

Università degli Studi di Roma "Tor Vergata"

CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2024-2025

Esame scritto del 9 Settembre 2025 — 3° appello, sessione autunnale

N.B.: compilare il compito in modo sintetico ma esauriente, spiegando chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.

..... *

[1] — Si consideri l'anello quoziente

$$A := (\mathbb{Z}_5[x])[y, y^{-1}] / (x^2 - 4y^{-1}, y - 8)$$

- (a) Determinare se A sia un campo.
- (b) Determinare la cardinalità di A .
- (c) Determinare la classe di isomorfismo del gruppo $U(A)$ delle unità dell'anello A .
- (d) Per ciascuno dei valori $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, determinare se nell'anello A esistano radici n -esime primitive dell'unità.

[2] — Si consideri il polinomio $f(x) := x^3 + 4x^2 + 10x - 6 \in \mathbb{F}_7[x]$, nella variabile x , a coefficienti nel campo $\mathbb{F}_7$ di sette elementi. Sia poi $\mathbb{K}_f$ l'anello quoziente $\mathbb{K}_f := \mathbb{F}_7[x] / (f(x))$.

- (a) Dimostrare che $\mathbb{K}_f$ è un campo.
- (b) Determinare la cardinalità di $\mathbb{K}_f$.
- (c) Determinare la classe di isomorfismo del gruppo di Galois $\text{Gal}(\mathbb{K}_f / \mathbb{F}_7)$ dell'estensione di campi $\mathbb{K}_f / \mathbb{F}_7$.
- (d) Determinare il numero dei campi intermedi tra $\mathbb{F}_7$ e $\mathbb{K}_f$.

[3] — Dato un numero naturale *dispari* $n \in (2\mathbb{N} + 1)$, si consideri il gruppo generale lineare $G := GL_n(\mathbb{Q})$ delle matrici quadrate invertibili $n \times n$ a coefficienti nel campo $\mathbb{Q}$, e siano $G_+ := \{ M \in G \mid \det(M) > 0 \}$ e $G_- := \{ M \in G \mid \det(M) < 0 \}$.

(a) Dimostrare che G_+ è sottogruppo normale di G .

(b) Dimostrare che G_- non è sottogruppo di G .

(c) Dimostrare che esiste in G un sottogruppo normale Z tale che G sia isomorfo al prodotto diretto di Z con G_+ , in formule $G \cong Z \times G_+$.

[4] — Sia $\mathbb{Z}[\sqrt{-11}] := \{ z \in \mathbb{C} \mid \exists a, b \in \mathbb{Z} : z = a + b\sqrt{-11} \}$.

(a) Dimostrare che $\mathbb{Z}[\sqrt{-11}]$ è un sottoanello di $\mathbb{C}$.

(b) Determinare se $\mathbb{Z}[\sqrt{-11}]$ sia un dominio (oppure no!).

(c) Determinare se l'ideale $I := (3, -1 + \sqrt{-11})$ in $\mathbb{Z}[\sqrt{-11}]$ sia principale (oppure no!).

(d) Determinare se $\mathbb{Z}[\sqrt{-11}]$ sia un dominio a fattorizzazione (non necessariamente unica).

(e) Determinare se $\mathbb{Z}[\sqrt{-11}]$ sia un dominio a fattorizzazione unica.

(f) Determinare se $\mathbb{Z}[\sqrt{-11}]$ sia un dominio a ideali principali.

(g) Determinare se $\mathbb{Z}[\sqrt{-11}]$ sia un dominio euclideo.

[5] — Siano G un gruppo, S ed S' due G -spazi, e $\varphi : S \longrightarrow S'$ un'applicazione tale che $\varphi(g.s) = g.\varphi(s)$ per ogni $g \in G$, $s \in S$.

Indicando con $\mathcal{O}_x$ e con St_x rispettivamente l'orbita e lo stabilizzatore di un punto x (in un qualsiasi G -spazio), dimostrare che:

(a) $\varphi(\mathcal{O}_s) = \mathcal{O}_{\varphi(s)}$ per ogni $s \in S$;

(b) $|St_{\varphi(s)}| \geq |St_s|$ per ogni $s \in S$;

(c) $St_{\varphi(s)} \supseteq St_s$ per ogni $s \in S$.

