Universita' degli Studi di Roma "Tor Vergata"
Laurea Triennale in Matematica - a.a. 2024/2025
Corso: Algebra 1
Docente: Prof.ssa I. Damiani, Codocente: Prof. F. Flamini

Esercitazioni/Tutorati 12-13 (26-27 Maggio 2025) - Prof. F. Flamini

Esercizio 1. Sia $\mathbb{Z}[i]$ l'**anello degli interi di Gauss**

(i) Dopo aver ricordato che $\mathbb{Z}[i]$ é **dominio euclideo**, dati $\alpha := 14-3i$, $\beta := 4+7i \in \mathbb{Z}[i]$, determinare MCD($\alpha$, β) e descrivere un'identità di Bezout per esso.

(ii) Dimostrare che l'ideale $I := (3) \subset \mathbb{Z}[i]$ é primo (equiv. massimale); dedurre che l'anello quoziente $\frac{\mathbb{Z}[i]}{I}$ é un campo $\mathbb{K}$ e se ne determini la cardinalitá e l'inverso in $\mathbb{K}$ dell'elemento $[2+i] := 2+i+I \in \mathbb{K}$.

(iii) Dimostrare che il campo $\mathbb{K}$ determinato al punto (ii) é isomorfo al campo $\mathbb{H} := \frac{(\mathbb{Z}/3\mathbb{Z})[x]}{(x^2+\overline{1})}$, con $x^2+\overline{1}$ polinomio irriducibile nell'anello euclideo $(\mathbb{Z}/3\mathbb{Z})[x]$.

(iv) Dato $a+bi := 3+i \in \mathbb{Z}[i]$, utilizzando che MCD$(a,b)$ = MCD$(3,1) = 1$ in $\mathbb{Z}$, stabilire che l'anello quoziente $\frac{\mathbb{Z}[i]}{(3+i)}$ é isomorfo all'anello quoziente $\mathbb{Z}/10\mathbb{Z}$, e dunque non é un dominio di integritá

(v) Dedurre che la procedura utilizzata per risolvere il punto (iv) si estende piú generalmente al seguente enunciato:
Dato $a+bi \in \mathbb{Z}[i]$ con MCD$(a,b) = 1$ *in $\mathbb{Z}$, i.e. a e b interi* **coprimi**, *l'anello quoziente $\frac{\mathbb{Z}[i]}{(a+ib)}$ é isomorfo all'anello quoziente $\mathbb{Z}/(a^2+b^2)\mathbb{Z}$, e pertanto é un campo se e solo se la* **valutazione** *dell'elemento $a+bi \in \mathbb{Z}[i]$ é un numero primo $p \in \mathbb{N}$.*

Esercizio 2. Si consideri il dominio euclideo $\mathbb{Z}$.
(i) Consideriamo $\mathbb{Z}[\frac{1}{2}] \subset \mathbb{Q}$ il minimo sottoanello di $\mathbb{Q}$ che contenga $\mathbb{Z}$ e $\{\frac{1}{2}\}$. Verificare che $\mathbb{Z}[\frac{1}{2}]$ é un **dominio euclideo**. Dedurre infine che **si arriva alla stessa conclusione** se si sostituisce 2 con un qualsiasi $a \in \mathbb{Z} \setminus \{0\}$ e si considera l'anello $\mathbb{Z}[\frac{1}{a}] \subset \mathbb{Q}$ (ritrovando $\mathbb{Z}$ se e solo se $a = \pm 1$).

(ii) Consideriamo $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ il minimo sottoanello di $\mathbb{R}$ che contenga $\mathbb{Z}$ e $\{\sqrt{2}\}$. Verificare che $\mathbb{Z}[\sqrt{2}]$ é un **dominio euclideo**. Osservare che, a differenza del caso (i), **non si arriva alla stessa conclusione** se si sostituisce 2 con un qualsiasi $a \in \mathbb{N} \setminus \{0\}$ e si considera l'anello $\mathbb{Z}[\sqrt{a}] \subset \mathbb{R}$, verificando ad esempio che $\mathbb{Z}[\sqrt{10}]$ non é **DFU** (quindi non puó essere euclideo) dimostrando che $10 \in \mathbb{Z}[\sqrt{10}]$ ha due fattorizzazioni non banali distinte in irriducibili.

(iii) Consideriamo $\mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$ il minimo sottoanello di $\mathbb{C}$ che contenga $\mathbb{Z}$ e l'insieme $\{\sqrt{-2} = i\sqrt{2}\}$. Verificare che $\mathbb{Z}[\sqrt{-2}]$ é un **dominio euclideo**. Osservare che, a differenza del caso (i), **non si arriva alla stessa conclusione** se si sostituisce 2 con un qualsiasi $a \in \mathbb{N} \setminus \{0\}$ e si considera l'anello $\mathbb{Z}[\sqrt{-a}] \subset \mathbb{C}$, verificando ad esempio che $\mathbb{Z}[\sqrt{-3}]$ non é **DFU** (quindi non puó essere euclideo) dimostrando che $1+\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ é un elemento **irriducibile** ma **non primo**.

(iii) Dedurre da (ii) e dal fatto che (x_0, y_0) é soluzione intera di $f(x,y)$, che allora gli elementi x_0+i, $x_0-i \in \mathbb{Z}[i]$ sono **cubi** in $\mathbb{Z}[i]$, i.e. esistono $\alpha := a+ib, \beta := a'+ib' \in \mathbb{Z}[i]$ tale che $x_0+i = \alpha^3$, $x_0 - i = \beta^3$.

(iv) Dedurre da (iii) che $f(x,y)$ ha come unica soluzione intera $(x_0, y_0) = (0,1)$ (equivalentemente l'unico punto P a coordinate intere su C é $P = (0,1)$).

Esercizio 5. (i) Si consideri il dominio euclideo $(\mathbb{Z}, +, \cdot)$ e l'anello **prodotto diretto** $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ con

$$(m,n) + (m',n') := (m+m', n+n') \text{ e } (m,n) \cdot (m'+n') := (m \cdot m', n \cdot n').$$

Dopo aver verificato che $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ é commutativo, unitario ma non é dominio di integritá, determinare (a meno di isomorfismo) la struttura del **gruppo degli automorfismi di anello** (i.e. omomorfismi dell'anello $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ che sono iniettivi e suirettivi)

$$(Aut(\mathbb{Z} \times \mathbb{Z}, +, \cdot), \circ),$$

dove l'operazione di gruppo $\circ$ é la composizione di automorfismi.

(ii) Si consideri il gruppo abeliano ciclico $(\mathbb{Z}, +)$ ed il gruppo additivo **prodotto diretto** $(\mathbb{Z} \times \mathbb{Z}, +)$ con

$$(m,n) + (m',n') := (m+m', n+n').$$

Dopo aver verificato che $(\mathbb{Z} \times \mathbb{Z}, +)$ é abeliano, determinare (a meno di isomorfismo) la struttura del **gruppo degli automorfismi di gruppo** (i.e. omomorfismi del gruppo abeliano $(\mathbb{Z} \times \mathbb{Z}, +)$ che sono iniettivi e suirettivi)

$$(Aut(\mathbb{Z} \times \mathbb{Z}, +), \circ),$$

dove l'operazione di gruppo $\circ$ é la composizione di automorfismi.

Esercizio 6. Per i seguenti gruppi sotto elencati, determinare la loro cardinalitá, stabilire se sono gruppi ciclici o meno, ed in caso di risposta affermativa determinare tutti i loro generatori, descrivere tutti i loro sottogruppi stabilendo se essi sono ciclici o meno, determinare infine la struttura (a meno di isomorfismi) del gruppo dato e di tutti i suoi sottogruppi.

(i) $U(\mathbb{Z}/8\mathbb{Z})$= gruppo moltiplicativo degli elementi invertibili nell'anello $(\mathbb{Z}/8\mathbb{Z}, +, \cdot)$: ha cardinalitá 4, non é ciclico, é isomorfo al gruppo additivo prodotto diretto $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ detto **gruppo di Klein**; dedurre un isomorfismo di esso con il **gruppo delle simmetrie di un quadrato** o con il **sottogruppo** di $S_4 = Sym(4)$ formato dalle permutazioni

$$U(\mathbb{Z}/8\mathbb{Z}) \simeq \{Id_{S_4}, (1,4)(2,3), (1,2)(3,4), (1,3),(2,4)\}.$$

Infine $U(\mathbb{Z}/8\mathbb{Z})$ ammette come sottogruppi propri non banali tre sottogruppi ciclici di ordine (o cardinalitá) 2.

(ii) $U(\mathbb{Z}/9\mathbb{Z})$= gruppo moltiplicativo degli elementi invertibili nell'anello $(\mathbb{Z}/9\mathbb{Z}, +, \cdot)$: ha cardinalitá 6, é ciclico, é isomorfo al gruppo additivo $(\mathbb{Z}/6\mathbb{Z}, +)$ ed il Teorema di Lagrange **si inverte con unicitá e ciclicitá**, in altri termini per ogni divisore k di $6 = |U(\mathbb{Z}/9\mathbb{Z})|$ esiste ed é unico il sottogruppo $H_k < U(\mathbb{Z}/9\mathbb{Z})$ di cardinalitá $|H_k| = k$ ed inoltre ciascun H_k é sottogruppo ciclico.

Svolgimento Esercizio 1

(i) Ricordo $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z},\ i^2=-1\} \subset \mathbb{C}$ interi di Gauss

dominio euclideo (comm. unitario integro con valutazione
$\nu: \mathbb{Z}[i]\setminus\{0\} \longrightarrow \mathbb{N}$
$a+ib \longrightarrow \|a+ib\| = a^2+b^2$
↓ ereditata da $\mathbb{C}$)

Ricordo che per essere valutazione su D dominio integro

$\forall a \neq 0$ in D
(i) $\nu(a) \leq \nu(a\cdot b)$, $\forall a,b \in D\setminus\{0\}$
(ii) $\forall a,b \in D$ t.c. $b \neq 0$, $\exists\ q, r \in D$ t.c.
$a = b\cdot q + r$ con $r=0$ oppure $\nu(r)<\nu(b)$

$\Rightarrow (D,\nu)$ si dice DOMINIO EUCLIDEO

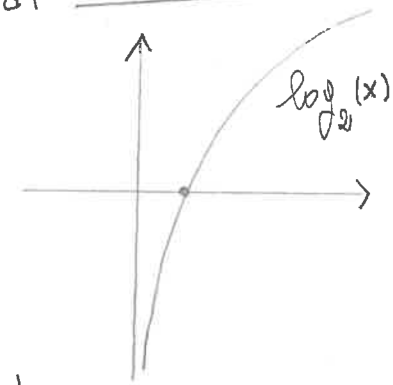
Oss: Possono $\exists$ più valutazioni su un medesimo D che lo rendano euclideo

E.g.

(1) $D = \mathbb{K}$ campo, $\forall a \in \mathbb{K}\setminus\{0\}$ $\nu(a):=1$ lo rende euclideo
$\nu(a):=2$ lo rende euclideo

(2) $D = \mathbb{Z}$ dominio integro $\forall a \in \mathbb{Z}\setminus\{0\}$ $\nu(a):=|a|$ lo rende euclideo

ma anche ad esempio



- se $a>0$ $\lfloor \log_2(a) \rfloor := \varepsilon \in \mathbb{Z}$

$\Downarrow$

$2^{\varepsilon} \leq a < 2^{\varepsilon+1}$

se $\varepsilon \geq 0 \Rightarrow \nu(a) = \varepsilon = \lfloor \log_2(a) \rfloor$

se $\varepsilon < 0 \Rightarrow \nu(a) = |\varepsilon| = |\lfloor \log_2(a) \rfloor|$

se $a<0$ $\lfloor \log_2(|a|) \rfloor := \varepsilon \in \mathbb{Z}$

$2^{\varepsilon} \leq |a| < 2^{\varepsilon+1} \Rightarrow -2^{\varepsilon+1} < a \leq -2^{\varepsilon}$
↓
$a<0$

e come prima $\boxed{\nu(a) = |\lfloor \log_2(|a|) \rfloor|}$

Ricordo

* $\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ elementi a valutazione minima $\nu(\cdot)=1$

valutazione di 1

* $\mathbb{Z}[i]$ euclideo $\Rightarrow$ DFU $\Rightarrow$ "primo = irriducibile"

Gli irriduc. (equiv. primi) di $\mathbb{Z}[i]$ (a meno di $\mathcal{U}(\mathbb{Z}[i])$) sono:

(1) $p \in \mathbb{Z}$ primi (= irriduc.) t.c. $p \equiv 3 \pmod 4$

(2) $a+ib \in \mathbb{Z}$ con $\nu(a+ib) = a^2+b^2 = p$ con $p \equiv 1 \pmod 4$

cioè $p = (a+ib)\cdot(a-ib)$ ma $a \pm ib \in \mathbb{Z}[i]$ irriducibili

($p \in \mathbb{Z}$, $(a+ib), (a-ib) \in \mathbb{Z}[i]$)

e.g. $5 = (2+i)(2-i)$, $\Rightarrow$ 5 non è più primo in $\mathbb{Z}[i]$

(era primo in $\mathbb{Z}$)

