \circ \lambda(b)$

Sia $g \in G$ elem. qualsiasi. Calcoliamo

$$\lambda_{ab}(g) \stackrel{?}{=} (\lambda_a \circ \lambda_b)(g)$$

$$\lambda_{ab}(g) = (ab)g \qquad (\lambda_a \circ \lambda_b)(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg)$$

$$(ab)g = a(bg) \quad \checkmark$$

- λ è iniettiva

$\lambda_a = \lambda_b$ significa che $\forall g \in G \;\; \lambda_a(g) = \lambda_b(g)$

cioè $\forall g \in G \;\; ag = bg \implies a = b$ ✓ ⋕

<u>Corollario</u> se $|G| = n < \infty$, allora G è isomorfo a un sottogruppo di S_n.

Teorema di Lagrange

G gruppo finito, $H \leq G$ sottogruppo, allora:

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

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

dim: Se mostriamo che le classi laterali hanno tutte lo stesso ordine, poiché formano una partizione:

$$|G| = |H| \cdot [G:H] \quad \checkmark$$

Infatti dimostriamo che:

$$|aH| = |Ha| = |H|$$

Perché l'applicazione $g: H \to aH$, $h \to ah$ è biettiva

(e similmente per l'applicazione $g': H \to Ha$, $h \to ha$)

- Iniettiva: siano $h_1, h_2 \in H$ t.c. $g(h_1) = g(h_2)$ (x legge di cancellazione)

$$ah_1 = ah_2 \implies h_1 = h_2 \quad \checkmark$$

- Suriettiva: un elemento $ah \in aH$ è immagine di $h \in H$ $\;\; g(h) = ah$ ⋕

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

dim: $\sigma \in S_n$, $a \in I_n$

$a, \sigma(a), \sigma^2(a) = \sigma(\sigma(a)), \dots, \sigma^K(a) = a$

- $K = n$ significa che σ è un ciclo di lunghezza n: $\sigma = (a\,\sigma(a), \sigma^2(a), \dots, \sigma^{K-1}(a))$
- $K < n$ significa che $\exists\, b \in I_n$ tale che $b \neq \sigma^i(a)\ \forall i$.

Calcoliamo $b, \sigma(b), \sigma^2(b), \dots, \sigma^h(b) = b$

- $K+h = n$ cioè $\sigma = (a\,\sigma(a) \dots \sigma^{K-1}(a))(b\,\sigma(b) \dots \sigma^{h-1}(b))$
- $K+h < n$ cioè $\exists\, c \in I_n$ tale che $c \neq \sigma^i(a)$ e $c \neq \sigma^j(b)$

ripeto il ragionamento su c, e procedo così fino a deconponimento σ in un prodotto di cicli, che sono disgiunti per costruzione.
Sempre per costruzione, la decomposizione è unica a meno dell'ordine dei fattori. ※

Teorema fondamentale di omomorfismi per gruppi

Sia $\varphi: G \to G'$ omomorfismi di gruppi e sia $K = Ker(\varphi)$.
Sia 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 $G/K \cong Im(\varphi)$

dim:
- definire $\overline{\varphi}$
- buona def.
- $\overline{\varphi} \circ \pi = \varphi$
- $\overline{\varphi}$ omomorfismo
- $\overline{\varphi}$ iniettivo.

- definiamo $\overline{\varphi}: G/K \longrightarrow G'$

$$aK \longrightarrow \varphi(a)$$

- mostriamo che è ben definita:

Sia $a' \in aK$ (cioè $a'K = aK$). Allora $\exists h \in K$ t.c. $a' = ah$

$$\overline{\varphi}(a'K) = \varphi(a') = \varphi(ah) = \varphi(a)\cdot\varphi(h)$$
$$= \varphi(a)\cdot 1_{G'} = \varphi(a) = \overline{\varphi}(aK)$$

- $\overline{\varphi} \circ \pi = \varphi$

Sia $a \in G$

$$\begin{tikzcd} a \arrow[r, mapsto] \arrow[d, mapsto] & \varphi(a) \\ aK \arrow[ur, mapsto] & \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r] \arrow[d, "\pi"'] & G' \\ G/K \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