ALGEBRA 2

SCRITTO del 9 SETTEMBRE 2025

— 0 —

[1] Sia $A := (\mathbb{Z}_5[x])[y, y^{-1}]$

$$\frac{\quad}{(x^2 - 4y^{-1}, y - 8)}$$

[Th:] (a) A è campo?

(b) Calcolare $|A|$.

(c) A quale gruppo è isomorfo $U(A)$?

(d) $\forall n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$,
esiste in A una radice n° primitiva
dell'unità?

Svolgimento:

Il Teorema del Doppio Quoziente da'

$$A := (\mathbb{Z}_5[x])[y, y^{-1}] \frac{\quad}{(x^2 - 4y^{-1}, y - 8)} \cong$$

$$\cong \frac{(\mathbb{Z}_5[x])[y, y^{-1}]}{(y - 8)} \frac{\quad}{(y - 8, x^2 - 4y^{-1})} \cong$$

$$\frac{\quad}{(y - 8)}$$

- 1 -

$$\mathbb{Z}_5[x] \big/ (x^2 - 4 \cdot 8^{-1}) = \mathbb{Z}_5[x] \big/ (x^2 - 3)$$

perché $(\mathbb{Z}_5[x])[y, y^{-1}] \cong \mathbb{Z}_5[x]$

$$\phi_*: \frac{(\mathbb{Z}_5[x])[y, y^{-1}]}{(y-8)} \xrightarrow{f(y, y^{-1}) \mapsto f(8, 8^{-1})} \mathbb{Z}_5[x]$$

tramite un isomorfismo indotto
(mediante il Teorema Fondamentale di
Isomorfismo) dal morfismo

$$\phi: (\mathbb{Z}_5[x])[y, y^{-1}] \longrightarrow \mathbb{Z}_5[x]$$

$$f(y, y^{-1}) \longmapsto f(8, 8^{-1}) = f(3, 3^{-1})$$

Inoltre, tramite l'isomorfismo ϕ_*
l'ideale $(y-8, x^2 - 4 \cdot y^{-1}) / (y-8)$ ha

per immagine l'ideale generato da

$$\phi_*(\overline{y-8}) = \phi(y-8) = 0 \text{ e da}$$

$$\begin{aligned} \phi_*(\overline{x^2 - 4 \cdot y^{-1}}) &= \phi(x^2 - 4y^{-1}) = x^2 - 4 \cdot 8^{-1} = \\ &= x^2 - 4 \cdot 3^{-1} = x^2 - 4 \cdot 2 = x^2 - 8 = x^2 - 3 \end{aligned}$$

Ora, $\alpha^2 \in \{0, 1, 4\} \quad \forall \alpha \in \mathbb{Z}_5, \Rightarrow$

$\Rightarrow \nexists \alpha \in \mathbb{Z}_5 : (x^2 - 3)(\alpha) = 0 \Rightarrow$

$\Rightarrow (x^2 - 3)$ è irriducibile in $\mathbb{Z}_5[x] \Rightarrow$

$\Rightarrow \mathbb{Z}_5[x]/(x^2 - 3)$ è campo, ~~o~~ A

estensione di $\mathbb{Z}_5$ di grado 2, $\Rightarrow$

$\Rightarrow A$ è campo $\rightsquigarrow$ (a)

& $|A| = |\mathbb{Z}_5^{x^2}| = 5^2 = 25$ $\rightsquigarrow$ (b)

Allora $U(A) = A \setminus \{0\}$ è ciclico di ordine $25 - 1 = 24$, cioè

$(U(A); \cdot) \cong (\mathbb{Z}_{24}; +)$ $\leftarrow$ ciclico $\rightsquigarrow$ (c)

QUINDI $\exists \alpha \in U(A)$ radice n^{a} prim. di 1



n divide 24



$n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$

DUNQUE la risposta a (d) è

$\forall n \in \{2, 3, 4, 6, 8, 12\}.$

$$\boxed{2} \quad f(x) := x^3 + 4x^2 + 10x - 6 \in \mathbb{F}_7[x]$$

$$K_f := \mathbb{F}_7[x] / (f(x))$$

- (a) K_f è campo.
- (b) $|K_f| = ?$
- (c) $\text{Gal}(K_f/\mathbb{F}_7) \cong ?$ (come gruppo)
- (d) Quanti sono i campi intermedi tra $\mathbb{F}_7$ e K_f ?

