

# Simulazione di Compito

31 maggio 2024

1. Sia  $A = \mathbb{Z}[x]/(x^3 - 1)$ .

- i) Descrivi gli ideali primi e massimali di  $A$ .
- ii) Trova gli elementi nilpotenti di  $A/(3)$ .
- iii) L'anello  $A$  è isomorfo a  $\mathbb{Z}[x]/(x - 1) \times \mathbb{Z}[x]/(x^2 + x + 1)$ ?

*Soluzione.* i) Gli ideali primi di  $A$  corrispondono agli ideali primi di  $\mathbb{Z}[x]$  che contengono  $I = (x^3 - 1)$ . Ricordiamo che i primi di  $\mathbb{Z}[x]$  sono della forma

- a)  $(p)$ , con  $p$  un primo di  $\mathbb{Z}$ : tali ideali certamente non contengono  $I$ , e pertanto non corrispondono mai a ideali di  $A$ ;
- b)  $p = (f(x))$ , con  $f(x)$  irriducibile in  $\mathbb{Z}[x]$ : un tale ideale contiene  $I$  se e solo se  $f(x)$  è un divisore di  $x^3 - 1$ , e quindi un suo fattore irriducibile. Poiché la fattorizzazione in irriducibili di  $x^3 - 1$  è  $(x - 1)(x^2 + x + 1)$  (quest'ultimo fattore chiaramente non ha radici in  $\mathbb{Z}$ ), gli  $f$  accettabili sono esattamente  $x - 1$  e  $x^2 + x + 1$ ;
- c)  $m = (p, f(x))$  con  $p$  un primo di  $\mathbb{Z}$  e  $f$  un polinomio in  $\mathbb{Z}[x]$  irriducibile modulo  $p$ . Poiché  $m$  è primo (in realtà, massimale), si ha che  $m \ni (x - 1)(x^2 + x + 1)$  se e solo se  $(\star) x - 1 \in m$  oppure  $(\diamond) x^2 + x + 1 \in m$ .

$(\star)$  Nel primo caso, vale  $(p, f(x)) = (p, f(x), x - 1) \supset (p, x - 1)$ : siccome  $J = (p, x - 1)$  è certamente massimale (il quoziente  $\mathbb{Z}[x]/J$  è isomorfo a  $\mathbb{F}_p$  o, equivalentemente,  $x - 1$  è irriducibile (mod  $p$ ) per ogni  $p$ ), l'inclusione è un'uguaglianza, per cui  $m$  è della forma  $(p, x - 1)$  con  $p$  un primo di  $\mathbb{Z}$ .

$(\diamond)$  Nel secondo caso, si ha  $x^2 + x + 1 \in (p, f(x))$  se e solo se  $\overline{x^2 + x + 1} \in (\overline{f(x)}) \subset \mathbb{Z}[x]/p\mathbb{Z}[x] = \mathbb{F}_p[x]$ , dove la barra indica la classe (mod  $p$ ), cioè se e solo se  $f(x)$  è un fattore irriducibile di  $x^2 + x + 1$  modulo  $p$ . Ora, in  $\mathbb{F}_p[x]$ , il polinomio  $x^2 + x + 1 = \frac{x^3 - 1}{x - 1}$  è irriducibile se e solo se non ha radici, cioè se e solo se  $\mathbb{F}_p$  non contiene radici terze dell'unità diverse da 1, e quindi primitive. Per definizione, le radici terze primitive dell'unità sono gli elementi di ordine 3 di  $\mathbb{F}_p^\times$ , che è ciclico: pertanto,  $\mathbb{F}_p$  contiene radici terze primitive dell'unità se e solo se 3 divide  $|\mathbb{F}_p^\times| = p - 1$ , cioè se e solo se  $p \equiv 1 \pmod{3}$ . In tal caso, vale  $x^2 + x + 1 = (x - \bar{a})(x - \bar{b}) \in \mathbb{F}_p[x]$  per certi  $a, b \in \mathbb{Z}$ , e si conclude che  $m$  è uno tra  $(p, x - a)$  e  $(p, x - b)$ ; viceversa, se  $x^2 + x + 1$  è irriducibile modulo  $p$ , dev'essere  $m = (p, x^2 + x + 1)$ .