$\varphi(a) = \varphi(a)$

- dati $aK, bK \in G/K$, allora

$$\overline{\varphi}((aK)(bK)) = \overline{\varphi}(abK) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aK)\overline{\varphi}(bK) \quad \checkmark$$

per def di gruppo quoziente; Per def di $\overline{\varphi}$; φ è omo

- iniettività

$$Ker(\overline{\varphi}) = \{ aK \in G/K \mid \overline{\varphi}(aK) = 1_{G'} \}$$
$$= \{ aK \in G/K \mid \varphi(a) = 1_{G'} \} = Ker(\varphi) = K = 1_{G/K} \quad \#$$

Morfismo unitano per anelli di caratteristica 0 e positività

Se A è un anello con $char(A) = 0$, allora l'omomorfismo unitano μ è iniettivo.

Se invece $char(A) = K > 0$. Allora $Ker(\mu) = K\mathbb{Z}$.

dim: $Ker(\mu) = \{ n \in \mathbb{Z} \mid \mu(n) = 0_A \} = \{ n \in \mathbb{Z} \mid n 1_A = 0_A \}$.

Se $char(A) = 0 \Rightarrow$ l'unico $n \in \mathbb{Z}$ t.c. $n 1_A = 0_A$ è $n = 0$, cioè $Ker(\mu) = \{0\}$ cioè μ è iniettivo.

Se $char(A) = K > 0$ significa che K è il minimo intero t.c. $K 1_A = 0_A$

Quindi sicuramente $Ker(\mu) = \{0, K, \dots, ?\}$

Sia $n \in Ker(\mu)$. Dividiamo n per K. $\exists q, r$ tali che $n = Kq + r$ $0 \leq r < K$

$r \cdot 1_A = ?$

$$r = n - Kq \Rightarrow r \cdot 1_A = (n - Kq) \cdot 1_A = \underbrace{n \cdot 1_A}_{\substack{= 0_A \\ \text{perché } n \in Ker}} - \underbrace{Kq \cdot 1_A}_{= q(K \cdot 1_A) = 0_A} = 0_A$$

Quindi necessariamente $r = 0$, altrimenti sarebbe un intero positivo t.c.

$r \cdot 1_A = 0_A$ più piccolo di $K = ord(1_A)$

$\Rightarrow n = Kq$, cioè $n \in K\mathbb{Z}$

$\Rightarrow Ker(\mu) \subseteq K\mathbb{Z}$
$\supseteq$ ovvio #

Formula 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 $-d$.

<u>dim</u>: a, b non entrambi nulli $\Rightarrow \underbrace{a^2 + b^2}_{a \cdot a + b \cdot b} > 0$

Quindi se definiamo l'insieme:

$S = \{ s \in \mathbb{N} \mid s = ax + by \text{ per qualche } x, y \in \mathbb{Z} \}$

$S \neq \emptyset$.

Per il buon ordinamento $\exists d = \min(S)$.

Mostriamo che d è un MCD di a e b.

$d \in S \Rightarrow \exists \alpha, \beta$ t.c. $\boxed{d = a \cdot \alpha + b \cdot \beta}$ ✓

- $d \mid a$
- $d \mid b$
- Se $x \mid a$ e $x \mid b \Rightarrow x \mid d$
- Per la divisione euclidea, $\exists q, r$ t.c. $a = q \cdot d + r$ $0 \leq r < d$

$r = a - q \cdot d = a - q(a\alpha + b\beta) = a\underbrace{(1 - q\alpha)}_{\in \mathbb{N}} + b\underbrace{(-q\beta)}_{\in \mathbb{N}}$.

quindi se $r \neq 0$ troviamo una contraddizione perché r sarebbe un elemento di S minore del primo elemento.

$\Rightarrow r=0$, cioè $a = q \cdot d$, $d \mid a$.

- $d \mid b$ si fa nello stesso modo.
- Sia x un divisore comune di a e b.