Svolgimento:

$$(a) \quad K_f := \mathbb{F}_7[x] / (f(x)) \text{ è campo } \Leftrightarrow$$

$$\Leftrightarrow f(x) \text{ è irriducibile in } \mathbb{F}_7[x] \Leftrightarrow$$

$$\Leftrightarrow \nexists \alpha \in \mathbb{F}_7 \text{ radice di } f(x)$$

MA i calcoli danno

$$f(0) = -6 \neq 0, \quad f(1) = -5 \neq 0, \quad f(2) = -4 \neq 0, \\ f(3) = -4 \neq 0, \quad f(4) = -6 \neq 0, \quad f(5) = 3 \neq 0, \quad f(6) = -6 \neq 0$$

QUINDI $\nexists$ radici di $f(x)$ in $\mathbb{F}_7$, $\Rightarrow$

$\Rightarrow K_f$ è campo and (a)

(b) $K_f := \mathbb{F}_2[x] / (f(x))$ è campo (per (a)),
estensione di $\mathbb{F}_2$ di grado $d := \partial(f(x)) = 3$,

QUINDI

$$|K_f| = |\mathbb{F}_2|^d = 2^3 = 343 \text{ end (b)}$$

(c) $K_f := \mathbb{F}_2[x] / (f(x))$ è il campo

di cardinalità $2^3 = 343$, ~~quindi~~

estensione di $\mathbb{F}_2$ di grado 3, QUINDI

$\text{Gal}(K_f/\mathbb{F}_2)$ è ciclico di ordine 3,
generato dall'automorfismo di Frobenius

$$\phi: K_f \longrightarrow K_f, \alpha \longmapsto \phi(\alpha) := \alpha^2$$

così $\text{Gal}(K_f/\mathbb{F}_2) = \langle \phi \rangle \cong (\mathbb{Z}_3; +)$ end (c)

(d) I campi intermedi $E: \mathbb{F}_2 \subseteq E \subseteq K_f$

sono in biiezione con i sottogruppi di

$$\text{Gal}(K_f/\mathbb{F}_2) \cong \mathbb{Z}_3, \text{ che sono}$$

soltanto $\{id\}$ e $\text{Gal}(K_f/\mathbb{F}_2)$

QUINDI i suddetti campi intermedi sono
esattamente 2, cioè K_f e $\mathbb{F}_2$.

OPPURE

(più semplice) Sia E un campo

$$\text{t. c. } \mathbb{F}_2 \subseteq E \subseteq \mathbb{K}_f$$

La moltiplicatività del grado ci dà

$$[\mathbb{K}_f : E] \cdot [E : \mathbb{F}_2] = [\mathbb{K}_f : \mathbb{F}_2] = 3$$

e quindi $[E : \mathbb{F}_2]$ divide 3, dunque dev'essere

$$[E : \mathbb{F}_2] = 1 \Rightarrow E = \mathbb{F}_2$$

oppure

$$[E : \mathbb{F}_2] = 3 \Rightarrow [\mathbb{K}_f : E] = \frac{[\mathbb{K}_f : \mathbb{F}_2]}{[E : \mathbb{F}_2]} = \frac{3}{3} = 1$$

$$\text{cioè } [\mathbb{K}_f : E] = 1, \Rightarrow E = \mathbb{K}_f$$

DUNQUE è $E = \mathbb{F}_2$ o $E = \mathbb{K}_f$

perciò i possibili campi intermedi sono soltanto questi 2 (in particolare, ne esistono esattamente 2).

3 Sia $n \in (2N+1)$, $G := GL_n(\mathbb{Q})$

$$G_+ := \{M \in G \mid \det(M) > 0\} \quad \text{e}$$

$$G_- := \{M \in G \mid \det(M) < 0\}.$$

Th: (a) $G_+ \trianglelefteq G$;

(b) $G_- \not\trianglelefteq G$;

(c) $\exists Z \trianglelefteq G : G \cong Z \times G_+.$

Svolgimento:

(a) L'applicazione $\phi: G \longrightarrow (\{+1, -1\}; \cdot)$

data da $\phi(M) := \det(M) \cdot |\det(M)|^{-1}$ è

un morfismo di gruppi (essenzialmente per il teorema di Binet, che garantisce che

$$\det(A \cdot B) = \det(A) \cdot \det(B) \quad \forall A, B \text{ matrici } n \times n),$$

e si ha, $\forall M \in G := GL_n(\mathbb{Q})$,

$$M \in \ker(\phi) \Leftrightarrow \phi(M) = 1 \Leftrightarrow$$

$$\Leftrightarrow \det(M) \cdot |\det(M)|^{-1} = 1 \Leftrightarrow$$

$$\Leftrightarrow \det(M) = |\det(M)| \Leftrightarrow$$

$$\Leftrightarrow \det(M) > 0 \Leftrightarrow M \in G_+$$

(con
 $|x| :=$ valore
assoluto
di x ,
 $\forall x \in \mathbb{Q} \setminus \{0\}$)

QUINDI $\bar{e} \in \text{Ker}(\phi) = G_+$, e allora

$$G_+ = \text{Ker}(\phi) \trianglelefteq G \quad \text{ovvero (a)}$$

(b) $G_- \not\leq G$, cioè G_- non è un sottogruppo di G , ad esempio perché non contiene l'identità del gruppo $G := GL_n(\mathbb{Q})$, che è $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, in quanto $\det(I_n) = 1 \neq 0$

OPPURE

perché $\forall A, B \in G_-$ (e tali A, B esistono...) si ha $A \cdot B \notin G_-$, quindi G_- non è chiuso per il prodotto.

(c) Si consideri la matrice

$$-I_n = \begin{pmatrix} -1 & & 0 \\ & -1 & \\ 0 & & \ddots \\ & & & -1 \end{pmatrix} = (-1) \cdot I_n$$

Per esso si ha

$$\begin{aligned} \det(-I_n) &= \det((-1) \cdot I_n) = \\ &= (-1)^n \cdot \det(I_n) = (-1)^n \cdot 1 = (-1)^n = -1 < 0 \end{aligned}$$

cioè $\det(-I_n) = -1 < 0$

QUINDI $(-I_n) \in G_-$, e $(-I_n) \notin G_+$

N.B.: qui si sfrutta l'ipotesi che $n \in (2N+1)$, cioè n è dispari

Gia $Z := \langle -I_n \rangle = \{-I_n, I_n\} \quad (\cong (\mathbb{Z}_2; +))$

il sottogruppo di G generato da $(-I_n)$.

Ovviamente è

$$(-I_n) \cdot M = M \cdot (-I_n) \quad \forall M \in G$$

quindi $(-I_n) \in Z(G) :=$ centro di G ,

e così in particolare $Z \leq Z(G)$, da cui segue che $Z \trianglelefteq G$.

Poiché $(-I_n) \notin G_+$ e $Z = \{-I_n, I_n\}$ si ha

$$Z \cap G_+ = \{I_n\} \quad (1)$$

mentre

$$G_+ \trianglelefteq G, \quad Z \trianglelefteq G \quad (2)$$

Infine, $\forall M \in G$ si ha (cf. pag. 5)

$$\varepsilon_M := \phi(M) \in \{+1, -1\}$$

che si sa

$$M = (\varepsilon_M \cdot I_n) \cdot (\varepsilon_M M) \quad (3)$$

$$\text{con } \varepsilon_M \cdot I_n \in \{-I_n, I_n\} = \mathbb{Z} \quad (4)$$

e $\varepsilon_M \cdot M \in G$ tale che

$\varepsilon_M^n = \varepsilon_M$ perché
 $n \in (2\mathbb{N}+1)$

$$\det(\varepsilon_M M) = \varepsilon_M^n \cdot \det(M) = \varepsilon_M \cdot \det(M) =$$

$$= \det(M) \cdot |\det(M)|^{-1} \cdot \det(M) =$$

$$= |\det(M)| \cdot \det(M)^{-1} \cdot \det(M) = |\det(M)|$$

((perché $q \cdot |q|^{-1} = |q| \cdot q^{-1}$, $\forall q \in \mathbb{Q} \setminus \{0\}$))

$$\text{cioè } \det(\varepsilon_M \cdot M) = |\det(M)| > 0$$

ossia che

$$\varepsilon_M \cdot M \in G_+$$

(5)