- ii) In  $A$ , l'ideale generato da 3 è  $(3, x^3 - 1)/(x^3 - 1)$ : per il terzo teorema di omomorfismo vale allora

$$A/(3) \simeq \mathbb{Z}[x]/(3, x^3 - 1) \simeq \mathbb{F}_3[x]/((x - 1)^3).$$

Ora, i nilpotenti di un anello  $B$  sono gli elementi di  $\sqrt{(0)}$  e, se  $B$  è un quoziente della forma  $A/I$ , tale ideale corrisponde in  $A$  a  $\sqrt{I}$ . Nel nostro caso si tratta quindi di trovare  $J = \sqrt{((x - 1)^3)} \subset \mathbb{F}_3[x]$ : certamente  $x - 1 \in J$ , e perciò  $(x - 1) \subset J$ . Siccome  $(x - 1)$  è massimale in  $\mathbb{F}_3[x]$ , si ottiene che vale l'uguaglianza. In conclusione, i nilpotenti di  $A/(3)$  corrispondono ai multipli di  $x - 1$  in  $\mathbb{F}_3[x]$ , cioè agli  $f(x) \in \mathbb{Z}[x]$  tali che  $f(1)$  è multiplo di 3.

- iii) La risposta è **no**. Un possibile motivo è questo: posto  $B = \mathbb{Z}[x]/(x - 1) \times \mathbb{Z}[x]/(x^2 + x + 1)$ , un isomorfismo  $\varphi : A \rightarrow B$  deve mandare 1 in  $(1, 1)$ , quindi 3 in  $(3, 3)$ , e di conseguenza  $\varphi(3A)$  è l'ideale  $(3) \times (3)$  generato da  $(3, 3)$  in  $B$ ; ne segue che, se  $A$  è isomorfo a  $B$ , anche  $A/(3)$  è isomorfo a  $B/((3, 3))$ . D'altra parte, usando il terzo teorema di omomorfismo e notando che  $x^2 + x + 1$  è irriducibile in  $\mathbb{F}_3[x]$  per quanto detto al punto (i), si ottiene

$$B/(3) \times (3) \simeq \mathbb{Z}[x]/(3, x - 1) \times \mathbb{Z}[x]/(3, x^2 + x + 1) \simeq \mathbb{F}_3 \times \mathbb{F}_9.$$

Quest'ultimo anello, però, non ha elementi nilpotenti non banali: preso  $(a, b) \in \mathbb{F}_3 \times \mathbb{F}_9$ , vale  $(a, b)^k = 0$  se e solo se  $a^k = 0$  e  $b^k = 0$ , cioè  $a = b = 0$  poiché entrambi  $\mathbb{F}_3, \mathbb{F}_9$  sono campi. In conclusione, un isomorfismo  $A/(3) \simeq B/((3, 3))$  contraddice il punto (ii), e pertanto  $A$  non può essere isomorfo a  $B$ .  $\square$

**Attenzione:** Al punto (iii) avete tutti risposto che i due anelli proposti sono isomorfi per il Teorema Cinese del Resto. Tuttavia, in questo caso, il TCR non era applicabile: l'ipotesi perché, dati due ideali  $I, J$  in un anello  $A$ , valga

$$A/IJ \simeq A/I \times A/J$$

è che i due ideali  $I, J$  siano comassimali, cioè valga  $I + J = (1)$ . Se  $A$  è un dominio, anche un UFD, e  $I = (f), J = (g)$  sono principali, questa condizione *non* è equivalente al fatto che  $f$  e  $g$  siano coprimi, cioè il loro massimo comun divisore sia 1. L'equivalenza è garantita solo se  $A$  è un PID, e ciò è falso per  $\mathbb{Z}[x]$ . L'esercizio sopra offre appunto un controesempio: i polinomi  $x - 1$  e  $x^2 + x + 1$  sono entrambi irriducibili, e in particolare coprimi, in  $\mathbb{Z}[x]$ , ma l'ideale da essi generato è

$$(x - 1, x^2 + x + 1) = (x - 1, x^2 + x + 1 - x(x - 1)) = (x - 1, 2x + 1) = (x - 1, 3),$$

che è un ideale massimale di  $\mathbb{Z}[x]$ , e *non* l'intero  $\mathbb{Z}[x]$ .

2. Sia  $A = \mathbb{Q}[x, y]/(f)$ , con  $f(x, y) = x^2y - y - 1 \in \mathbb{Q}[x, y]$ .

i) Mostra che  $A$  è isomorfo a un sottoanello di  $\mathbb{Q}(t)$ .

ii) Dimostra che  $A$  è un PID e descrivi gli ideali primi di  $A$ .