Allora
$$\left.\begin{array}{l} x \mid a \Rightarrow x \mid a\cdot\alpha \\ x \mid b \Rightarrow x \mid b\cdot\beta \end{array}\right] \Rightarrow x \mid \underbrace{a\cdot\alpha + b\cdot\beta}_{d}$$

(ii) Sia d' un altro $MCD(a,b)$. Per definizione:

$$d' \mid a,\ d' \mid b \underset{d \text{ è } MCD}{\Rightarrow} d' \mid d \Rightarrow d = d'x$$

$$d \mid a,\ d \mid b \underset{d' \text{ è } MCD}{\Rightarrow} d \mid d' = d' = d\cdot y$$

$$d = d'x = (dy)\cdot x \Rightarrow d = d(x\cdot y)$$

Siccome siamo in un dominio di integrità:

$$x\cdot y = 1 \begin{cases} x=y=1 \Rightarrow d=d' \\ x=y=-1 \Rightarrow d=-d' \end{cases}$$

$\#$

Teorema cinese dei resti

Formulazione astratta

Siano $m_1, m_2, m_3, \dots, m_s \in \mathbb{N}$ a due a due coprimi e sia $n = m_1 m_2 \dots m_s$ il loro prodotto.

Allora l'applicazione

$$\Gamma: \mathbb{Z}_n \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_s}$$
$$[a]_n \mapsto ([a]_{m_1}, [a]_{m_2}, \dots, [a]_{m_s})$$

è biettiva.

es: $m_1 = 2$, $m_2 = 3$, $n=6$

$$\mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$$
$$[0] \mapsto ([0]_2, [0]_3)$$
$$\vdots$$
$$[3]_6 \rightarrow ([1]_2, [0]_3)$$
$$\vdots$$

dim: • ben definita
• iniettiva
• suriettiva

Ben definita

• Siano $a,b \in \mathbb{Z}$ tali che $[a]_n = [b]_n$

$\Rightarrow [a-b]_n = [0]_n$

$\Rightarrow n \mid a-b \ , \ n = m_1 \cdot m_2 \cdot \ldots \cdot m_s$

$\Rightarrow m_i \mid a-b \ \forall i \Rightarrow [a-b]_{mi} = [0]_{mi} \ \forall i$

$\Rightarrow [a]_{mi} = [b]_{mi} \ \forall i \Rightarrow \Gamma([a]_n) = \Gamma([b]_n)$ ✓

• Iniettività

Siano $a,b \in \mathbb{Z}$ t.c. $\Gamma([a]_n) = \Gamma([b]_n)$

$$([a]_{m_1}, [a]_{m_2}, \ldots [a]_{m_s}) = ([b]_{m_1}, [b]_{m_2}, \ldots, [b]_{m_s})$$

$\Rightarrow [a]_{mi} = [b]_{mi} \ \forall i = 1, \ldots, s$

$\Rightarrow m_i \mid a-b \ \forall i = 1, \ldots, s$

Poichè gli mi sono a 2 a 2 coprimi, questo implica che $n = m_1 \ldots m_s \mid a-b$.

$\Rightarrow [a]_n = [b]_n$, Γ iniettiva ✓

• Suriettività è "gratis"

$|\mathbb{Z}_n| = n$

$|\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_s}| = m_1 \cdot m_2 \cdot \ldots \cdot m_s = n$

Cioè Γ è un applicazione iniettiva tra insiemi finiti con la ~~classe~~ stessa cardinalità è anche suriettiva. #

2 Formulazione

TEOREMA: Siano m_1 e $m_2 \geq 1$ due interi coprimi.

Allora per ~~ogni~~ ogni coppia $a,b \in \mathbb{Z}$ il sistema di congruenze

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

ammette sempre soluzioni.

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

i) I è primo $\Leftrightarrow A/I$ è dominio di integrità.

ii) I è massimale $\Leftrightarrow A/I$ è un campo.

OSS: 1) Questo fornisce una seconda dim. del fatto che max $\Rightarrow$ primo

2) Corollario quasi immediato il fatto che A PID $\Leftrightarrow (0)$ è primo.

dim: A/I anello commutativo

$$0_{A/I} = 0_A + I = I \qquad 1_{A/I} = 1_A + I$$

i) A/I dominio di integrità

$\Leftrightarrow \forall a,b \in A$, se $(a+I)(b+I) = 0_{A/I} = I$
allora o $a+I = I$, oppure $b+I = I$

$\Leftrightarrow \forall a,b \in A$ se $ab + I = I$
allora o $a+I = I$ oppure $b+I = I$

$\Leftrightarrow \forall a,b \in A$, se $ab \in I$
allora o $a \in I$ oppure $b \in I$

$\Leftrightarrow I$ è primo.

ii) I max $\Leftrightarrow A/I$ campo

($\Leftarrow$) ipotesi: A/I campo. Sia J un ideale tale che:

$$I \subseteq J \subseteq A$$

$\to I = J$

$\to I \subsetneq J$, quindi $\exists K \in J \setminus I$

Allora la classe laterale di K in A/I:

$$I + K \neq I = 0_{A/I}$$

Cioè $I+K$ è un elemento non nullo in A/I campo.