(3) $1+i \in \mathbb{Z}$

$\nu(1+i) = 2 \not\equiv 1 \pmod 4$ ma è irriduc. in $\mathbb{Z}[i]$

(in particolare e.g. $2 = -i(1+i)(1+i)$ non è più primo in $\mathbb{Z}[i]$)

E' ovvio che con $\nu(a+ib) := \|a+ib\| = a^2+b^2$ si ha

$\nu(a+ib) = 0 \iff a+ib = 0$

$\nu((a+ib)\cdot(a'+ib')) = \nu(a+ib)\cdot\nu(a'+ib') \Rightarrow \nu(a+ib) \le \nu(a+ib)(a'+ib')$ $\forall\, a'+ib' \in \mathbb{Z}[i] \setminus \{0\}$

* Voglio fare divisione euclidea in $\mathbb{Z}[i] \subset \mathbb{C}$

$\mathbb{Z}[i] \ni \alpha = a+ib$, $\beta = a'+ib' \neq 0$, con $\mathbb{Z}[i] \subset \mathbb{C}$ uso per conto

$\Rightarrow$ $\frac{\alpha}{\beta}$ (in $\mathbb{C}$) $= \alpha \cdot \beta^{-1} = \alpha \cdot \frac{\overline{\beta}}{\|\beta\|} \in \mathbb{C}$

Ma poiché $\alpha, \beta \in \mathbb{Z}[i] \Rightarrow a, b, a', b' \in \mathbb{Z} \Rightarrow (a')^2 + (b')^2 \in \mathbb{Z}$

$\Rightarrow$ $\alpha \cdot \frac{\overline{\beta}}{\|\beta\|} \in \mathbb{Q}[i] \subset \mathbb{Q}(i) \subset \mathbb{C}$

cioè

$$\boxed{\xi := \frac{\alpha}{\beta} = p_1 + i\, p_2 \quad \text{con } p_1, p_2 \in \mathbb{Q}}$$

Allora $\exists$ certamente interi

$$m_1, m_2 \in \mathbb{Z}_+ \text{ t.c.}$$

$$\boxed{0 \leq |p_1 - m_1| \leq \tfrac{1}{2} \quad \text{e} \quad 0 \leq |p_2 - m_2| \leq \tfrac{1}{2}}$$

Poniamo

$$\boxed{\gamma := m_1 + i\, m_2 \in \mathbb{Z}[i]}$$

$$\Downarrow$$

$$(*) \quad \xi - \gamma = (p_1 - m_1) + i\,(p_2 - m_2) \Rightarrow \|\xi - \gamma\| = (p_1 - m_1)^2 + (p_2 - m_2)^2 \leq \tfrac{1}{4} + \tfrac{1}{4} < 1$$

$\|\cdot\|$ in $\mathbb{Q}[i]$

Poniamo

$$\boxed{\omega := \alpha - \beta \cdot \gamma}$$

Poichè $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ anello $\Rightarrow$ $\boxed{\omega \in \mathbb{Z}[i]}$

Inoltre

$$\left\| \frac{\omega}{\beta} \right\| = \left\| \frac{\alpha - \beta\gamma}{\beta} \right\| = \left\| \frac{\alpha}{\beta} - \gamma \right\| = \|\xi - \gamma\| \underset{(*)}{<} 1$$

$$\Rightarrow \quad \left\| \frac{\omega}{\beta} \right\| = \frac{\|\omega\|}{\|\beta\|} < 1 \Rightarrow \underline{\nu(\omega) < \nu(\beta)}$$

Inoltre

$$\boxed{\begin{array}{c} \alpha = \beta\gamma + \omega \quad \text{e} \\ 0 \leq \nu(\omega) = m_1^2 + m_2^2 < \nu(\beta) \end{array}}$$

Pertanto vediamo come usare con esempio

$$\boxed{\alpha := 14 - 3i \qquad \beta := 4 + 7i}$$

$$\nu(\alpha) = 196 + 9 = 205 > \nu(\beta) = 65$$

$\Rightarrow$ scriverò $\boxed{\alpha = \beta \cdot \gamma + \omega}$

$$\gamma = \frac{\alpha}{\beta} = (14-3i)\cdot\frac{(4-7i)}{16+49} = \frac{(14-3i)(4-7i)}{65} =$$

$$= \frac{35 - 110\,i}{65} = \frac{7}{13} - \frac{22}{13}\,i = p_1 + p_2 \cdot i \quad \text{come prima}$$

Prendo $n_1 = 1$ così $\left|\frac{7}{13} - 1\right| = \left|-\frac{6}{13}\right| = \frac{6}{13} < \frac{1}{2}$ ($\frac{6}{13} \simeq 0{,}46$)

$n_2 = -2$ $\left|-\frac{22}{13} + 2\right| = \left|+\frac{4}{13}\right| = \frac{4}{13} \leq \frac{1}{2}$ ($\frac{4}{13} \simeq 0{,}30$)

Oss: se 1 $\left|\frac{22}{13} - 1\right| = \left|\frac{9}{13}\right| \simeq 0{,}69 > \frac{1}{2}$ no

$\Rightarrow$ $\boxed{\delta = 1 - 2i \in \mathbb{Z}[i]}$

Prendiamo

$$\omega := \alpha - \beta\cdot\delta = (14-3i) - (4+7i)(1-2i)$$
$$= -4 - 2i = -2(2+i)$$

$\Rightarrow$ $0 < N(\omega) = 16 + 4 = 20 < N(\beta) = 65$

Inoltre

$$\alpha = \beta\delta + \omega \quad \text{cioè} \quad \text{ho scritto divisione euclidea}$$

(I) $(14-3i) = (4+7i)\cdot(1-2i) + (-4-2i)$

α β δ ω

come $a = b\,q + r$ scriveremo in $\mathbb{Z}$ (resto)

Ora da capo troviamo con stessa procedura

(II) $(4+7i) = (-4-2i)(-1-i) + (2+i)$

(III) $(-4-2i) = -2(2+i) + 0$

Come in divisione euclidea $\Rightarrow$ ultimo resto non nullo è $\boxed{(2+i)}$

$\Rightarrow$ $\boxed{MCD(\alpha, \beta) = MCD(14-3i,\ 4+7i) = 2+i}$

* Per trovare un'identità di Bezout

Da (II)

$$(2+i) = (4+7i) + (-4-2i)(1+i)$$

$$= (4+7i) + [(14-3i) + (4+7i)(-1+2i)](1+i)$$

$\downarrow$ (I)

$$= (14-3i)(1+i) + (4+7i)[1 + (1+i)(-1+2i)]$$

$$= \underset{\alpha}{(14-3i)} \cdot \underset{s}{(1+i)} + \underset{\beta}{(4+7i)} \underset{t}{(-2+i)}$$

Cioè è scritto in forma Bezout $\boxed{MCD(\alpha, \beta) = \alpha s + \beta t}$

(iii) * $p = 3 \in \mathbb{Z}$ è un primo di $\mathbb{Z}$ t.c. $p \equiv 3 \pmod 4$

$\Rightarrow$ è irriducibile (e quindi primo) in $\mathbb{Z}[i]$

* Siccome Euclideo $\Rightarrow$ PID

$I = (3)$ ideale primo e max $\Rightarrow$ $\frac{\mathbb{Z}[i]}{(3)}$

è campo

Sia $\boxed{\mathbb{K} = \frac{\mathbb{Z}[i]}{(3)}}$

$|\mathbb{K}| = ?$ i.e. quanti elementi ha?

L'ideale $(3) = \{3h + 3ki \mid h, k \in \mathbb{Z}\} \subset \mathbb{Z}[i]$

Ma se $a \in \mathbb{Z}$, $b \in \mathbb{Z}$

$$a = 3q + r \quad \text{con} \quad 0 \leq r < 3$$
$$b = 3\bar{q} + \bar{r} \quad \text{con} \quad 0 \leq \bar{r} < 3$$

divisione euclidea in $\mathbb{Z}$

$\Rightarrow \forall\ a + bi \in \mathbb{Z}[i]$ si può scrivere come:

$$(a + bi) = (3q + r) + (3\bar{q} + \bar{r})i =$$
$$= (r + i\bar{r}) + \underbrace{3(q + \bar{q}i)}_{(3) \subset \mathbb{Z}[i]}$$

$\Rightarrow$ in $\dfrac{\mathbb{Z}[i]}{(3)}$ $\ni [a + bi] = [r + i\bar{r}]$ con $0 \leq r, \bar{r} < 3$

* Perciò elementi di $\mathbb{K}$ sono della forma

$$[r + i\bar{r}] \in \mathbb{K} \quad \text{t.c.} \quad r, \bar{r} \in \mathbb{Z}/3\mathbb{Z}$$

3 scelte per r, 3 scelte per $\bar{r}$ $\Rightarrow$ $|\mathbb{K}| = 9 = 3^2$ elementi

$$\mathbb{K} = \{[\bar{0}], [\bar{1}], [\bar{2}], [\bar{1}i], [\bar{2}i], [\bar{1} + \bar{1}i], [\bar{1} + \bar{2}i], [\bar{2} + \bar{1}i], [\bar{2} + \bar{2}i] \mid \bar{0}, \bar{1}, \bar{2} \in \mathbb{Z}/3\mathbb{Z}\}$$

* Preso

$$[\bar{2} + \bar{1}i] \in \mathbb{K} \setminus \{[\bar{0}]\}$$

$$[\bar{2} + \bar{1}i]^{-1} = ? \text{ in } \mathbb{K}$$

Per semplicità notazionale

$[\bar{2} + \bar{1}i] = \bar{2} + \bar{1} \cdot i$ e cerco $[\bar{a} + \bar{b}i] = \bar{a} + \bar{b}i \in \mathbb{K}$ t.c.

$$\bar{1} = (\bar{2} + \bar{1}i)(\bar{a} + \bar{b}i) = (\underbrace{\bar{2} \cdot \bar{a} - \bar{1} \cdot \bar{b}}_{\text{operaz. in } \mathbb{Z}/3\mathbb{Z}}) + (\bar{2} \cdot \bar{b} + \bar{1} \cdot \bar{a})i$$

(molt. in $\mathbb{K}$)

Cerco in $\mathbb{Z}/3\mathbb{Z}$ $\quad \bar{a}, \bar{b} \in \mathbb{Z}/3\mathbb{Z}$ t.c.

$$\begin{cases} \bar{1} = \bar{2}\cdot\bar{a} - \bar{1}\cdot\bar{b} = \overline{2a-b} \\ \bar{0} = \bar{2}\,\bar{b} + \bar{1}\cdot\bar{a} = \overline{2b+a} \end{cases} \quad \text{in } \mathbb{Z}/3\mathbb{Z}$$

cioè cerco $a, b \in \mathbb{Z}$ t.c. risolva il sistema

$$\begin{cases} 2b+a \equiv 0 \pmod 3 \\ (2a-b) \equiv 1 \pmod 3 \end{cases}, \quad 0 \le a, b \le 2$$

$$\Rightarrow \begin{cases} 2b+a = 3h \\ 2a-b = 1+3k \end{cases} \Rightarrow \quad b = 2a-1+3(-k)$$

$$2(2a-1+3(-k))+a = 3h$$

$$4a-2-3k+a = 3h$$

$$5a-2 = 3(h+k) \Rightarrow \quad 2a-2 = 3(h+k-a)$$

$$\Leftrightarrow \quad 2(a-1) \equiv 0 \pmod 3 \Leftrightarrow \quad \bar{2}\cdot(\overline{a-1}) = 0 \text{ in } \mathbb{Z}/3\mathbb{Z} \text{ campo}$$

$$\Leftrightarrow \quad \overline{a-1} = \bar{0} \quad \Leftrightarrow \quad \boxed{\bar{a} = \bar{1}}$$

Ma se $\bar{a} = \bar{1} \Rightarrow b = 2\cdot 1 - 1 + 3(-k) = 1 + 3(-k)$

$$\Rightarrow \boxed{\bar{b} = \bar{1}}$$

$$\Rightarrow \quad \boxed{(\bar{2} + \bar{1}\,i)^{-1} = (\bar{1} + \bar{1}\,i)}$$

Infatti in $\mathbb{K}$ si ha

$$\begin{aligned} (\bar{2} + \bar{1}\,i)\cdot(\bar{1} + \bar{1}\,i) &= \bar{2} + \bar{2}\,i + \bar{1}\,i - \bar{1} = \\ &= \bar{2} - \bar{1} + \bar{3}\,i \\ &= \bar{1} + \bar{0}\,i \\ &= \bar{1} \quad \text{(ok)} \end{aligned}$$