ALLORA (3) insieme a (4) e (5) ci dà

$$G = \mathbb{Z} \cdot G_+$$

(6)

e infine $(1) + (2) + (6)$ ci dà

$$G \cong \mathbb{Z} \times G_+$$

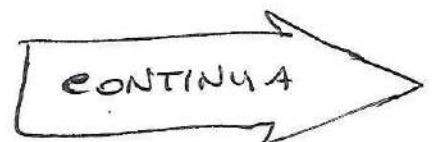
dove un isomorfismo esplicito è
dato proprio da

$$\begin{aligned} G &\xrightarrow{\cong} \mathbb{Z} \times G_+ \\ M &\longmapsto (\varepsilon_M I_n, \varepsilon_M M) \end{aligned}$$

con inverso

$$\begin{aligned} \mathbb{Z} \times G_+ &\longrightarrow G \\ (z, M_+) &\longmapsto z \cdot M_+ := (z \cdot m_{ij})_{\substack{\hat{i}=1, \dots, n; \\ \hat{j}=1, \dots, n;}} \\ &\text{se } M_+ := (m_{ij})_{\substack{\hat{i}=1, \dots, n; \\ \hat{j}=1, \dots, n;}} \end{aligned}$$

il che dimostra (c).



$$\boxed{4} \quad \mathbb{Z}[\sqrt{-11}] := \{ z \in \mathbb{C} \mid \exists a, b \in \mathbb{Z} : z = a + b\sqrt{-11} \}$$

$\boxed{\text{Th:}}$ (a) $\mathbb{Z}[\sqrt{-11}]$ è sottoanello di $\mathbb{C}$.

(b) $\mathbb{Z}[\sqrt{-11}]$ è dominio?

(c) L'ideale $(3, -1 + \sqrt{-11}) =: I$ in $\mathbb{Z}[\sqrt{-11}]$ è primo?

(d) $\mathbb{Z}[\sqrt{-11}]$ è dominio a fattorizzazione?

(e) $\mathbb{Z}[\sqrt{-11}]$ è dominio a fattorizzazione unica?

(f) $\mathbb{Z}[\sqrt{-11}]$ è dominio a ideali principali?

(g) $\mathbb{Z}[\sqrt{-11}]$ è dominio euclideo?

Svolgimento:

$$(a) \quad 0_{\mathbb{C}} = (0_{\mathbb{Z}} + 0_{\mathbb{Z}} \cdot \sqrt{-11}) \in \mathbb{Z}[\sqrt{-11}]$$

$$\text{e } \forall (a' + b'\sqrt{-11}), (a'' + b''\sqrt{-11}) \in \mathbb{Z}[\sqrt{-11}]$$

(con $a', b', a'', b'' \in \mathbb{Z}$) si ha che

$$\begin{aligned}
 (a' + b'\sqrt{-11}) - (a'' + b''\sqrt{-11}) &= \\
 = \left(\underbrace{(a' - a'')}_{\substack{\cap \\ \mathbb{Z}}} + \underbrace{(b' - b'')}_{\substack{\cap \\ \mathbb{Z}}} \sqrt{-11} \right) &\in \mathbb{Z}[\sqrt{-11}]
 \end{aligned}$$

$$\begin{aligned}
 &^e (a' + b'\sqrt{-11}) \cdot (a'' + b''\sqrt{-11}) = \\
 &= \left(\underbrace{(a'b' - 11b'b'')}_{\substack{\cap \\ \mathbb{Z}}} + \underbrace{(a'b'' + b'a'')}_{\substack{\cap \\ \mathbb{Z}}} \sqrt{-11} \right) \in \mathbb{Z}[\sqrt{-11}]
 \end{aligned}$$

quindi $\mathbb{Z}[\sqrt{-11}]$ è sottoanello di $\mathbb{C}$.

(b) $\mathbb{Z}[\sqrt{-11}]$ è sottoanello di $\mathbb{C}$, il quale è un dominio, e allora anche il sottoanello $\mathbb{Z}[\sqrt{-11}]$ è automaticamente un dominio.

(c) Supponiamo che l'ideale

$\bar{I} := (3, -1 + \sqrt{-11})$ sia principale, generato da $\zeta := (a + b\sqrt{-11}) \in \mathbb{Z}[\sqrt{-11}]$.