Quindi esiste l'inverso di $I+K$ in A/I.

$\exists\ I + h$ tale che $(I+h)(I+K) = 1_{A/I} = I + 1_A$

$\Rightarrow 1_A \in I + hK$

Cioè $\exists\ i \in I$ tale che possiamo scrivere

$$1_A = \underset{\in I}{i} + \underset{\in J}{hK} \in J \Rightarrow J = A$$

$|\Rightarrow|$ ipotesi: I è max. Sia $I+K \in A/I$ un elemento non nullo.

$$I+K \neq I = 0_{A/I}$$

Cioè l'elemento $K \notin I$.

Quindi l'ideale somma $I+(K)$ è tale che

$$I \subsetneq I+(K) \subseteq A$$

I massimali $\Rightarrow I+(K) = A$

In particolare, $1_A \in I+(K)$ cioè $\exists\ i \in I$ e $h \in A$

tali che $\quad 1_A = i + hK$

Quindi la classe laterale $(I+1_A) = I+(i+hK) = I + hK = (I+h)(I+K)$.

$\Rightarrow I+h = (I+K)^{-1}$ nell'anello A/I che quindi è un campo. #

{Teorema: No!!!

Siano K campo, $g(x) \in K[x]$ un polinomio. Allora per ogni $f(x) \in K[x]$, esistono $q(x)$ (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:

dim: (i) esistenza

(ii) unicità

(i) Sia $g(x) = \sum_{i=0}^{n} a_i x^i$

$f(x) = \sum_{i=0}^{m} b_i x^i$

- $f=0 \Rightarrow f = 0 \cdot g + 0$ ✓

- $f \neq 0$: procediamo per induzione $m = \deg(f)$.

$\boxed{m=0}$ passo base dell'induzione

$f(x) = b_0$

- se $n = \deg(g) \geq 1 \Rightarrow f = 0 \cdot g + f = 0\,g(x) + b_0 \rightarrow$ resto che ha grado $0 < n = \deg(g)$.
- se $n = \deg(g) = 0$ cioè $g(x) = a_0 \in K$

$$\Rightarrow f = \underbrace{a_0}_{g} \cdot \underbrace{(a_0^{-1} \cdot b_0)}_{q} + \underbrace{0}_{r} \qquad \deg(r) = -\infty < \underset{\overset{\|}{1}}{\deg(g)}$$

Prop: K campo $\Rightarrow$ PID $K[x]$

dim: $I \subseteq K[x]$ ideale

- $I = \{0_K\} = (0_K)$ è principale
- $I \neq \{0\}_K$ quindi I contiene almeno un elemento non nullo.

Definiamo quindi
$$n := \min \{\deg(g) \mid g \neq 0, g \in I\}$$

Scegliamo in I l'elemento $f(x)$ di grado n.

Mostriamo che $I = (g(x))$

$(\supseteq)$ $(f(x)) = \{p(x) \cdot f(x) \mid p(x) \in K[x]\}$

$\Rightarrow$ poiché $f(x) \in I \Rightarrow (g) \subseteq I$

$(\subseteq)$ Sia $\alpha(x) \in I$ qualsiasi.

Vogliamo dim $\alpha = q \cdot f$.

Dividiamo $\alpha(x)$ per $f(x)$: $\exists\, q(x), r(x)$ tali che
$$\alpha(x) = f(x) \cdot q(x) + r(x)$$

Con o $r(x) = 0$, oppure $\deg(r) < \deg(f)$.