(iii) Sia $\mathbb{K} = \dfrac{\mathbb{Z}[i]}{(3)}$ campo

$\| 2$

$\mathbb{Z}/3\mathbb{Z}[i]$

Consideriamo $(\mathbb{Z}/3\mathbb{Z})[x]$ è Euclideo perché $(\mathbb{Z}/3\mathbb{Z})$ campo

$(\bar{1}x^2 + \bar{1}) \in \dfrac{\mathbb{Z}}{3\mathbb{Z}}[x]$ è polinomio irriducibile infatti

$\bar{1}x^2 + \bar{1}$ non ha soluzioni in $\mathbb{Z}/3\mathbb{Z}$

$(\bar{0})^2 + \bar{1} \neq \bar{0}$, $(\bar{1})^2 + \bar{1} = \bar{2} \neq \bar{0}$

$(\bar{2})^2 + \bar{1} = \bar{4} + \bar{1} = \bar{1} + \bar{1} \neq \bar{0}$

$\Rightarrow$ $\dfrac{\left(\dfrac{\mathbb{Z}}{3\mathbb{Z}}\right)[x]}{(\bar{1}x^2 + \bar{1})} = \mathbb{H}$ campo $\left((\mathbb{Z}/3\mathbb{Z})[x] \text{ euclideo} \Downarrow \text{PID} \right)$

$$\mathbb{H} = \{ \bar{a} + \bar{b}\,\bar{x} \mid \bar{a}, \bar{b} \in \mathbb{Z}/3\mathbb{Z} \text{ e } (\bar{x})^2 = -\bar{1} = \bar{2} \text{ in } \mathbb{Z}/3\mathbb{Z} \}$$

$\bar{2}$ non quadrato in $\mathbb{Z}/3\mathbb{Z}$

$\Downarrow$

$|\mathbb{H}| = 9$ e

$$\mathbb{H} \xrightarrow[\cong]{\varphi} \mathbb{K}$$

$$\bar{a} + \bar{b}\,\bar{x} \longrightarrow \bar{a} + \bar{b}\,i$$

$\bar{x}^2 = -\bar{1} = \bar{2}$ $\qquad$ $i^2 = -1 = 2$ in $\dfrac{\mathbb{Z}[i]}{(3)}$

$\Downarrow$

$$\boxed{\mathbb{H} \cong \mathbb{K}}$$

(iv) Sia $\alpha = 3 + i \in \mathbb{Z}[i]$

Considero $J := (\alpha) = (3 + i) \subset \mathbb{Z}[i]$ ideale principale

Noto che $N(\alpha) = 9 + 1 = 10 \in \mathbb{Z}$ non primo in $\mathbb{Z}$

Siccome $10 = 2 \cdot 5$, considero fattorizz. non banale di α

$(3+i) = (1+i)(2-i)$

$\Rightarrow$ (α) no ideale primo e no max

$\Rightarrow$ $\dfrac{\mathbb{Z}[i]}{(3+i)}$ no dominio integro (ma comm. unitario)

Abbiamo

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\ j\ } & \mathbb{Z}[i] \\ & \searrow^{\varphi} & \downarrow \pi \\ & & \dfrac{\mathbb{Z}[i]}{(3+i)} \end{array}$$

- j omomorf inclusione
- π omom. proiez. canonica

$\Rightarrow$ $\varphi = \pi \circ j$ è omomorfismo anelli

Notiamo che se $\alpha = 3 + i = a + bi \Rightarrow a^2 + b^2 = 10 \in \mathbb{Z}$

e siccome $a^2 + b^2 = (a+ib)\cdot(a-ib)$ in $\mathbb{Z}[i]$

$a^2+b^2 = 10$, $(a+ib)(a-ib) = (3+i)\cdot(3-i)$

$\Rightarrow$ $\boxed{a^2+b^2 = 10 \in \ker(\varphi)}$ perché $10 \in (\alpha) = (3+i)$

$\Rightarrow$ Per teorema omomorfismo anelli si ha

$$\frac{\mathbb{Z}}{\ker(\varphi)} \xrightarrow[\cong]{\ \bar{\varphi}\ } \mathrm{Im}(\varphi) \subseteq \frac{\mathbb{Z}[i]}{(3+i)}$$

① Poiché $a = 3$, $b = 1$ t.c. $MCD(a,b) = MCD(3,1) = 1$

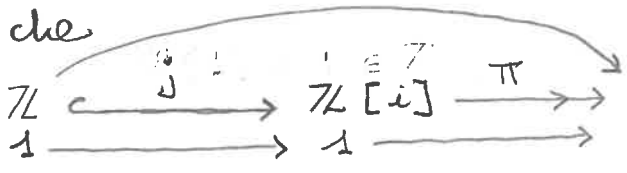
$\Rightarrow$ φ suriettivo

Se dimostro ciò $\Rightarrow$ $\overline{\varphi}$ suriettivo cioè $Im(\overline{\varphi}) \cong \frac{\mathbb{Z}[i]}{(3+i)}$

cioè avrò

$$\boxed{\frac{\mathbb{Z}}{(\ker\varphi)} \cong \frac{\mathbb{Z}[i]}{(3+i)}}$$

Notiamo che



$\Rightarrow \varphi(1) = 1$ morfismo unitario

⊛ $i \in Im(\varphi) \Leftrightarrow \exists\, m \in \mathbb{Z}$ t.c. $\varphi(m) = i$

Ovviamente il morfismo φ opera così:

$$\boxed{m \xrightarrow{\varphi} m + (3+i)}$$

perciò $\quad i = \varphi(m) \Leftrightarrow \exists\, m \in \mathbb{Z}$ t.c. $\dot{i} - \dot{m} \in (3+i)$ in $\mathbb{Z}[i]$

Perciò $\Leftrightarrow$ $\exists\, a+ib \in \mathbb{Z}[i]$ e $m \in \mathbb{Z}$ t.c.

$$(i - m) = (3+i)(a+ib) \Leftrightarrow$$

$$(-m + i) = (3a - b) + i(3b + a) \Leftrightarrow$$

$$\begin{cases} (3a - b) = -m \\ (3b + a) = 1 \end{cases}$$

Poiché $MCD(3,1) = 1$ $\Rightarrow$ Bezout $3(1) + 1(-2) = 1$ (b, a) $\quad \boxed{\begin{matrix} a = -2 \\ b = 1 \end{matrix}}$

Ma allora $\quad 3(-2) - (1) = -6 - 1 = -7 = -m$

$\Rightarrow$ $(i - 7) = (3+i)(-2+i)$ (OD)

$\Rightarrow$ $\varphi(7) = i \in \frac{\mathbb{Z}[i]}{(3+i)}$

Siccome gli elementi di $\frac{\mathbb{Z}[i]}{(3+i)}$ sono della forma

$$\{\overline{a+ib}\} \bmod (3+i) \text{ con } a, b \in \mathbb{Z}$$

$\forall\ \overline{a+ib} \in Im(\varphi)$ infatti

$$\overline{a} = \varphi(a), \quad \overline{b} = \varphi(b), \quad \overline{i} = \varphi(i)$$

e φ morfismo anelli

$$\overline{a} + \overline{i}\,\overline{b} = \varphi(a) + \varphi(i)\cdot\varphi(b) = \varphi(a+ib)$$

$\Rightarrow$ φ suriettivo

(2) $\ker(\varphi) = (10) = (a^2+b^2)$

$m \in \mathbb{Z} \in \ker(\varphi) \iff \varphi(m) = 0$ in $\frac{\mathbb{Z}[i]}{(3+i)}$

$\iff m \in (3+i) \subset \mathbb{Z}[i] \iff$

$m \in \mathbb{Z} \cap J = (3+i)$

($\mathbb{Z}$: sottoanello di $\mathbb{Z}[i]$; J: ideale principale in $\mathbb{Z}[i]$)

$\iff m = (3+i)\cdot(a+ib) = (3a-b) + i(a+3b)$

$\iff \begin{cases} m = 3a - b \\ a + 3b = 0 \end{cases} \iff a = -3b$

$m = 3(-3b) - b = 10(-b) \iff m \in (10) \subset \mathbb{Z}$ ($10 = a^2+b^2$)

Perciò si ha

$$\frac{\mathbb{Z}[i]}{(3+i)} \cong \frac{\mathbb{Z}}{10\mathbb{Z}}$$

comm. unitario non integro con 10 elementi

Più in generale, con le stesse strategie note

$a, b \in \mathbb{Z}$ t.c. $MCD(a,b) = 1$

Allora

$$\frac{\mathbb{Z}[i]}{(a+ib)} \cong \frac{\mathbb{Z}}{(a^2+b^2)} = \frac{\mathbb{Z}}{(a^2+b^2)\cdot\mathbb{Z}}$$

che perciò è campo (equiv. dominio) $\Leftrightarrow$

$a^2+b^2 = N(a+ib) \in \mathbb{Z}$ è un primo

Svolgimento esercizio 2

(i) $\mathbb{Z} \subset \mathbb{Q}$, $\frac{1}{2} \in \mathbb{Q} \Rightarrow \mathbb{Z}\left[\frac{1}{2}\right] \subset \mathbb{Q}$ minimo sottoanello di $\mathbb{Q}$ contenente $\mathbb{Z}$ e $\{\frac{1}{2}\} \subset \mathbb{Q}$

$$\mathbb{Z}\left[\tfrac{1}{2}\right] := \left\{ \frac{m}{2^n} \;\middle|\; m \in \mathbb{Z},\ n \in \mathbb{N} \right\}$$

- se $n = 0$ ho $\mathbb{Z}$
- se $n > 0$ ho denominatore non banale

↓

elemento così perché struttura duello

Ovviamente si può assumere $MCD(m, 2) = 1$ per via frazioni ridotte

- $\mathbb{Z}\left[\frac{1}{2}\right]$ è commutativo unitario
- $\mathbb{Z}\left[\frac{1}{2}\right] \subset \mathbb{Q}$ è dominio integro perché contenuto in $\mathbb{Q}$ campo
- $\mathbb{Z}\left[\frac{1}{2}\right]$ è dominio euclideo

infatti si ha la valutazione

$$v\left(\frac{m}{2^n}\right) := |m| \cdot 2^n \qquad n \in \mathbb{N},\ MCD(m,2) = 1$$

soddisfa assiomi valutazione

Procedimento si estende per $\forall\ a \in \mathbb{Z} \setminus \{0\}$

$\mathbb{Z}\left[\frac{1}{a}\right]$ è euclideo (se $a = \pm 1$ ritrovo $\mathbb{Z}$)

(ii) $\mathbb{Z} \subset \mathbb{R}$, $\sqrt{2} \in \mathbb{R} \Rightarrow \mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ minimo sottoanello di $\mathbb{R}$ contenente $\mathbb{Z}$ e $\{\sqrt{2}\}$.

$$\mathbb{Z}[\sqrt{2}] := \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \subset \mathbb{R}$$

* è commutativo unitario e integro

* è euclideo

$$v(a + b\sqrt{2}) = |a^2 - 2b^2|$$

- $\nu : \mathbb{Z}[\sqrt{2}] \setminus \{0\} \longrightarrow \mathbb{N}$
- $\nu(\alpha \cdot \beta) = \nu(\alpha) \cdot \nu(\beta)$
- $\forall\, \alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ t.c. $\beta \neq 0$
  $\exists\, q, r \in \mathbb{Z}[\sqrt{2}]$ t.c. $\alpha = \beta q + r$, $0 \leq \nu(r) < \nu(\beta)$

Infatti $\gamma := \frac{\alpha}{\beta} \in \mathbb{Q}[\sqrt{2}]$

Se $\alpha = a + b\sqrt{2}$ $\beta = a' + b'\sqrt{2} \neq 0 \Rightarrow$

$$\gamma = \frac{\alpha}{\beta} = \frac{a + b\sqrt{2}}{a' + b'\sqrt{2}} = \frac{(a + b\sqrt{2})(a' - b'\sqrt{2})}{(a')^2 - 2(b')^2} = p_1 + p_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

Scelgo $\boxed{q = m_1 + m_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ t.c.}}$

$$|p_1 - m_1| \leq \tfrac{1}{2} \text{ e } |p_2 - m_2| \leq \tfrac{1}{2}$$

$$\Rightarrow \gamma - q = (p_1 - m_1) + (p_2 - m_2)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

Poniamo

$$r := \beta(\gamma - q) = \beta\gamma - \beta q = \underset{\mathbb{Z}[\sqrt{2}]}{\alpha - \beta q} \in \mathbb{Z}[\sqrt{2}]$$

$$\nu(r) = \nu(\beta) \cdot \nu(\gamma - q) \leq \tfrac{1}{4}\nu(\beta) < \nu(\beta)$$

$$\nu(\gamma - q) = |(p_1 - m_1)^2 - 2(p_2 - m_2)^2|$$
$$\leq \left|\tfrac{1}{4} - 2 \cdot \tfrac{1}{4}\right| = \left|\tfrac{1}{4} - \tfrac{1}{2}\right| = \tfrac{1}{4}$$

$$\Rightarrow \boxed{\alpha = \beta q + r}$$

Oss A differenza di prima NON È VERO che $\forall\, a \in \mathbb{N}$ $\mathbb{Z}[\sqrt{a}]$ è euclideo