*Soluzione.* i) Notiamo che  $f(x, y) = (x^2 - 1)y - 1$ : pertanto, in  $A$ ,  $f = 0$  implica che  $y$  è invertibile di inverso  $x^2 - 1$ . Quindi, è plausibile che  $A$  sia isomorfo all'anello  $B = \mathbb{Q}\left[t, \frac{1}{t^2-1}\right] \subset \mathbb{Q}(t)$ . Per mostrarlo, consideriamo l'omomorfismo  $\varphi : \mathbb{Q}[x, y] \rightarrow \mathbb{Q}(t)$  indotto dalle assegnazioni  $x \mapsto t, y \mapsto \frac{1}{t^2-1}$ . L'immagine di tale omomorfismo è chiaramente  $B$ , e vale evidentemente  $f\left(t, \frac{1}{t^2-1}\right) = 0$ , cioè  $\ker \varphi \supset (f(x, y))$ : resta quindi da mostrare che  $\ker \varphi \subset (f(x, y))$ .

Sia allora  $g \in \mathbb{Q}[x, y]$  tale che  $\varphi(g) = 0$ , e supponiamo per assurdo che  $g \notin (f)$ , cioè  $g$  non è un multiplo di  $f$  in  $\mathbb{Q}[x, y]$ . Poiché  $f$  è primitivo in  $\mathbb{Q}[x][y] = \mathbb{Q}[x, y]$ , in quanto  $c(f) = \gcd(x^2 - 1, 1) = 1$ , per il lemma di Gauss ciò equivale a dire che  $g$  non è un multiplo di  $f$  in  $\mathbb{Q}(x)[y]$ . Ne segue che la divisione euclidea di  $g$  per  $f$  in  $\mathbb{Q}(x)[y]$  ha la forma  $g = q(x, y)f + r(x, y)$ , con  $q, r \in \mathbb{Q}(x)[y]$  e  $r$  un polinomio non nullo e di grado  $< 1$  in  $y$ , cioè  $r = \frac{r_1(x)}{r_2(x)} \in \mathbb{Q}(x)^\times$ , per certi  $r_i(x) \in \mathbb{Q}[x] \setminus \{0\}$ .

D'altra parte, l'omomorfismo  $\varphi$  si estende a  $\psi : \mathbb{Q}(x)[y] \rightarrow \mathbb{Q}(t)$  ponendo

$$\psi\left(\sum_{i=0}^n \frac{f_i(x)}{g_i(x)} y^i\right) = \frac{\varphi(f_i(x))}{\varphi(g_i(x))} \varphi(y)^i,$$

e vale allora  $\psi(g) = \varphi(g) = 0$ , cioè

$$0 = \psi(qf + r) = \psi(q)\varphi(f) + \psi(r) = \psi(r) = \frac{\varphi(r_1)}{\varphi(r_2)},$$

da cui  $\varphi(r_1) = r_1(t) = 0$ , cioè  $r_1(x) = 0$ . In conclusione, si ha  $r(x) = 0$ , il che risulta assurdo, e ciò dimostra che dev'essere  $g \in (f)$ , cioè  $\ker \varphi = (f)$ . Per il primo teorema di omomorfismo, si ottiene perciò  $A \simeq \mathbb{Q}\left[t, \frac{1}{t^2-1}\right]$ .

ii) Visti i risultati del punto (i), studiamo l'anello  $B = \mathbb{Q}\left[t, \frac{1}{t^2-1}\right]$ . Intanto, notiamo che  $B$  coincide con la localizzazione di  $\mathbb{Q}[t]$  all'elemento  $t^2 - 1$ , cioè alla parte moltiplicativa  $S = \{(t^2 - 1)^k\}_{k \geq 0}$ : infatti, certamente  $B$  contiene gli elementi della forma  $f(t)/(t^2 - 1)^k \in \mathbb{Q}(t)$  con  $f(t) \in \mathbb{Q}[t]$ ; viceversa, poiché  $\mathbb{Q}[t]_{t^2-1} \subset \mathbb{Q}(t)$  contiene  $\mathbb{Q}, t$  e  $\frac{1}{t^2-1}$ , contiene certamente anche il sottoanello di  $\mathbb{Q}(t)$  da essi generato, che è appunto  $B$ .