- Se $r(x) = 0$ ✓
- Se $r(x) \neq 0$, troviamo una contraddizione: $r(x) = \underset{\in I}{\alpha(x)} - \underbrace{f(x) \cdot q(x)}_{\in I} \in I$

Perché $r(x)$ sarebbe un elemento di I di grado $\deg(r) < n =$ minimo. #

Teorema di Ruffini

Sia $f(x) \in K[x]$. Un elemento $a \in K$ è radice di f se e solo se $(x-a)$ divide $f(x)$.
$$[f(a) = 0 \iff (x-a) \mid f]$$

dim: $(\Leftarrow)$ Se $x-a \mid f$, significa che $\exists\, g(x)$ tale che
$$f(x) = (x-a) \cdot g(x)$$
$$f(a) = (a-a) \cdot g(a) = 0 \ ✓$$

$(\Rightarrow)$ Supponiamo che $f(a) = 0$ e dividiamo $f(x)$ per $(x-a)$: $\exists\, q(x), r(x)$ t.c.
$$\boxed{f(x) = (x-a) \cdot q(x) + r(x)}$$

dove o $r(x) = 0$ ✓

oppure $\deg(r(x)) < \deg(x-a) = 1$ cioè $r(x) = r_0$ costante. Per capire chi è la costante

r_0 valutiamo $r(x)$ in a:

$$r_0 = r(x) = f(x) - (x-a)\cdot q(x)$$

$$r_0 = r(a) = \underset{\overset{||}{0}}{f(a)} - \underbrace{(a-a)\cdot q(a)}_{0} = 0$$

✓ #

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

$$\varphi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$
$$f(x) \longrightarrow \overline{f(x)}$$

dove se $f(x) = a_0 + a_1 x + \dots + a_n x^n$ con $\overline{f(x)}$ denotiamo il polinomio

$$\overline{f(x)} = \overline{a_0} + \overline{a_1}x + \overline{a_2}x^2 + \dots + \overline{a_n}x^n$$

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

→ Dim: controlliamo che φ_p è omomorfismo di anelli unitari.

Siano $f(x), g(x) \in \mathbb{Z}[x]$

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

$$g(x) = \sum_{i=0}^{m} b_i x^i$$

Supponiamo $m \geq n$

$$\Rightarrow \overline{f(x)+g(x)} = \sum_{i=0}^{m} (\overline{a_i + b_i})\, x^i$$
$$= \sum_{i=0}^{n} \overline{a_i}\, x^i + \sum_{i=0}^{m} \overline{b_i} x^i = \overline{f(x)} + \overline{g(x)}$$

$$\overline{f(x)\cdot g(x)} = \sum_{h=0}^{n+m} \Big(\sum_{i+j=h} \overline{a_i b_j} \Big) x^h = \sum_{h=0}^{n+m} \Big(\sum_{i+j=h} \overline{a_i}\cdot\overline{b_j} \Big)\cdot x^h = \overline{f(x)}\cdot\overline{g(x)}$$

e chiaramente la riduzione modulo p del polinomio costante 1 è $\overline{1}$.

#

Lemma di Gauss.

Il prodotto di polinomi primitivi è primitivo.

dim: Siano $f(x), g(x) \in \mathbb{Z}[x]$ polinomi primitivi.

Supponiamo per assurdo che il prodotto $f(x)\cdot g(x)$ non sia primitivo.

Quindi $\exists$ un primo $p \in \mathbb{Z}$ che divide tutti i coefficienti di $f(x)\cdot g(x)$.

Se prendiamo la riduzione modulo p del prodotto $f \cdot g$ abbiamo:

$$\overline{0} \overset{1}{=} \overline{f\cdot g} = \overline{f}\cdot\overline{g}$$

Perchè p divide tutti i coefficienti di $f \cdot g$

Perchè la riduzione è omo.