Ad esempio $\mathbb{Z}[\sqrt{10}]$ non è DFU $\Rightarrow$ non è euclideo

Infatti:

$10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$ in $\mathbb{Z}[\sqrt{10}]$ due fattorizzazioni

* Dimostro che $2, 5, \sqrt{10}$ irriducibili in $\mathbb{Z}[\sqrt{10}]$

- $2 = (a + b\sqrt{10})(c + d\sqrt{10}) \iff \begin{cases} ac + 10bd = 2 \\ ad - bc = 0 \end{cases} \Rightarrow \begin{cases} ac + 10bd = 2 \\ ad = bc \end{cases}$

$\Rightarrow$ o $b = 0 \Rightarrow a = 0$ o $d = 0 \to 2 = a \cdot (c + d\sqrt{10}) \Rightarrow d = 0$, $2 = a \cdot c$ in $\mathbb{Z}$ irr.

o $d = 0 \Rightarrow b = 0$ v $c = 0 \to 2 = (a + b\sqrt{10})(c) \Rightarrow b = 0$

2 irriducibile in $\mathbb{Z}[\sqrt{10}]$

- $5 \iff \begin{cases} ac + 10bd = 5 \\ ad - bc = 0 \end{cases}$ comprimo

5 irriducibile in $\mathbb{Z}[\sqrt{10}]$

- $\sqrt{10} \iff \begin{cases} ac + 10bd = 0 \\ ad - bc = \sqrt{10} \end{cases}$ ※ $a, b, c, d \in \mathbb{Z}$

* Ma infatti la funzione usata prima in $\mathbb{Z}[\sqrt{2}]$, in $\mathbb{Z}[10]$

$$N(a + b\sqrt{10}) = |a^2 - 10b^2|$$

non fornisce una valutazione

$\alpha = \sqrt{10}$ $\beta = 2$ $N(\alpha) = \|\alpha\| = |-10| = 10$

$N(\beta) = \|\beta\| = |4| = 4$

$\beta = 2 \neq 0$

Vorrei trovare $q, r \in \mathbb{Z}[\sqrt{10}]$ t.c.

$\alpha = \beta q + r$ con $0 \leq N(r) = \|r\| < N(\beta) = 4$

$\rho = \frac{\alpha}{\beta} = \frac{\sqrt{10}}{2} \in \mathbb{Q}[\sqrt{10}]$ $\Rightarrow \rho = \frac{\alpha}{\beta} = \frac{1}{2}\sqrt{10} = 0 + \frac{1}{2}\sqrt{10} \in \mathbb{Q}[\sqrt{10}]$

$\Rightarrow$ $q = 0 + m_2\sqrt{10}$ con $m_2 = \begin{cases} 0 \\ 1 \end{cases}$ ↓ interi più vicini a $\rho_2 = \frac{1}{2}$

$\Rightarrow$ o $q = 0 + 0\sqrt{10}$ o $q = 0 + 1\sqrt{10}$

- Se $q = 0 + 0\sqrt{10}$

$$r := \beta\delta - \beta q = \alpha - \beta \cdot 0 = \alpha \quad \#\#$$

$$\nu(r) = \nu(\alpha) > \nu(\beta) = 4$$
$$= 10$$

- se $q = 0 + 1\sqrt{10}$

$$r := \beta \cdot \delta - \beta \cdot q = \sqrt{10} - 2\sqrt{10} = -\sqrt{10}$$

$$\nu(r) = \nu(-\sqrt{10}) = 10 > \nu(\beta) = 4 \#\#$$

Il fatto che non sia DFU è più forte perché comporta che non può esistere nessuna valutazione su $\mathbb{Z}[\sqrt{10}]$ che lo renda euclideo

(iii) $\mathbb{Z} \subset \mathbb{C}$, $i\sqrt{2} = \sqrt{-2} \in \mathbb{C}$

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$$

minimo sottoanello di $\mathbb{C}$ che contiene $\mathbb{Z}$ e $\sqrt{-2}$

* è dominio di integrità perché contenuto in $\mathbb{C}$

* è euclideo

$$\nu(a + b\sqrt{-2}) = a^2 + 2b^2$$

soddisfa assiomi valutazione

simili conti come con $\mathbb{Z}[\sqrt{2}]$

Oss Non è vero che $\forall\, a \in \mathbb{N}_{>0} \setminus \{1\}$ $\mathbb{Z}[\sqrt{-a}]$ è sempre euclideo

* **Esempio**

$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ NO DFU

Con i soliti conti (vedi [Piacentini - Cattaneo, pp. 185-186])

$$U(\mathbb{Z}[\sqrt{-3}]) = \{\pm 1\}$$

* **$1 + \sqrt{-3}$ è irriducibile**

se fosse $1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$

$$\Rightarrow \begin{cases} ac - 3bd = 1 \\ ad + bc = 1 \\ 4 = (a^2 + 3b^2)(c^2 + 3d^2) \end{cases}$$

$4 = \| 1 + \sqrt{-3} \|$

$\Rightarrow a^2 + 3b^2 = \begin{matrix} \nearrow 1 \\ \searrow 4 \end{matrix}$ perché $a^2 + 3b^2 = 2$ in $\mathbb{Z}$ impossibile

- $a^2 + 3b^2 = 1 \Rightarrow a = \pm 1 \quad b = 0 \quad (a + b\sqrt{-3}) \in U(\mathbb{Z}[\sqrt{-3}])$

  $\Rightarrow c^2 + 3d^2 = 4 \Rightarrow \begin{matrix} \nearrow c = 2, d = 0 \text{ ✗} \\ \searrow c = d = 1 \Rightarrow c + d\sqrt{-3} = 1 + \sqrt{-3} \end{matrix}$

- Se $a^2 + 3b^2 = 4 \Rightarrow c^2 + 3d^2 = 1$ e ragiono come sopra

  $c + d\sqrt{-3}$ unità e $a + b\sqrt{-3} = 1 + \sqrt{-3}$

* $(1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}) = 4 = 2 \cdot 2$

$\Rightarrow 1 + \sqrt{-3} \mid 4$ in $\mathbb{Z}[\sqrt{-3}]$

ma $(1 + \sqrt{-3}) \nmid 2$ in $\mathbb{Z}[\sqrt{-3}]$

Infatti se $2 = (1 + \sqrt{-3})(a + b\sqrt{-3}) \Rightarrow$ le norme devono

$\| 2 \| = 4 = 4 \cdot (a^2 + 3b^2) \Rightarrow a^2 + 3b^2 = 1$

$\Rightarrow a + b\sqrt{-3}$ unità in $\mathbb{Z}[\sqrt{-3}]$ cioè

$2 = \pm(1 + \sqrt{-3})$ ✗

perciò $(1 + \sqrt{-3})$ è un irriducibile che non è primo

Svolgimento Esercizio 3

(i) $(\mathbb{K}[[x]], +, \cdot)$ anello serie formali a coeff. in $\mathbb{K}$ e indet x

Ψ

$\sum_{n \geq 0} a_n x^n$

$\underline{a} := \sum_{n \geq 0} a_n x^n$, $\underline{b} := \sum_{n \geq 0} b_n x^n \in \mathbb{K}[[x]]$

* Operazioni anello

- $\underline{a} + \underline{b} := \sum_{n \geq 0} (a_n + b_n) x^n$

somme finite per ogni n

$$\underline{a} \cdot \underline{b} := \left(\sum_{n \geq 0} a_n x^n \right) \cdot \left(\sum_{s \geq 0} b_s x^s \right) := \sum_{m \geq 0} \left(\sum_{n+s=m} a_n \cdot b_s \right) x^m$$

* Poiché $a_n, b_s \in \mathbb{K}$ commutativo $\Rightarrow$ $(\mathbb{K}[[x]], +, \cdot)$ commutativo

- $1 \in \mathbb{K} \subset \mathbb{K}[[x]]$ $\quad 1 = 1 + \sum_{n > 0} 0 \, x^n$ $\Rightarrow$ unitario

(ii) Definisco per $\underline{a} \neq \underline{0} \left(= \sum_{n \geq 0} 0 \, x^n \right)$, $\underline{a} \in \mathbb{K}[[x]]$

$$\boxed{\deg(\underline{a}) := \min_{n \in \mathbb{N}} \{ n \mid a_n \neq 0 \}}$$ ($\mathbb{N}$ ben ordinato)

Noto che se $\underline{a}, \underline{b} \in \mathbb{K}[[x]] \setminus \{\underline{0}\}$

$$\deg(\underline{a} \cdot \underline{b}) = \deg\left(\sum_{m \geq 0} \left(\sum_{n+s=m} a_n \cdot b_s \right) x^m \right)$$

$$= \deg(\underline{a}) + \deg(\underline{b})$$

Perciò $\underline{a}, \underline{b} \neq \underline{0} \Rightarrow (\underline{a} \cdot \underline{b}) \neq \underline{0}$

$\Rightarrow$ $\boxed{\mathbb{K}[[x]] \text{ dominio integrale}}$

(iii) Da (ii) $\Rightarrow$ $\mathcal{U}(\mathbb{K}[[x]])$ (unità o invertibili di $\mathbb{K}[[x]]$) $\subseteq \{ \underline{a} \in \mathbb{K}[[x]] \mid \deg(\underline{a}) = 0$ i.e. $a_0 \neq 0 \}$

Infatti $\underline{a} \in \mathcal{U}(\mathbb{K}[[x]]) \Leftrightarrow \exists\, \underline{b} \in \mathbb{K}[[x]]$ per cui

$\underline{a} \cdot \underline{b} = 1$ in $\mathbb{K}[[x]]$

$\Rightarrow$ $\underline{a} \cdot \underline{b} := a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \cdots$ $\Rightarrow$ $\boxed{a_0 \cdot b_0 = 1}$

$\underline{a} \cdot \underline{b} = 1$

$\mathbb{K}$

$\Downarrow$

$a_0, b_0 \in \mathbb{K} \setminus \{0\}$

$\Downarrow$

$\boxed{a_0, b_0 \neq 0}$

Più precisamente

$$\underline{a} \in U(\mathbb{K}[[x]]) \iff a_0 \neq 0$$

oltre

($\Rightarrow$) se $\underline{a} \in U(\mathbb{K}[[x]])$ allora $a_0 \neq 0$

($\Leftarrow$) Sia $\underline{a} = a_0 + a_1 x + a_2 x^2 + \cdots$

Sia $\underline{b} = b_0 + b_1 x + b_2 x^2 + \cdots \in U(\mathbb{K}[[x]])$ t.c.

$$\underline{a} \cdot \underline{b} = 1$$

termine noto $\quad a_0 b_0 = 1 \Rightarrow \boxed{b_0 = a_0^{-1} \in \mathbb{K}}$, $(a_0 \neq 0$ in $\mathbb{K})$

Coeff. $x \quad a_0 b_1 + b_0 a_1 = 0 \Rightarrow a_0 b_1 \underset{b_0 = a_0^{-1}}{=} -a_1 \cdot a_0^{-1} \Rightarrow \boxed{b_1 = -a_1 a_0^{-2}}$ ($\in \mathbb{K}$)

Coeff $x^2 \quad a_0 b_2 + a_1 b_1 + b_0 a_2 = 0$

$$\Rightarrow a_0 b_2 + a_1 \cdot (-a_1 a_0^{-2}) + a_0^{-1} a_2 = 0$$

$$\Rightarrow a_0 b_2 = -a_2 \cdot a_0^{-1} + a_1^2 \cdot a_0^{-2}$$

$$\Rightarrow \boxed{b_2 = -a_2 a_0^{-2} + a_1^2 \cdot a_0^{-3} \in \mathbb{K}}$$

si procede così per ricorsività ∎

Oss In particolare in $\mathbb{K}[[x]]$ si ha la ben nota formula

$$\boxed{(1-x)^{-1} = \left(\frac{1}{1-x}\right) = 1 + x + x^2 + \cdots = \sum_{n \geq 0} x^n}$$

(iv) $\forall\ \underline{a} \in \mathbb{K}[[x]]$ t.c. $\operatorname{ord}(\underline{a}) = n \geq 1 \Rightarrow \boxed{a_0 = \cdots = a_{n-1} = 0, a_n \neq 0}$

$$\underline{a} = \sum_{n \geq n} a_n x^n = x^n \cdot \underline{u}, \text{ con } \underline{u} = \sum_{n \geq n} a_n x^{n-n} \in U(\mathbb{K}[[x]])$$