Si ottiene allora che

- $B$  è un PID, in quanto localizzazione di  $\mathbb{Q}[t]$ , che è un PID;
- gli ideali primi di  $B$  sono in bigezione con i primi di  $\mathbb{Q}[t]$  che non intersecano  $S$ ; d'altra parte, i primi di  $\mathbb{Q}[t]$  sono gli ideali della forma  $p = (h(t))$  con

$h \in \mathbb{Q}[t]$  irriducibile, e un tale  $p$  contiene  $(t^2 - 1)^k$  per qualche  $k > 0$  se e solo se contiene  $t^2 - 1$  (poiché  $p$  è primo), cioè se e solo se  $h(t)$  è un fattore irriducibile di  $t^2 - 1$ . In conclusione i primi di  $B$  corrispondono, a meno di localizzare, agli ideali  $(h(t)) \subset \mathbb{Q}[t]$  con  $h(t)$  irriducibile e diverso da  $t \pm 1$ .

Perciò,  $A$  è un PID in quanto isomorfo a un PID e, leggendo  $\varphi$  al contrario, si ottiene che gli ideali primi di  $A$  sono della forma  $(\overline{h(x)})$ , dove  $\overline{h(x)}$  è la classe in  $A$  di un polinomio  $h(x) \in \mathbb{Q}[x] \subset \mathbb{Q}[x, y]$  irriducibile in  $\mathbb{Q}[x]$  e distinto da  $x \pm 1$ .  $\square$

3. Sia  $f(x) \in \mathbb{Q}[x]$  il polinomio  $x^{12} - 4$ , e sia  $L$  il suo campo di spezzamento su  $\mathbb{Q}$ .

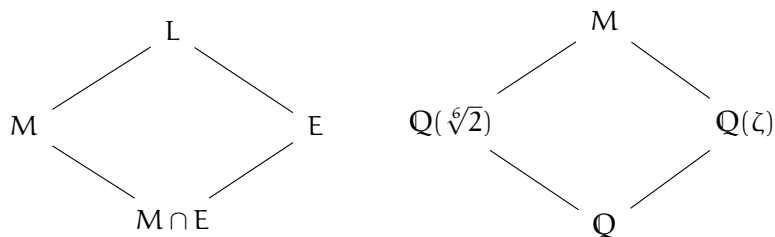
- i) Trova il gruppo di Galois di  $L$  su  $\mathbb{Q}$ .
- ii) Mostra che  $L$  ha un'unica sottoestensione  $K$  di grado 6 e di Galois su  $\mathbb{Q}$ .
- iii) Calcola  $G(K | \mathbb{Q})$  e descrivi le sottoestensioni di  $K$ .

*Soluzione.* i) La fattorizzazione di  $f(x)$  in  $\mathbb{Q}[x]$  è  $x^{12} - 4 = (x^6 + 2)(x^6 - 2)$ , poiché entrambi i fattori risultano irriducibili per Eistenstein. Le radici di  $f(x)$  sono quindi della forma  $\sqrt[6]{2} \cdot \zeta_{12}^j$  con  $j = 0, \dots, 11$  e  $\zeta_{12}$  una radice dodicesima primitiva di 1 in  $\mathbb{C}$ . Si ha allora

$$L = \mathbb{Q}(\sqrt[6]{2} \cdot \zeta_{12}^j \mid j = 0, \dots, 11) = \mathbb{Q}(\sqrt[6]{2}, \zeta_{12}) = \mathbb{Q}(\sqrt[6]{2}, \zeta_3, i) = \mathbb{Q}(\sqrt[6]{2}, \zeta_6, i)$$

per quanto noto sulle estensioni ciclotomiche, e tenendo conto che  $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ .

Poniamo allora  $\zeta = \zeta_6$  e  $M = \mathbb{Q}(\sqrt[6]{2}, \zeta)$  e  $E = \mathbb{Q}(i)$ . Otteniamo i diagrammi



in cui  $M, E$  sono entrambe estensioni normali su  $\mathbb{Q}$ : la prima, in quanto campo di spezzamento di  $x^6 - 2$ , la seconda in quanto di grado 2. Pertanto, se mostriamo che  $M \cap E = \mathbb{Q}$ , la teoria vista a lezione assicura che  $G(L | \mathbb{Q}) \simeq G(M | \mathbb{Q}) \times G(E | \mathbb{Q})$ .