Allora in particolare 3 e $(-1 + \sqrt{-11})$

sono multipli di z , cioè

$$\exists \delta \in \mathbb{Z}[\sqrt{-11}] : 3 = z \cdot \delta \quad (7)$$

&

$$\exists \eta \in \mathbb{Z}[\sqrt{-11}] : (-1 + \sqrt{-11}) = z \cdot \eta \quad (8)$$

Osserviamo ora che esiste una funzione

$$v : \mathbb{Z}[\sqrt{-11}] \longrightarrow \mathbb{N}$$

$$a + b\sqrt{-11} \longmapsto v(a + b\sqrt{-11}) := a^2 + 11b^2$$

che coincide con la restrizione della norma dei numeri complessi

$$N : \mathbb{C} \longrightarrow \mathbb{R}_{\geq 0}$$

$$z \longmapsto N(z) := z \cdot \bar{z}$$

da cui segue che $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-11}]$ si ha

$$v(\alpha \cdot \beta) = v(\alpha) \cdot v(\beta) \quad (9)$$

(che si può anche verificare a mano).

Da (7)+(9) e da (8)+(9) segue che

$$9 = v(3) = v(z \cdot \delta) = v(z) \cdot v(\delta)$$

$$e \quad 12 = v(-1 + \sqrt{-11}) = v(z \cdot \eta) = v(z) \cdot v(\eta)$$

QUINDI $v(\zeta)$ è un numero in $\mathbb{N}$ t.c.

$v(\zeta) \mid 9$ e $v(\zeta) \mid 12$, quindi

$$v(\zeta) \mid \text{MCD}(9, 12) = 3$$

cioè $v(\zeta) \mid 3$ (in $\mathbb{N}$) e

QUINDI
$$v(\zeta) \in \{1, 3\}$$

MA ζ ha forma $\zeta = a + b\sqrt{-11}$ con
 $a, b \in \mathbb{Z}$ e allora

$$\left. \begin{array}{l} v(\zeta) = a^2 + 11b^2 \\ a, b \in \mathbb{Z} \end{array} \right\} \Rightarrow v(\zeta) = a^2 + 11b^2 \neq 3$$

e quindi $v(\zeta) = a^2 + 11b^2 = 1$,

da cui $\zeta = \pm 1$.

MA $\zeta = \pm 1$ genera l'ideale totale

$$(\pm 1) = \mathbb{Z}[\sqrt{-11}], \text{ quindi}$$

sarebbe anche $\bar{I} := (3, -1 + \sqrt{-11}) = (1) = \mathbb{Z}[\sqrt{-11}]$

MA questo è assurdo! Infatti,
se così fosse, allora

$$\exists (a' + b'\sqrt{-11}), (a'' + b''\sqrt{-11}) \in \mathbb{Z}[\sqrt{-11}]$$

tali che

$$1 = 3 \cdot (a' + b'\sqrt{-11}) + (-1 + \sqrt{-11})(a'' + b''\sqrt{-11})$$

che sviluppando i calcoli si ha

$$1 = (3a' - a'' - 11b'') + (3b' - b'' + a'') \cdot \sqrt{-11}$$

e quindi

$$\begin{cases} 3a' - a'' - 11b'' = 1 \\ 3b' - b'' + a'' = 0 \end{cases} \quad (\text{in } \mathbb{Z})$$

che a sua volta implica

$$\begin{cases} -a'' - 11b'' \equiv 1 \pmod{3} \\ -b'' + a'' \equiv 0 \pmod{3} \end{cases}$$

e anche (poiché $-11 \equiv 1 \pmod{3}$)

$$\begin{cases} -a'' + b'' \equiv 1 \pmod{3} \\ b'' - a'' \equiv 0 \pmod{3} \end{cases} \quad \textcircled{\text{⚡}}$$

e quindi concludiamo che l'ideale

$I := (3, -1 + \sqrt{-11})$ non è principale.

(d) La funzione $\nu: \mathbb{Z}[\sqrt{-11}] \longrightarrow \mathbb{N}$
 $a + b\sqrt{-11} \longmapsto a^2 + 11b^2$

considerata a pag. 14 è moltiplicativa, cioè gode della proprietà (9); in particolare, essa è una funzione di "valutazione" per il dominio $\mathbb{Z}[\sqrt{-11}]$, e da questo segue (per un risultato generale) che $\mathbb{Z}[\sqrt{-11}]$ è un dominio a fattorizzazione.