$a_n \neq 0$ è di fronte a $x^{n-n} = x^0 = 1$

$$\Rightarrow \boxed{\underline{a} = x^n \cdot \underline{u}, \text{ con } \underline{u} \in U(\mathbb{K}[[x]])}$$

$\Rightarrow \quad \underline{a} \in \mathbb{K}[[x]] \setminus U(\mathbb{K}[[x]])$

$\Rightarrow \quad (x^n) \subset \mathbb{K}[[x]]$ è ideale $\forall\, n \geq 1$

Poiché
- ideali contengono non-invertibili di $\mathbb{K}[[x]]$
- invertibili di $\mathbb{K}[[x]] \iff a_0 \neq 0$

$\Downarrow$

non-invertibili di $\mathbb{K}[[x]] \iff \deg(\underline{a}) = n \geq 1$

$\Downarrow$

tutti e soli ideali di $\mathbb{K}[[x]]$ sono della forma (x^n), $n \geq 1$

$\Downarrow$

$\mathbb{K}[[x]]$ è PID

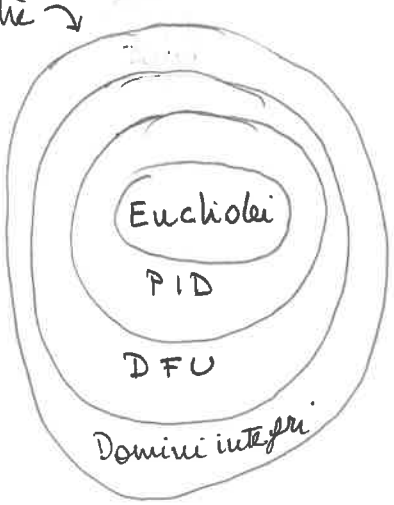
Ideali sono a catena

$$(x^n) \subsetneq (x^{n-1}) \subsetneq \cdots \subsetneq (x) \subsetneq \mathbb{K}[[x]]$$

x è unico irriducibile in $\mathbb{K}[[x]] \Rightarrow (x)$ è unico ideale massimale = unico ideale primo

perché PID

$\Rightarrow$ $\mathbb{K}[[x]]$ è pure DFU perché



(V) Notare inoltre che, $\forall\, n \geq 1$ consideriamo l'anello quoziente

$$\frac{\mathbb{K}[[x]]}{(x^n)}$$

$$\underline{a} = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \cdot (\underline{u})$$

$\underline{u} \in U(\mathbb{K}[[x]])$

Perciò $> m$

$$\Bbbk[[x]] \twoheadrightarrow \frac{\Bbbk[[x]]}{(x^m)}$$

$$\underline{a} \longrightarrow [\underline{a}] =: [a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}]$$

Perciò

$$\boxed{\frac{\Bbbk[[x]]}{(x^m)} \cong \frac{\Bbbk[x]}{(x^m)}}$$

dove $\Bbbk[x]$ anello dei polinomi a coeff in $\Bbbk$ (euclideo)

(vi) Poiché $\Bbbk[[x]]$ dominio intero $\Rightarrow \exists\ Q(\Bbbk[[x]])$ campo delle frazioni

tale che $\Bbbk[[x]] \hookrightarrow \boxed{Q(\Bbbk[[x]]) := \Bbbk((x))}$

Come è fatto $Q(\Bbbk[[x]])$?

Poiché $\forall\ \underline{b} \neq \underline{0}$ è t.c. $\underline{b} = x^n \cdot \underline{u}$, $\underline{u} \in U(\Bbbk[[x]])$

Allora prei $\underline{b}, \underline{a} \in \Bbbk[[x]]$, $\underline{b} \neq \underline{0}$ e $\underline{a} = x^m \cdot \underline{v}$ e $\underline{0}$

$$\boxed{\frac{\underline{a}}{\underline{b}} := \frac{x^m \cdot \underline{v}}{x^n \cdot \underline{u}} = x^{m-n} \cdot (\underline{v} \cdot \underline{u}^{-1})} \quad \text{e } \underline{0} \text{ se } \underline{a} = 0$$

Se $m \geq n \Rightarrow \dfrac{\underline{a}}{\underline{b}} \in \Bbbk[[x]]$ perché x^{m-n} è t.c. $m - n \geq 0$

Se $m < n \Rightarrow \dfrac{\underline{a}}{\underline{b}} = \dfrac{1}{x^{n-m}} \cdot (\underline{v} \cdot \underline{u}^{-1}) = ?$

$n - m > 0$

$$\Downarrow$$

$$\boxed{\Bbbk((x)) = Q(\Bbbk[[x]]) = \left\{ \sum_{n \geq N} a_n x^n \;\middle|\; N \in \mathbb{Z} \right\}}$$

dove

$$\sum_{n \geq N} a_n x^n = a_N \frac{1}{x^N} + a_{N-1} \frac{1}{x^{N-1}} + \cdots + a_0 + a_1 x + a_2 x^2 + \cdots$$

(vii) Ricordando inoltre per $\mathbb{K}[x]$

$$\mathbb{K}[x] \hookrightarrow Q(\mathbb{K}[x]) = \mathbb{K}(x)$$

$\mathbb{K}[x]$: polinomi — $\mathbb{K}(x)$: funzioni razionali

$$\mathbb{K}[x] \hookrightarrow \mathbb{K}(x)$$
$$p(x) = \frac{p(x)}{1} \qquad \frac{f(x)}{g(x)}$$

Abbiamo un morfismo iniettivo di anelli:

$$\mathbb{K}[x] \xrightarrow{j} \mathbb{K}[[x]]$$

$p(x) = a_0 + a_1 x + \dots + a_m x^m$ interpretabile come una serie formale di definitivamente nulla

$p(x) \in \mathbb{K}[x]$ è

$$\Rightarrow \quad \mathbb{K}[x] \xrightarrow{j} \mathbb{K}[[x]] \hookrightarrow \mathbb{K}((x))$$

$\mathbb{K}((x))$: campo

Poiché $Q(\mathbb{K}[x]) = \mathbb{K}(x)$ è minimo campo a contenere $\mathbb{K}[x]$ e $\mathbb{K}((x))$ è campo

$$\Downarrow$$

$$\boxed{\mathbb{K}(x) \subseteq \mathbb{K}((x))}$$

* Come vedo $\mathbb{K}(x)$ come sotto campo di $\mathbb{K}((x))$?

$f(x), g(x) \in \mathbb{K}[x]$ t.c. $g(x) \neq 0$

- Se $\deg(f(x)) > \deg(g(x))$

$\mathbb{K}[x]$ euclideo $\Rightarrow$ $f(x) = q(x) \cdot g(x) + r(x)$ divisione euclidea

$r(x)$ resto $\begin{cases} 0 \\ \deg(r(x)) < \deg(g(x)) \end{cases}$

$$\Rightarrow \quad \frac{f(x)}{g(x)} = \underset{\mathbb{K}[x]}{q(x)} + \frac{r(x)}{g(x)}$$

Ora se $\deg(g) = m$ e $g(x) = b_t x^t + \dots + b_m x^m =$

$$= x^t \underbrace{(\underset{\neq 0}{b_t} + \dots + b_m x^{m-t})}_{u(x) \in \mathbb{K}[x] \subset \mathbb{K}[[x]] \text{ t.c. } u(x) \in \mathcal{U}(\mathbb{K}[[x]])}$$

$$\Rightarrow \quad \frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{x^t \cdot u(x)}$$

$$= q(x) + \frac{r(x) \cdot (u(x))^{-1}}{x^t}$$

$\uparrow$
$\mathbb{K}[x]$

- $r(x) \in \mathbb{K}[x]$ è polinomio $\Rightarrow$ serie formale definitivamente nulla
- $u(x) \in \mathbb{K}[x]$ è polinomio con termine noto $b_t \neq 0$
  $\Rightarrow$ è serie formale definitivamente nulla ma invertibile in $\mathbb{K}[[x]]$
  $\Rightarrow (u(x))^{-1} \in \mathbb{K}[[x]]$

$$\Rightarrow \quad \frac{f(x)}{g(x)} = \frac{q(x) \cdot x^t + r(x) \cdot (u(x))^{-1}}{x^t}$$

è della forma $\sum_{n \geq -t} a_n x^n \in \mathbb{K}((x))$

- Se $\deg(f(x)) < \deg(g(x))$

  $\frac{f(x)}{g(x)}$ è come il caso $\frac{r(x)}{g(x)}$ di prima

(viii) Usiamo costruzione di $\mathbb{K}((x))$ per dimostrare che $\mathbb{K}[[x]]$ euclideo (dunque PID, dunque $D \neq U$)

Prendo come per i polinomi

$$\nu : \mathbb{K}[[x]] \setminus \{\underline{0}\} \longrightarrow \mathbb{N}$$
$$\underline{a} \longrightarrow \text{oleg}(\underline{a})$$

ma stavolta oleg definito con minimo

Siccome $\nu(\underline{a}\cdot\underline{b}) = \nu(\underline{a}) + \nu(\underline{b})$ ola prima

- $\nu(\underline{a}) \leq \nu(\underline{a}\cdot\underline{b})$, $\forall\ \underline{b} \neq \underline{0}$
- $\forall\ \underline{a}, \underline{b} \in \mathbb{K}[[x]]$, $\underline{b} \neq \underline{0}$, $\exists\ \underline{q}, \underline{r} \in \mathbb{K}[[x]]$ t.c.

$$\underline{a} = \underline{b}\cdot\underline{q} + \underline{r}, \quad \text{con } 0 \leq \nu(\underline{r}) < \nu(\underline{b})$$

(i) Se $\underline{b} \in U(\mathbb{K}[[x]])$

$\nu(\underline{b}) = \text{oleg}(\underline{b}) = 0$ per caratt. di $U(\mathbb{K}[[x]])$

$$\Rightarrow \quad \underline{q} = \underline{a}\cdot\underline{b}^{-1} \quad \text{e} \quad \underline{r} = \underline{0}$$

(ii) Se $\underline{b} \in \mathbb{K}[[x]] \setminus U(\mathbb{K}[[x]])$

Da prima $\underline{b} \in (x^m)$ per qualche $m \geq 1$

$$\Rightarrow \quad \underline{b} = x^m \cdot \underline{u}, \quad \text{con } \underline{u} \in U(\mathbb{K}[[x]])$$

$$\Rightarrow \quad \boxed{\nu(\underline{b}) = m}$$

Sia $\boxed{\nu(\underline{a}) = m \geq 0}$ $\Rightarrow$ $\underline{a} \in (x^m)$ se $m > 0$
o $\underline{a} \in U(\mathbb{K}[[x]])$ se $m = 0$

Allora in $\mathbb{K}((x))$

$$\frac{\underline{a}}{\underline{b}} = \frac{a_m x^m + a_{m+1} x^{m+1} + \cdots}{b_m x^m + b_{m+1} x^{m+1} + \cdots}$$

$\underline{a} = x^m \cdot \underline{u}$, $\underline{b} = x^n \cdot \underline{v}$ $\quad \underline{u}, \underline{v} \in \mathcal{U}(\mathbb{K}[[x]])$

Se $m \geq n$

$$\frac{\underline{a}}{\underline{b}} = x^{m-n} \cdot \underbrace{(\underline{u} \cdot \underline{v}^{-1})}_{\mathcal{U}(\mathbb{K}[[x]])}$$

$$\Rightarrow \quad \underline{a} = \underline{b} \cdot \underbrace{(x^{m-n} \cdot \underline{u} \cdot \underline{v}^{-1})}_{\underline{q}} + \underbrace{\underline{0}}_{\underline{r} = \underline{0}}$$

ok

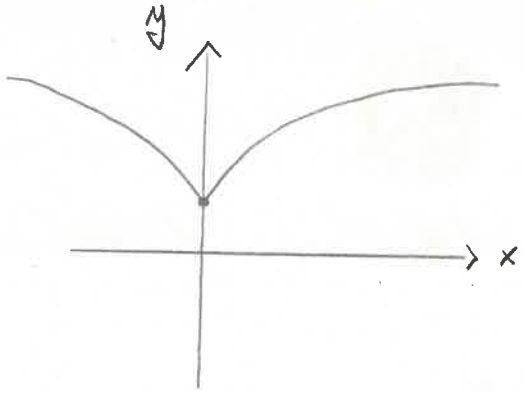
Se $m < n$

$$\underline{a} = \underline{b} \cdot \underbrace{\underline{0}}_{\underline{q}} + \underbrace{\underline{a}}_{\underline{r}}$$

Com $\nu(\underline{r}) = \nu(\underline{a}) = m < n = \nu(\underline{b})$ ok

Svolgimento esercizio 4

Consideriamo



$$C = \{ y^3 = x^2 + 1 \} \subset \mathbb{R}^2$$

Verificare che le uniche soluzioni in $\mathbb{Z} \times \mathbb{Z}$ (cioè punti interi) di C sono $(x, y) = (0, 1)$