Poichè f è primitivo, $\bar{f} \neq \bar{0}$ $\forall p \in \mathbb{Z}$ è similmente $\bar{g} \neq \bar{0}$ $\forall p \in \mathbb{Z}$.
Quindi abbiamo in $\mathbb{Z}_p[x]$ dominio di integrità 2 elementi $\neq \bar{0}$ il cui prodotto è $\bar{0}$ $\Rightarrow$ ASSURDO ⋇

Teorema: Sia $F|K$ un'estensione di campi, ~~se~~ e $s \in F$ un elemento.
i) l'elemento s è algebrico $\Leftrightarrow K[s] = K(s)$
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.

dim: poichè per $s=0$ non c'è nulla da dimostrare
quindi supponiamo $s \neq 0$.
i) L'elemento s è algebrico $\Leftrightarrow K[s] = K(s)$
($\Leftarrow$) $\frac{1}{s} \in K(s) = K[s] \Rightarrow \exists\, a_0, a_1, \dots, a_n \in K$ tali che

$$\frac{1}{s} = a_0 + a_1 \cdot s + a_2 s^2 + \dots + a_n s^n$$

$$1 = a_0 s + a_1 s^2 + a_2 s^3 + \dots + a_n s^{n+1}$$

$\Rightarrow s$ è radice del polinomio

$$g(x) = a_n x^{n+1} + \dots + a_1 x^2 + a_0 x - 1 \quad ✓$$

($\Rightarrow$) Sia $p(x)$ il polinomio minimo di s su K, e sia $I = (p(x))$.
Sia $\frac{\alpha(s)}{\beta(s)} \in K(s)$. Osserviamo che il fatto che $\beta(s) \neq 0$ significa che $\beta(x) \notin I$ e quindi $p(x) \nmid \beta(x)$.
Poichè $p(x)$ è irriducibile, se $p \nmid \beta$ allora $MCD(p(x), \beta(x)) = 1$.
Per Bezout $\exists\, r(x), t(x) \in K[x]$ t.c.

$$1 = r(x) \cdot p(x) + t(x) \cdot \beta(x)$$

Valutiamo questa uguaglianza in $x = s$

$$1 = r(s) \cancel{p(s)} + t(s) \cdot \beta(s)$$

$$\Rightarrow 1 = t(s) \cdot \beta(s) \Rightarrow \frac{1}{\beta(s)} = t(s) \Rightarrow \frac{\alpha(s)}{\beta(s)} = \alpha(s) \cdot t(s) \in K[s] \quad ✓$$

ii) Sia $u(x) \in K[x]$ e $u(s) \in K[s]$ la sua valutazione in s.
Dividiamo il polinomio $u(x)$ per il polinomio minimo $p(x)$: $\exists\, q(x), r(x) \in K[x]$ t.c.

$$u(x) = p(x) \cdot q(x) + r(x).$$

Con o $r(x) = 0$, oppure $\deg(r) < \deg(p)$.

Valutiamo l'uguaglianza in $X=S$ $\quad u(s) = p(s)\cancel{q}(s) + r(s)$

Quindi $u(s) = r(s)$ ha grado $n = \deg(p)$

Per unicità, osserviamo che se: $u(s) = v(s)$ con $u(x), v(x) \in K[x]$ di grado $< n$, allora

$u(s) - v(s) = 0$

$\Rightarrow u(x) - v(x) \in I$ quindi se $u(x) - v(x)$ fosse $\neq 0$ sarebbe un elemento

di I di grado $<$ grado del generatore ↯

$\Rightarrow u(x) = v(x)$ ✓

⋇

Prop K campo finito. Il gruppo moltiplicativo $G = K^*$ è ciclico.

dim: Sia $l = |G| = |K^*| < \infty$

Per dim G ciclico dobbiamo trovare un elemento di ordine l.

Sia $m = \mathrm{mcm}(\mathrm{ord}(a) \mid a \in G)$

Allora $a^l = 1 \ \forall a \in G \Rightarrow \mathrm{ord}(a) \mid l \ \forall a \in G \Rightarrow m \leq l$.

D'altra parte, l'equazione $x^m - 1 = 0$ ha al massimo m soluzioni, e tutti gli elementi di G sono soluzioni.

Allora $m \geq l$

In totale quindi $|G| = l = m = \mathrm{mcm}(\mathrm{ord}(a) \mid a \in G)$

applicando il Lemma $\Rightarrow$ ✓ ⋇.

Lemma: A gruppo commutativo. Se $a_1, a_2, \dots, a_h \in A$ hanno ordine $\mathrm{ord}(a_i) = m_i$, e se $m = \mathrm{mcm}(m_1, \dots, m_h)$, allora $\exists$siste un elemento $b \in A$ t.c. $\mathrm{ord}(b) = m$.