(e) L'elemento $12 \in \mathbb{Z}[\sqrt{-11}]$ ammette le due fattorizzazioni

$$12 = 3 \cdot 2 \cdot 2 \quad (10)$$

$$e \quad 12 = (-1 + \sqrt{-11}) \cdot (-1 - \sqrt{-11}) \quad (11)$$

in cui tutti i fattori coinvolti sono irriducibili! Infatti,

- sia $3 = \alpha \cdot \beta$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-11}]$;
allora è $9 = \nu(3) = \nu(\alpha \beta) = \nu(\alpha) \cdot \nu(\beta)$
da cui $\nu(\alpha), \nu(\beta) \in \{1, 3\}$

MA $\nu(r) = a^2 + 11b^2 \neq 3$

$$\forall r = (a + b\sqrt{-11}) \in \mathbb{Z}[\sqrt{-11}]$$

QUINDI dev'essere

$$\begin{cases} \nu(\alpha) = 1 \\ \nu(\beta) = 3 \end{cases} \quad \text{oppure} \quad \begin{cases} \nu(\alpha) = 3 \\ \nu(\beta) = 1 \end{cases}$$

da cui

$$\alpha = \pm 1 \quad \text{e} \quad \beta = \pm 1$$

e siccome ± 1 è invertibile in $\mathbb{Z}[\sqrt{-11}]$,
suol dire che la fattorizzazione

$3 = \alpha \cdot \beta$ è necessariamente banale,
dunque 3 è irriducibile, q.e.d.

- sia $2 = \alpha \cdot \beta$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-11}]$;
come sopra, si ha $4 = \nu(2) = \nu(\alpha) \cdot \nu(\beta)$

da cui $\nu(\alpha), \nu(\beta) \in \{1, 2\}$,

MA $\nu(\gamma) = a^2 + 11 \cdot b^2 \neq 2 \quad \forall \gamma \in \mathbb{Z}[\sqrt{-11}]$

QUINDI si trova $\nu(\alpha) = 1$ e $\nu(\beta) = 1$

da cui $\alpha = \pm 1$ e $\beta = \pm 1$ e

$2 = \alpha \cdot \beta$ è fattorizzazione banale,
dunque 2 è irriducibile, q.e.d.

• sia $(-1 \pm \sqrt{-11}) = \alpha \cdot \beta$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-11}]$;

allora $12 = \nu(-1 \pm \sqrt{-11}) = \nu(\alpha) \cdot \nu(\beta)$

da cui $\nu(\alpha), \nu(\beta) \in \{1, 2, 3, 4, 6, 12\}$.

MA $\nu(\gamma) = a^2 + 11b^2 \notin \{2, 3, 6\}$

QUINDI dev'essere

$\begin{cases} \nu(\alpha) = 1 \\ \nu(\beta) = 12 \end{cases} \Rightarrow \begin{cases} \alpha = \pm 1 \\ \beta = \pm(-1 \pm \sqrt{-11}) \end{cases} \Rightarrow$ la fattorizzazione
 $(-1 \pm \sqrt{-11}) = \alpha \cdot \beta$
è banale.

oppure $\begin{cases} \nu(\alpha) = 12 \\ \nu(\beta) = 1 \end{cases} \Rightarrow \begin{cases} \alpha = \pm(-1 \pm \sqrt{-11}) \\ \beta = \pm 1 \end{cases}$ 

OPPURE dov'essere

$$\nu(\alpha) = 4 \Rightarrow \nu(\beta) = 3 \quad \textcircled{\text{f}} \quad (\text{IMPOSSIBILE})$$

$$\textcircled{\text{f}} \quad \nu(\beta) = 4 \Rightarrow \nu(\alpha) = 3 \quad \textcircled{\text{f}} \quad (\text{IMPOSSIBILE})$$

ANQUE (10) e (11) sono due

fattorizzazioni di 12 in irriducibili, che sono certamente non equivalenti perché hanno un numero di fattori irriducibili diverso (3 fattori nella (10) e 2 fattori nella (11)).

QUINDI $\mathbb{Z}[\sqrt{-11}]$ non è dominio a fattorizzazione unica.

(f) Ogni dominio a ideali principali è anche dominio a fattorizzazione unica, $\Rightarrow$ in forza del punto (e), si conclude che $\mathbb{Z}[\sqrt{-11}]$ non è un dominio a ideali principali.