* $C \cap (\mathbb{Z} \times \mathbb{Z}) \neq \emptyset$ poichè $(0,1) \in C \cap (\mathbb{Z} \times \mathbb{Z})$

* Sia $(x_0, y_0) \in C \cap (\mathbb{Z} \times \mathbb{Z})$ una soluzione

$\Rightarrow$ $x_0 \in \mathbb{Z}$ è necessariamente pari

Se p.a. x_0 dispari $\Rightarrow$ x_0^2 dispari $\Rightarrow$ $x_0^2 + 1$ pari

$\Rightarrow$ y_0^3 è pari $\Rightarrow$ y_0 è pari $\Rightarrow$ y_0^3 è t.c.

$$\boxed{y_0^3 \equiv 0 \pmod 8}$$

$\Rightarrow$ $x_0^2 + 1 \equiv 0 \pmod 8$ $\Rightarrow$ $x_0^2 \equiv -1 \pmod 8$

i.e. $x_0^2 \equiv 7 \pmod 8$

Ma Per $\forall\, x_0 \in \mathbb{Z}/8\mathbb{Z}$, $\{ x_0^2 \mid x_0 \in \mathbb{Z}/8\mathbb{Z} \} = \{0, 1, 4\}$

perciò $\nexists\, x_0 \in \mathbb{Z}/8\mathbb{Z}$ per cui $x_0^2 = 7$ in $\mathbb{Z}_8$

$\Rightarrow$ x_0 è pari ∎

(ii) $y^3 = x^2 + 1 = (x+i)(x-i)$

fattorizzazione in $(\mathbb{Z}[i])[x]$

Perciò se $(x_0, y_0) \in C \cap (\mathbb{Z} \times \mathbb{Z})$ è soluzione

$$(x_0+i),\ (x_0-i) \in \mathbb{Z}[i]$$

* Ora se coinsideriamo

$J := (x_0+i,\ x_0-i) \subset \mathbb{Z}[i]$ ideale

$\Rightarrow$ $x_0 + i - (x_0 - i) = 2i \in J$

$\Rightarrow$ $(-i)\cdot 2i = 2 \in J \cap \mathbb{Z}$

* Però $x_0^2 + 1 \in J$ perchè $x_0^2 + 1 = (x_0+i)(x_0-i) \in J$

e x_0 pari oltre (ii) $\Rightarrow$ $x_0^2 + 1 \in \mathbb{Z}$, dispari

$\Rightarrow$ $x_0^2 + 1 \in J \cap \mathbb{Z}$ e x_0^2+1 dispari

Poichè $x_0^2 + 1 = 2k + 1$, $k \in \mathbb{Z}$

$\Rightarrow$ $(x_0^2+1) - 2(k) = (2k+1) - 2k = 1$

$\Rightarrow$ $1 \in J$ $\Rightarrow$ $J = (1)$

$\Rightarrow$ $J = (x_0+i,\ x_0-i) = (1)$

$\Rightarrow$ $\exists\ \alpha, \beta \in \mathbb{Z}[i]$ t.c $(x_0+i)\cdot\alpha + (x_0-i)\beta = 1$

cioè $\boxed{MCD(x_0+i,\ x_0-i) = 1 \text{ in } \mathbb{Z}[i]}$

$\Rightarrow$ (x_0+i) e (x_0-i) coprimi in $\mathbb{Z}[i]$

(iii) Siccome $MCD(x_0+i, x_0-i)=1$ e

$$(x_0-i)(x_0+i) = y_0^3 \quad \text{in } \mathbb{Z}[i]$$

$y_0 \in \mathbb{Z} \subset \mathbb{Z}[i]$ euclideo $\Rightarrow$ DFU

$$y_0 = \prod_{j=1}^{k} \alpha_j \qquad \text{con } \alpha_j \in \mathbb{Z}[i]$$

tutti e soli gli irriducibili = primi di $\mathbb{Z}[i]$ della sua fattorizzazione (a meno di un.)

$$\Rightarrow \quad y_0^3 = \prod_{j=1}^{k} \alpha_j^3$$

$$\forall\, \alpha_j \mid y_0 \quad \Rightarrow \quad \alpha_j \mid (x_0-i)(x_0+i)$$

α_j primo $\Rightarrow$ $\alpha_j \mid (x_0-i)$ oppure $\alpha_j \mid (x_0+i)$

Siccome $MCD(x_0-i, x_0+i) = 1$, se $\alpha_j \mid (x_0-i) \Rightarrow \alpha_j \nmid (x_0+i)$

Perciò possiamo assumere $\exists$ indice t t.c.

$$1 < t \leq k$$

per cui $\alpha_j \mid (x_0-i)$ e $\alpha_j \nmid (x_0+i)$, $1 \leq j \leq t$

$\alpha_s \nmid (x_0-i)$ e $\alpha_s \mid (x_0+i)$, $t < s \leq k$

$$\Rightarrow \quad (x_0-i) = \alpha_1^3 \cdot \ldots \cdot \alpha_t^3 = (\alpha_1 \cdot \ldots \cdot \alpha_t)^3$$

$$(x_0+i) = (\alpha_{t+1} \cdot \ldots \cdot \alpha_s)^3$$

$\Rightarrow$ x_0-i e x_0+i cubi in $\mathbb{Z}[i]$.

(iv) Visto che (x_0+i) e (x_0-i) sono in $\mathbb{Z}[i] \Rightarrow$

$\exists (a+ib) \in \mathbb{Z}[i]$ t.c

$$(x_0+i) = (a+bi)^3 = (a^3-3ab^2) + i(3a^2b-b^3)$$

$$\Updownarrow$$

$$\begin{cases} x_0 = a(a^2-3b^2) \\ 1 = b(3a^2-b^2) \end{cases} \quad \text{in } \mathbb{Z}$$

(I)
(II)

Dalla (II) equazione in $\mathbb{Z}$

- se $b=1 \Rightarrow 3a^2 = 1 \not\Rightarrow a \in \mathbb{Z}$
- se $b=-1 \Rightarrow 3a^2 - 1 = -1 \Rightarrow 3a^2 = 0 \Rightarrow a = 0$

$$\Rightarrow \quad a+bi = -i \quad \text{i.e} \quad \boxed{a=0,\ b=-1}$$

Ma allora dalla (I) $\Rightarrow x_0 = 0 \Rightarrow y_0 = 1$

$$\boxed{(x_0, y_0) = (0,1)}$$ unica soluzione

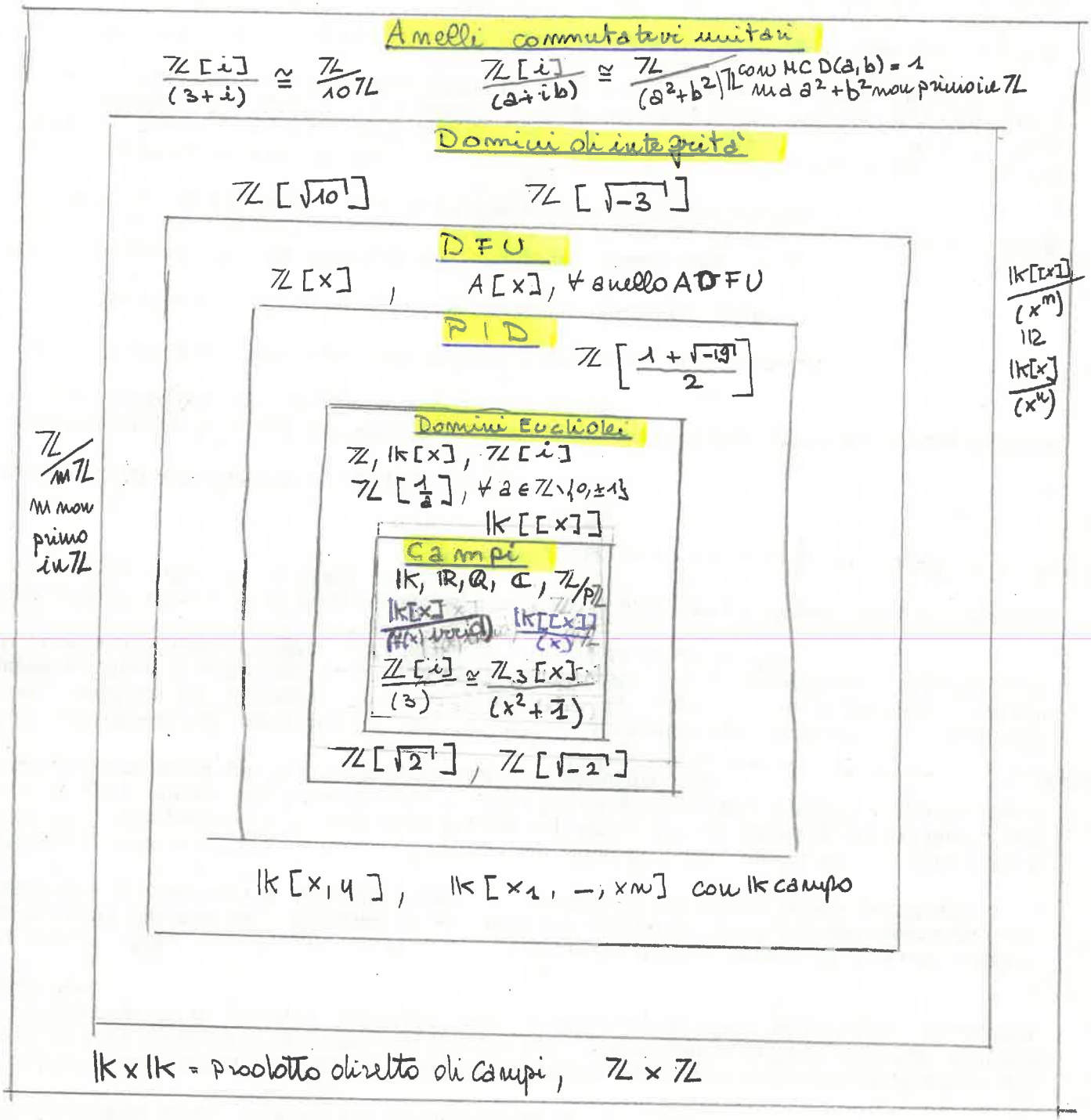
Approccio classico di risolvere problemi in anelli A e approcciarli in sovraanelli

$$A \subsetneq B$$

$\mathbb{Z} \qquad \mathbb{Z}[i]$

Quadro riassuntivo

Scatwisce alle tutti esercizi considerati



Svolgimento esercizio 5

(i) $(\mathbb{Z}, +, \cdot)$ dominio euclideo

$(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ prodotto diretto di domini euclidei

$$(m, n) \dot{+} (m', n') = (m \dot{+} m', n \dot{+} n')$$

operazioni anello = componente per componente

$(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$
* è commutativo
* è unitario, $(1,1)$ è sua unità molt.
* non è più dominio integro infatti

$$(1,0) \cdot (0,1) = (0,0)$$
$$\#(0,0) \qquad \#(0,0)$$

$\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z})$ = Gruppo automorfismi di anello $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$

i.e. $\varphi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$
omomorfismo iniettivo e suriettivo di anelli (è un automorfismo)

* Operazione di gruppo su $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z})$

$\varphi \circ \psi$ composizione automorfismi

* $\mathrm{Id}_{\mathbb{Z} \times \mathbb{Z}} \in \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z})$
* $\varphi \in \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}) \Rightarrow \varphi^{-1} \in \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z})$
* $\varphi, \psi \in \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}) \Rightarrow \varphi \circ \psi \in \mathrm{Aut}(\mathbb{Z} \times \mathbb{Z})$

Voglio determinare, a meno di isomorfismo di gruppi, la struttura di $(\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}), \circ)$

• Noto che in $(\mathbb{Z}\times\mathbb{Z}, +, \cdot)$ si ha:

$$(1,0)\cdot(1,0) = (1,0)$$

cioè $(1,0) \in \mathbb{Z}\times\mathbb{Z}$ è <u>idempotente</u>

$$\boxed{(1,0)^2 = (1,0) \quad \text{in } \mathbb{Z}\times\mathbb{Z}}$$

analogo $\boxed{(0,1)^2 = (0,1)}$

• Sia $(a,b) \in \mathbb{Z}\times\mathbb{Z}$ e assumiamo <u>(a,b) idempotente</u>

$$(a,b)^2 = (a^2, b^2) = (a,b)$$

(idempotenza)

$$\Leftrightarrow \begin{cases} a^2 = a \\ b^2 = b \end{cases} \Leftrightarrow \begin{cases} a(a-1) = 0 & \text{in } \mathbb{Z} \\ b\cdot(b-1) = 0 & \text{in } \mathbb{Z} \end{cases}$$