Calcoliamo intanto  $G(M | \mathbb{Q})$ : è chiaro che  $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$  e che  $\zeta \notin \mathbb{Q}(\sqrt[6]{2})$ , da cui si deduce immediatamente che  $[M : \mathbb{Q}] = 12$  e che i coniugati di  $\zeta$  su  $\mathbb{Q}(\sqrt[6]{2})$  sono  $\zeta$  e  $\bar{\zeta} = \zeta^{-1}$ . La teoria generale degli omomorfismi di estensioni finite di campi garantisce allora che gli elementi di  $G(M | \mathbb{Q})$  sono le mappe  $\sigma_{ij} : M \rightarrow M$

definite da  $\sigma_{ij}(\sqrt[6]{2}) = \sqrt[6]{2} \cdot \zeta^i$ ,  $\sigma_{ij}(\zeta) = \zeta^j$ , con  $i = 0, \dots, 5$  e  $j = \pm 1$ . Perciò, posto  $r = \sigma_{11}$ ,  $s = \sigma_{0,-1}$  si ottiene subito  $G(M | Q) = \langle r \rangle \langle s \rangle$ , in quanto  $r$  ha ordine 6,  $s$  ha ordine 2 e  $G(M | Q)$  ha ordine 12, e  $srs = r^{-1}$ , da cui si conclude  $G(M | Q) \simeq D_6$ . A questo punto, per vedere  $M \cap E = Q$  è sufficiente verificare che nessuna delle sottoestensioni quadratiche di  $M$  coincida con  $E = Q(i)$ : tali sottoestensioni corrispondono ai sottogruppi di indice 2 di  $D_6$ , e sono quindi 3 (come è noto, i sottogruppi di  $D_6$  di indice 2 sono  $\langle r \rangle$ ,  $\langle r^2, s \rangle$ ,  $\langle r^2, rs \rangle$ ). Certamente  $M$  contiene  $Q(\sqrt{2})$ ,  $Q(\zeta) = Q(\sqrt{-3})$  e  $Q(\sqrt{-6})$ : poiché tali estensioni sono tutte distinte tra loro, e tutte distinte da  $Q(i) = E$ , si ottiene quanto voluto.

In conclusione,  $G(L | Q) \simeq G(M | Q) \times G(E | Q) \simeq D_6 \times \mathbb{Z}/2$ .

- ii) Per la teoria di Galois, una sottoestensione di grado 6 e di Galois su  $Q$  corrisponde a un sottogruppo normale di indice 6, cioè di ordine 4, in  $G = G(L | Q) \simeq D_6 \times \mathbb{Z}/2$ : pertanto, bisogna far vedere che un tale sottogruppo  $N$  esiste ed è unico. Notiamo che un tale  $N$ , in quanto 2-sottogruppo normale di  $G$ , è necessariamente contenuto nell'intersezione dei suoi 2-Sylow.

Ora, poiché  $Q(\sqrt[3]{2})$  è una sottoestensione di  $L$  di grado 3 su  $Q$  e non normale,  $G$  possiede un sottogruppo non normale di indice 3; ne segue che  $G$  non ha un unico 2-Sylow, e che quindi  $n_2(G) = 3$ . Allora, se  $\{P_1, P_2, P_3\} = \text{Syl}_2(G)$ , certamente  $P_1 \cap P_2 \cap P_3$  ha ordine al più 4; viceversa,  $\langle (r^3, 0), (1, 1) \rangle$  è un sottogruppo normale di ordine 4 in  $G$ , e pertanto vale  $P_1 \cap P_2 \cap P_3 = \langle (r^3, 0), (1, 1) \rangle$ , che è quindi l'unico sottogruppo normale di ordine 4 di  $G$ , ed è l' $N$  cercato.

- iii) Ricordando ancora che  $Q(\zeta) = Q(\zeta_3) = Q(\sqrt{-3})$ , la sottoestensione  $K = Q(\sqrt[3]{2}, \zeta)$  di  $L$  è normale su  $Q$ , in quanto campo di spezzamento di  $X^3 - 2$ , e ha grado 6: pertanto, è l'estensione corrispondente al sottogruppo  $N$  al punto (ii). Un ragionamento del tutto analogo a quello fatto su  $M = Q(\sqrt[3]{2}, \zeta)$  conclude che  $G(K | Q) \simeq D_3 \simeq S_3$ ; in alternativa, si può osservare che  $G(K | Q) \simeq G/N$ , che ha ordine 6 e non è abeliano (ad esempio in quanto  $(r^2, 0) \in G' \setminus N$ , per cui  $N \not\trianglelefteq G'$ ), e quindi ancora  $G(K | Q) \simeq S_3$ . Considerando che  $S_3$  ha tre sottogruppi di indice 3 e uno di indice 2, la corrispondenza di Galois fornisce allora il reticolo di sottoestensioni