OPPURE

(più diretto) al punto (c) abbiamo visto
che l'ideale $I := (3, -1 + \sqrt{-11})$ in
 $\mathbb{Z}_4[\sqrt{-11}]$ non è principale,

QUINDI si conclude che $\mathbb{Z}_4[\sqrt{-11}]$ non
è un dominio a ideali principali.

(8) Ogni dominio euclideo è anche
dominio a ideali principali, $\Rightarrow$
 $\Rightarrow$ in forza del punto (f), si conclude
che $\mathbb{Z}_4[\sqrt{-11}]$ non è un dominio euclideo. $\square$

CONTINUA

[5] Sia G un gruppo, S e S' due G -spazi, e $\varphi: S \rightarrow S'$ una funzione t.c. $\varphi(g \cdot s) = g \cdot \varphi(s)$, $\forall g \in G, \forall s \in S$
 $\forall x \in S \cup S'$, siano

$\mathcal{O}_x := G$ -orbita di x ,

$\text{St}_x :=$ stabilizzatore di x .

[Th:] (a) $\varphi(\mathcal{O}_s) = \mathcal{O}_{\varphi(s)}$, $\forall s \in S$;

(b) $|\text{St}_{\varphi(s)}| \geq |\text{St}_s|$, $\forall s \in S$;

(c) $\text{St}_{\varphi(s)} \geq \text{St}_s$, $\forall s \in S$.

Svolgimento:

(a) Ogni elemento di $\mathcal{O}_s$ è del tipo $g \cdot s$ per un certo $g \in G$, e allora
 $\varphi(g \cdot s) = g \cdot \varphi(s) \in \mathcal{O}_{\varphi(s)} \quad \forall g \in G$

ci garantisce che $\varphi(\mathcal{O}_s) \subseteq \mathcal{O}_{\varphi(s)}$.

VICEVERSA, ogni elemento di $\mathcal{O}_{\varphi(s)}$

è della forma $g \cdot \varphi(s)$ per un opportuno $g \in G$, e allora da

$$g \cdot \varphi(s) = \varphi(g \cdot s) \quad \forall g \in G$$

segue subito che $\mathcal{O}_{\varphi(s)} \subseteq \varphi(\mathcal{O}_s)$.

(b) $\forall$ punto x in un G -spazio X vale la relazione

$$\mathcal{O}_x \cong G / \mathcal{H}_x$$

da cui segue $|\mathcal{O}_x| = |G / \mathcal{H}_x| = \frac{|G|}{|\mathcal{H}_x|}$

e quindi

$$|\mathcal{H}_x| = |G| / |\mathcal{O}_x|$$

Applicando tutto ciò a $x = \varphi(s)$ in S' e a $x = s$ in S si trova che

$$\begin{aligned}
 |\mathcal{H}_{\varphi(s)}| &= |G| / |\mathcal{O}_{\varphi(s)}| \stackrel{\substack{\uparrow \\ \text{per (a)}}}{=} |G| / |\varphi(\mathcal{O}_s)| \stackrel{\substack{\uparrow \\ \text{perché}}}{\geq} \\
 &\geq \frac{|G|}{|\mathcal{O}_s|} = |\mathcal{H}_s|
 \end{aligned}$$

dunque $|\mathcal{H}_{\varphi(s)}| \geq |\mathcal{H}_s|$ q.e.d.

N.B.: naturalmente (b) è anche conseguenza diretta di (c), perché $\forall$ insiemi A e B si ha sempre

$$A \supseteq B \Leftrightarrow |A| \geq |B|.$$

(c) $\forall s \in S$, dato $g \in \mathcal{L}t_s$ si ha

$$g \in \mathcal{L}t_s \Leftrightarrow g \cdot s = s,$$

$\Leftrightarrow$

$$\varphi(g \cdot s) = \varphi(s)$$

$$\underline{MA} \quad \varphi(g \cdot s) = g \cdot \varphi(s) \quad \Rightarrow \quad g \cdot \varphi(s) = \varphi(s)$$

$\Leftrightarrow$

$$g \in \mathcal{L}t_{\varphi(s)}$$

QUINDI è

$$g \in \mathcal{L}t_{\varphi(s)} \quad \forall g \in \mathcal{L}t_s,$$

così

$$\mathcal{L}t_{\varphi(s)} \supseteq \mathcal{L}t_s, \quad \forall s \in S, \quad \text{q.e.d. } \square$$