Siccome $\mathbb{Z}$ dominio

$$\text{o } \underline{a=0} \quad \text{o} \quad \underline{a=1}$$

$$\text{e } \underline{b=0} \quad \text{o} \quad \underline{b=1}$$

<u>quindi idempotenti in $\mathbb{Z}\times\mathbb{Z}$</u>

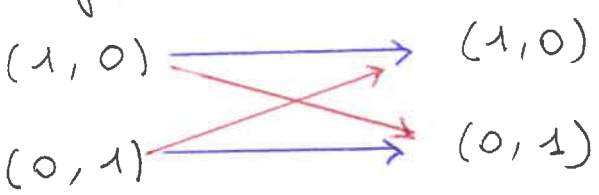
$$\boxed{\{(0,0), (1,1), (0,1), (1,0)\}}$$

• Visto che $\varphi \in \mathrm{Aut}(\mathbb{Z}\times\mathbb{Z}) \Rightarrow$

* <u>φ preserva struttura gruppo</u> $\Rightarrow \boxed{\varphi(0,0) = (0,0)}$

* φ automorfismo $\Rightarrow \varphi$ suriettivo e
$\varphi((1,1))$ opera come elemento neutro (prodotto) sinistro
e destro su tutto $\mathbb{Z}\times\mathbb{Z} \Rightarrow \boxed{\varphi((1,1)) = (1,1)}$

Perciò rimangono (iniettività e suriettività)



Nel caso $\rightarrow$

$\varphi((1,0)) = (1,0)$ $\quad$ e $\quad$ $\varphi((0,1)) = (0,1)$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

- $m > 0$

$$\varphi((m,0)) = \varphi(\underbrace{(1,0) + \dots + (1,0)}_{m\text{-volte}})$$

$$= \varphi((1,0)) + \dots + \varphi((1,0))$$

φ morf. Quelli

$$= \underbrace{(1,0) + \dots + (1,0)}_{m\text{-volte}}$$

$$= (m,0)$$

$\varphi((m,0)) = (m,0)$

analogo $\rightarrow$ $\varphi(0,m) = (0,m)$

- $\varphi((0,0)) = \varphi((1-1,0))$

$(0,0)$ $\qquad$ $\varphi((1,0)) + \varphi((-1,0))$

$(1,0) + \varphi((-1,0))$

$\Downarrow$

$\varphi((-1,0)) = -(1,0) = (-1,0)$ $\xrightarrow{\text{analogo}}$ $\varphi((0,-1)) = (0,-1)$

$\Downarrow$

$\forall m > 0$ $\quad \varphi((-m,0)) = (-m,0)$ $\longrightarrow$ $\varphi((0,-m)) = (0,-m)$

$$\Rightarrow \quad \varphi((m,n)) = \varphi((m,0) + (0,n)) =$$

$$= \varphi((m,0)) + \varphi((0,n))$$

$$= (m,0) + (0,n)$$

$$= (m,n) \qquad \forall (m,n) \in \mathbb{Z} \times \mathbb{Z}$$

$$\Rightarrow \quad \varphi = Id_{\mathbb{Z} \times \mathbb{Z}}$$

Nel caso $\longrightarrow$

$\varphi((1,0)) = (0,1) \quad \Rightarrow \quad \varphi((0,1)) = (1,0)$

$\Rightarrow$ iniett. e surjett.

Ma allora come prima

$\varphi((m,0)) = (0,m)$

$\varphi((0,m)) = (m,0)$

$$\boxed{\varphi((n,m)) = (m,n) \qquad \forall\ (n,m) \in \mathbb{Z} \times \mathbb{Z}}$$

Notiamo che per un tale $\varphi \neq Id_{\mathbb{Z}\times\mathbb{Z}}$

$$\varphi \circ Id_{\mathbb{Z}\times\mathbb{Z}} = Id_{\mathbb{Z}\times\mathbb{Z}} \circ \varphi = \varphi$$

$$\varphi \circ \varphi = Id_{\mathbb{Z}\times\mathbb{Z}}$$

Perciò

$$\boxed{(Aut(\mathbb{Z}\times\mathbb{Z}), \circ) = \langle \varphi \rangle \cong \left(\mathbb{Z}/2\mathbb{Z}, +\right)}$$

$\downarrow$

gruppo ciclico di ordine 2

Isomorfismo esplicito di gruppi

$$(Aut(\mathbb{Z}\times\mathbb{Z}), \circ) \xrightarrow{\cong} \left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right)$$

$$Id_{\mathbb{Z}\times\mathbb{Z}} \longrightarrow \bar{0}$$

$$\varphi \longrightarrow 1$$

(ii) Se invece considero solo

$(\mathbb{Z}\times\mathbb{Z}, +)$ gruppo abeliano

$$\boxed{(n, m) + (n', m') := (n+n', m+m')}$$

$(\mathbb{Z}\times\mathbb{Z}, +) \subset (\mathbb{R}\times\mathbb{R}, +)$ struttura gruppo compatibile

Inoltre $\mathbb{Z}$ agisce su $\mathbb{Z}\times\mathbb{Z}$

$$k \cdot (n, m) := (k\cdot n, k\cdot m)$$

Se $k>0$ $\quad k\cdot m = \underbrace{m + n + \cdots + m}_{k \text{ volte}}$

se $k<0$ $\quad k\cdot m = -|k|\cdot m = -(\underbrace{m+\cdots+m}_{|k|\text{-volte}})$

Azione compatibile con azione di $\mathbb{R}$ su $(\mathbb{R}\times\mathbb{R}, +)$

$\Downarrow$

struttura di $\mathbb{R}^2$ come $\mathbb{R}$-sp. vettoriale

$\Rightarrow$ $\mathbb{Z}\times\mathbb{Z} \subset \mathbb{R}^2$ $\Rightarrow$ vettori $\underline{v} = \begin{pmatrix} m \\ n \end{pmatrix}$ coordinate intere

Ora $Aut(\mathbb{R}^2)$ con $\mathbb{R}^2$ come spazio vettoriale

$$Aut(\mathbb{R}^2) = GL(2, \mathbb{R}) = \{ A \in M(2\times 2; \mathbb{R}) \mid \det(A) \neq 0 \}$$

$$\Psi$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$\Rightarrow$ $A \circ \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} am+bn \\ cm+dn \end{pmatrix} \in \mathbb{Z}\times\mathbb{Z}$ $\Leftrightarrow$ $a, b, c, d \in \mathbb{Z}$ perché $m, n \in \mathbb{Z}$

$\mathbb{Z}\times\mathbb{Z} \subset \mathbb{R}^2$

- Poiché $\varphi \in Aut(\mathbb{Z}\times\mathbb{Z}, +)$ $\Rightarrow$ $\exists\, \varphi^{-1} \in Aut(\mathbb{Z}\times\mathbb{Z}, +)$

Se $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\Rightarrow$ $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} +d & -b \\ -c & a \end{pmatrix}$

$\Rightarrow$ per fornire un elemento di $\mathbb{Z}\times\mathbb{Z}$ se applicato a $\begin{pmatrix} m' \\ n' \end{pmatrix}$

$\Rightarrow$ $\frac{1}{\det(A)} \in \mathbb{Z}$ $\Leftrightarrow$ $\det(A) \mid 1$ in $\mathbb{Z}$ $\Leftrightarrow$

$\det(A) \in U(\mathbb{Z})$ $\Leftrightarrow$ $\det(A) = \pm 1$

Perciò

$$\boxed{\mathrm{Aut}(\mathbb{Z}\times\mathbb{Z},+) = \{A \in GL(2,\mathbb{Z}) \mid \det(A) = \pm 1\}}$$

gruppo non abeliano di cardinalità infinita

$\Downarrow$

struttura di anello è molto più rigida rispetto automorfismi che quella di solo gruppo

Svolgimento esercizio 6

(i) $U(\mathbb{Z}/8\mathbb{Z}) = \{ a \in \mathbb{Z}/8\mathbb{Z} \mid MCD(a,8) = 1 \}$

$$|U(\mathbb{Z}/8\mathbb{Z})| = \varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 2^2(2-1) = 4$$

φ = Phi di Eulero

è un gruppo con 4 elementi

$$U(\mathbb{Z}/8\mathbb{Z}) = \{ \overline{1}, \overline{3}, \overline{5}, \overline{7} \}$$

$\overline{3}\cdot\overline{3} = \overline{9} = \overline{1}$
$\overline{5}\cdot\overline{5} = \overline{25} = \overline{1}$
$\overline{7}\cdot\overline{7} = \overline{49} = \overline{1}$

$\Rightarrow$ $\text{ord}(\overline{3}) = \text{ord}(\overline{5}) = \text{ord}(\overline{7}) = 2$
$\text{ord}(\overline{1}) = 1$

$\Rightarrow$ $U(\mathbb{Z}/8\mathbb{Z})$ NON È CICLICO

- Per Lagrange i possibili sottogruppi hanno cardinalità che dividono $|U(\mathbb{Z}/8\mathbb{Z})| = 4$

$\Downarrow$

divisori di 4 : 1, 2, 4

- Sgr. ordine 1 : $\{\overline{1}\}$
- Sgr. ordine 4 : $U(\mathbb{Z}/8\mathbb{Z})$

  > banali

- Sgr. di ordine 2 : $\{\overline{1}, \overline{3}\}$
  $\{\overline{1}, \overline{5}\}$
  $\{\overline{1}, \overline{7}\}$

  ci sono 3 diversi con lo stesso ordine

$$U(\mathbb{Z}/8\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$$

Gruppo di Klein

Esplicito isomorfismo

$$\mathcal{U}(\mathbb{Z}/8\mathbb{Z}) \xrightarrow{\ \psi\ \cong\ } (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$$

$$\bar{1} \longrightarrow ([0], [0])$$

$$\bar{3} \longrightarrow ([1], [0])$$

$$\bar{5} \longrightarrow ([0], [1])$$

$$\bar{7} \longrightarrow ([1], [1])$$

Infatti

$$\bar{3} \cdot \bar{5} = \overline{15} = \bar{7} \Rightarrow \psi(\bar{3} \cdot \bar{5}) = \psi(\bar{3}) + \psi(\bar{5})$$

$$\psi(\bar{3} \cdot \bar{5}) = \psi(\bar{7})$$

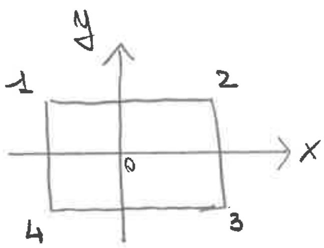
$$\psi(\bar{3}) + \psi(\bar{5}) = ([1],[0]) + ([0],[1]) = ([1],[1])$$

analogo con altri

$$\bar{3} \cdot \bar{7} = \bar{5}$$

$$\bar{7} \cdot \bar{5} = 3$$

Anche simmetrie quadrato $\cong$ Klein



$\{Id, \sigma_x, \sigma_y, \sigma_x \circ \sigma_y\}$, $\quad \sigma_x \circ \sigma_y = \sigma_0$

oppure in $S_4 = \text{Sym}(4)$

$$\{Id, (1,4)(2,3), (1,2)(3,4), (1,3)(2,4)\}$$

$$\cong$$

Klein

(ii) $U(\mathbb{Z}/9\mathbb{Z})$

$$|U(\mathbb{Z}/9\mathbb{Z})| = \varphi(9) = \varphi(3^2) = 3^2 - 3 = 3(3-1) = 6$$

$$U(\mathbb{Z}/9\mathbb{Z}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$$

I possibili sottogruppi di $U(\mathbb{Z}/9\mathbb{Z})$ hanno cardinalità
$1, 2, 3, 6$

* 1 e 6 → sottogruppi banali

* $\bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{8}, \bar{2}^4 = \bar{2}^3 \cdot \bar{2} = \bar{8} \cdot \bar{2} = \bar{16} = \bar{7}, \bar{2}^5 = \bar{2}^4 \cdot \bar{2} = \bar{7} \cdot \bar{2} = \bar{14} = \bar{5}$
$\bar{2}^6 = \bar{2}^5 \cdot \bar{2} = \bar{5} \cdot \bar{2} = \bar{10} = \bar{1}$

$\Rightarrow$ $U(\mathbb{Z}/9\mathbb{Z}) = \langle \bar{2} \rangle$ ciclico $\Rightarrow$ $\cong \left(\frac{\mathbb{Z}}{6\mathbb{Z}}, +\right)$

$\Rightarrow$ ogni sottogruppo è ciclico

* Poiché $|U(\mathbb{Z}/9\mathbb{Z})| = 6$

ricordo che $\forall\, g \in G$ t.c. $|G| = n \Rightarrow g^n = Id_G$

$\Rightarrow$ gli esponenti coprimi con 6 forniscono altri generatori i.e.

- $U(\mathbb{Z}/9\mathbb{Z}) = \langle \bar{2} \rangle = \langle \bar{2}^5 = \bar{5} \rangle$ $\Rightarrow$ $\bar{2}$ e $\bar{5}$ generatori di $U(\mathbb{Z}/9\mathbb{Z})$
- $\langle \bar{2}^2 = 4 \rangle$ sottogruppo di ordine $\frac{6}{2} = 3$

in fatti

$$\langle \bar{2}^2 \rangle = \{\bar{2}^2 = \bar{4},\ \bar{2}^4 = \bar{7},\ \bar{2}^6 = \bar{1}\} \cong \left(\frac{\mathbb{Z}}{3\mathbb{Z}}, +\right)$$
$$= \langle \bar{4} \rangle = \langle \bar{7} \rangle$$

- $\langle \bar{2}^3 = \bar{8} \rangle$ sottogruppo di ordine $\frac{6}{3} = 2$

$$\langle \bar{2}^3 \rangle = \{\bar{8}, \bar{1}\} \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right)$$

$\mapsto$ Lagrange si inverte con ciclicità nei gruppi ciclici
cioè $\forall$ divisore di $|G|$, G ciclico, $\exists!$ sgr. di quell'ordine

(iii) $U(\mathbb{Z}/10\mathbb{Z})$

$$|U(\mathbb{Z}/10\mathbb{Z})| = \varphi(10) = \varphi(5\cdot 2) = \varphi(5)\cdot\varphi(2)$$
$$= 4 \cdot 1 = 4$$

$$|U(\mathbb{Z}/10\mathbb{Z})| = 4 = |U(\mathbb{Z}/8\mathbb{Z})|$$

$$U(\mathbb{Z}/10\mathbb{Z}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

$\overline{3}^2 = \overline{9}$, $\overline{3}^3 = \overline{27} = \overline{7}$, $\overline{3}^4 = \overline{7}\cdot\overline{3} = \overline{21} = \overline{1}$

$\Rightarrow$ $\text{ord}(\overline{3}) = 4$ $\Rightarrow$

$U(\mathbb{Z}/10\mathbb{Z})$ È CICLICO

Pure se $|U(\mathbb{Z}/10\mathbb{Z})| = |U(\mathbb{Z}/8\mathbb{Z})| = 4$

$\Rightarrow$ $U(\mathbb{Z}/10\mathbb{Z}) \not\cong U(\mathbb{Z}/8\mathbb{Z})$

$U(\mathbb{Z}/10\mathbb{Z})$ → è ciclico. Lagrange si inverte con ciclicità

$U(\mathbb{Z}/8\mathbb{Z})$ → gruppo di Klein: tutti elementi hanno periodo 2, e ammette 3 sottogruppi di stesso ordine 2

Infatti

- $U(\mathbb{Z}/10\mathbb{Z}) = \langle \overline{3} \rangle = \langle \overline{3}^3 = \overline{7} \rangle$ (112) $(\mathbb{Z}/4\mathbb{Z}, +)$ — generatori; potenze coprime con 4
- $\langle \overline{3}^2 = \overline{9} \rangle = \{\overline{9}, \overline{9}^2 = \overline{3}^4 = \overline{1}\} \cong (\mathbb{Z}/2\mathbb{Z}, +)$

genera un unico sottogruppo proprio di ordine 2

Svolgimento esercizio 7

(i) $(Aut(\mathbb{Z}/12\mathbb{Z}, +), 0)$ struttura a meno di isomorfismo

$(\mathbb{Z}/12\mathbb{Z}, +)$ è CICLICO

Da chi è generato?

$\mathbb{Z}/m\mathbb{Z} = \langle \bar{a} \rangle \iff$ $ord(\bar{a}) = m$ e non di meno quando?

Se $a \in \mathbb{Z}$ è un intero t.c.

$MCD(a, m) = d > 1 \Rightarrow$

$a = d \cdot a'$ e $m = d \cdot m'$, $m' < m$

si ha allora

$$m' \cdot a = m' d \cdot a' = m \cdot a'$$

cioè $\underbrace{a + a + \dots + a}_{m' \text{ volte}} \equiv 0 \pmod{m}$

cioè $ord(a) = m' < m$

Perciò cerco $a \in \mathbb{Z}/12\mathbb{Z}$ t.c.

$MCD(a, 12) = 1$ per trovare i generatori

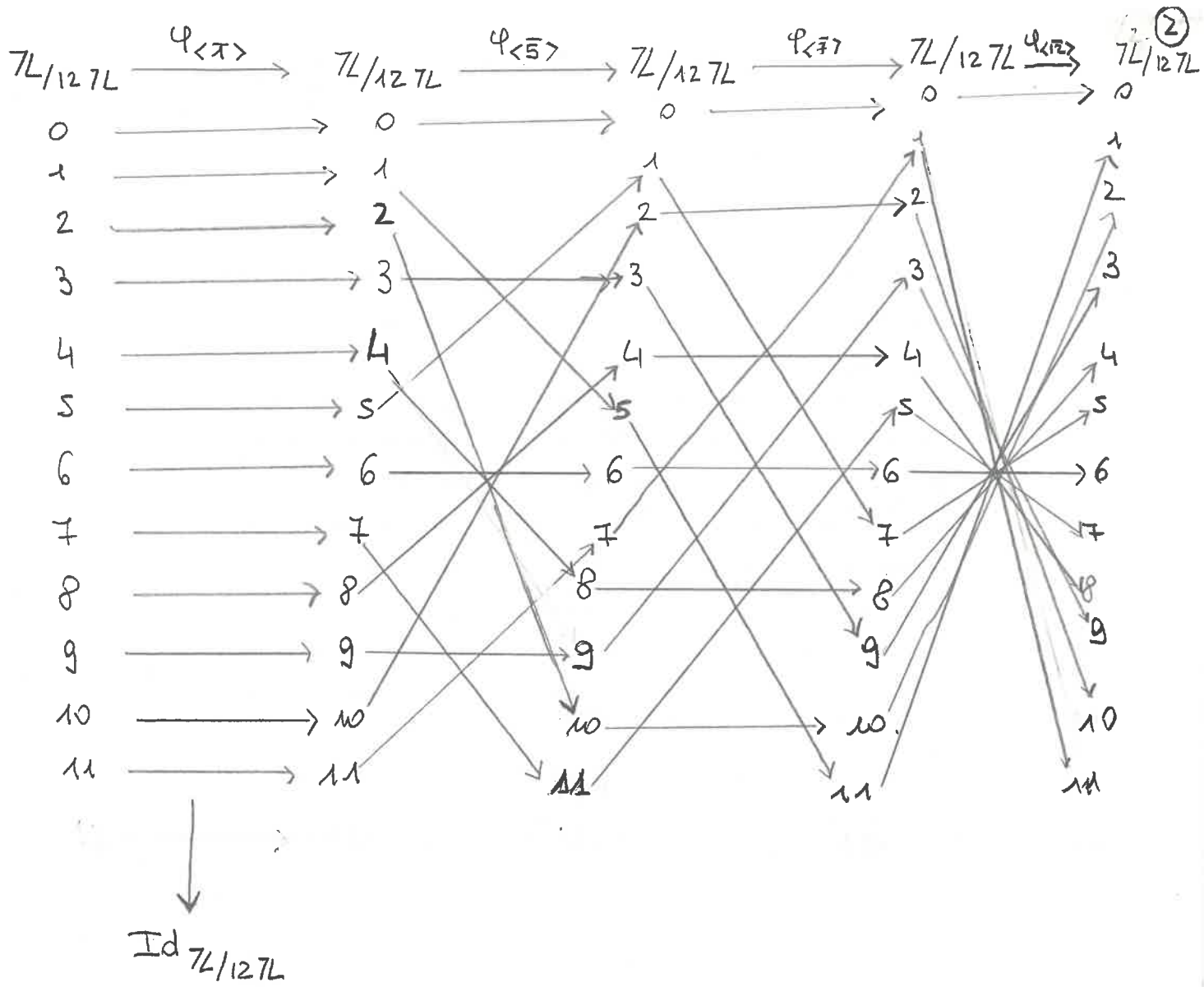
$$\left(\mathbb{Z}/12\mathbb{Z}, +\right) = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$$

Perciò

$$\text{Generatori di } \left(\mathbb{Z}/12\mathbb{Z}, +\right) = U(\mathbb{Z}/12\mathbb{Z})$$

- Poichè in un automorfismo di $(\mathbb{Z}/12\mathbb{Z}, +)$ generatori vanno in generatori $\Rightarrow$

$$Aut(\mathbb{Z}/12\mathbb{Z}) \cong U(\mathbb{Z}/12\mathbb{Z})$$



(ii) $(\mathbb{Z}/12\mathbb{Z}, +)$ è ciclico di cardinalità 12

$(\mathbb{Z}/13\mathbb{Z}, +, \cdot)$ campo finito perché $p = 13$ primo

$\Rightarrow \mathcal{U}(\mathbb{Z}/13\mathbb{Z}) = (\mathbb{Z}/13\mathbb{Z})^* = \mathbb{Z}/13\mathbb{Z} \setminus \{0\}$

che ha cardinalità 12

Poiché $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ è SEMPRE CICLICO per un campo finito

$\Rightarrow$ Per forza

$$\boxed{(\mathbb{Z}/12\mathbb{Z}, +) \cong (\mathcal{U}(\mathbb{Z}/13\mathbb{Z}), \cdot)}$$

per determinare un isomorfismo esplicito basta considerare $(\mathbb{Z}/12\mathbb{Z}, +) = \langle \bar{1} \rangle$, $\mathcal{U}(\mathbb{Z}/13\mathbb{Z}) = \langle \bar{2} \rangle$ e considerare $\varphi : \bar{1} \to \bar{2}$ e poi operare di conseguenza sugli altri elementi

(iii) Tutti i gruppi immagine omomorfa di

$\mathbb{Z}/12\mathbb{Z}$

Cerco $H \leq \mathbb{Z}/12\mathbb{Z}$ (che è ciclico)

$\Rightarrow$ La proiezione si inverte con minimità

$\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$ generatori

Mentre

$$\text{ord}(\bar{a}) = \frac{m}{MCD(a,m)} \quad \text{in } \mathbb{Z}/m\mathbb{Z}$$

Perciò

$\text{ord}(\bar{2}) = \frac{12}{2} = 6 = \text{ord}(\bar{10})$

$\text{ord}(\bar{3}) = \frac{12}{3} = 4 = \text{ord}(\bar{9})$

$\text{ord}(\bar{6}) = \frac{12}{6} = 2$

$\text{ord}(\bar{4}) = \frac{12}{4} = 3$

Se uso $H = \langle \bar{0} \rangle$ $\quad \mathbb{Z}/12\mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}/12\mathbb{Z}$

Se uso $H = \mathbb{Z}/12\mathbb{Z}$ $\quad \mathbb{Z}/12\mathbb{Z}/H = \{0\}$

Se uso $H = \langle \bar{2} \rangle = \langle \bar{10} \rangle$ $\quad \mathbb{Z}/12\mathbb{Z} / 2\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$

Se uso $H = \langle \bar{3} \rangle = \langle \bar{9} \rangle$ $\quad \mathbb{Z}/12\mathbb{Z} / 3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$

Se uso $H = \langle \bar{6} \rangle$ $\quad \mathbb{Z}/12\mathbb{Z} / 6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$

Se uso $H = \langle \bar{4} \rangle$ $\quad \mathbb{Z}/12\mathbb{Z} / 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$

$\rightarrow$ Tutti i gruppi (a meno di iso) Immagine omomorfa di $\mathbb{Z}/12\mathbb{Z}$

(iv) $U(\mathbb{Z}/12\mathbb{Z}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

$|U(\mathbb{Z}/12\mathbb{Z})| = \Phi(12) = 4$

Poiché $\overline{5}\cdot\overline{5} = \overline{25} = \overline{1}$
$\overline{7}\cdot\overline{7} = \overline{49} = \overline{1}$
$\overline{11}\cdot\overline{11} = \overline{121} = \overline{1}$

$\Rightarrow$ ogni elemento non $\overline{1}$ ha ordine 2

$\Downarrow$

$U(\mathbb{Z}/12\mathbb{Z}) \cong$ Gruppo di Klein $= \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

- Abbiamo già visto che ha 3 sottogruppi propri di ordine 2 ed i due banali $\{\overline{1}\}$ e $U(\mathbb{Z}/12\mathbb{Z})$

$\Downarrow$

I gruppi immagine omomorfa di $U(\mathbb{Z}/12\mathbb{Z})$ sono

* $\dfrac{U(\mathbb{Z}/12\mathbb{Z})}{\{0\}} \cong U(\mathbb{Z}/12\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ Klein

* $\dfrac{U(\mathbb{Z}/12\mathbb{Z})}{U(\mathbb{Z}/12\mathbb{Z})} \cong \{0\}$ gruppo nullo

* $\dfrac{U(\mathbb{Z}/12\mathbb{Z})}{\langle\overline{5}\rangle} \cong \dfrac{U(\mathbb{Z}/12\mathbb{Z})}{\langle\overline{7}\rangle} \cong \dfrac{U(\mathbb{Z}/12\mathbb{Z})}{\langle\overline{11}\rangle} \cong \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\downarrow}$

ciclico di ordine 2