SCRITTI DI ALGEBRA 2

FABRIZIO CASELLI

Contents

09 Gennaio 2017

Esercizio 1 Sia $f = X^4 + 6X^2 + 4$. Sia $K = \mathbb{Q}[\sqrt{5}]$, L il campo di spezzamento di f su $\mathbb{Q}$, e $\alpha \in L$ una radice di f.

a. Mostrare che $K \subset L$.
b. Scomporre f in fattori irriducibili in $\mathbb{Q}[X]$ e in $K[X]$;
c. Determinare il polinomio minimo di α^{-1} su $\mathbb{Q}$.
d. Determinare $[L : \mathbb{Q}]$ (Suggerimento: quali elementi di un campo K ammettono radice quadrata in un'estensione quadratica $K[\sqrt{d}]$?)

Esercizio 2 Sia $A = \mathbb{Z}[\sqrt{3}]$.

a. Determinare l'inverso di $1 + 2\sqrt{3}$ in $\mathbb{Q}[\sqrt{3}]$.
b. Mostrare che $1 + 2\sqrt{3}$ è associato a $8 + 5\sqrt{3}$ in A e che non è associato a $17 + 10\sqrt{3}$ in A.
c. Mostrare che il gruppo $\mathcal{U}(A)$ degli invertibili di A contiene infiniti elementi.

Esercizio 3 Si consideri il sistema

$$\begin{cases} X^{19} = X \\ X^3 + 13X^2 + 48X + 36 = 0 \end{cases}$$

a. Verificare che esistono esattamente quattro soluzioni distinte in $\mathbb{Z}_{665}$.
b. Determinare esplicitamente almeno tre soluzioni.

23 Gennaio 2017

Esercizio 1 Sia $f = X^4 - 8X^2 + 1$, K il campo di spezzamento di f su $\mathbb{Q}$ e $L \subset \mathbb{C}$ il campo di spezzamento di f su $\mathbb{Q}[\sqrt{-2}]$.

a. Verificare che se α è una radice di f anche α^{-1} lo è.
b. Determinare $[K : \mathbb{Q}]$.
c. Determinare $[L : \mathbb{Q}[\sqrt{-2}]]$.
d. Determinare il campo di spezzamento di f su $\mathbb{Z}_{11}$.

Esercizio 2 Sia $A = \mathbb{Z}[\sqrt{-2}]$ e $\alpha = 20 - 5\varepsilon$.

a. Determinare una scomposizione in fattori irriducibili di α.
b. Mostrare che $A/(\alpha)$ ha un numero finito di ideali.
c. Descrivere gli ideali massimali di $A/(\alpha)$.
d. Quali campi possono essere ottenuti come quoziente di $A/(\alpha)$?

Esercizio 3 Sia A un dominio e Q il suo campo dei quozienti. Un sottoinsieme $S \subset A$ si dice moltiplicativo se $1 \in S$, $0 \notin S$ e S è chiuso rispetto al prodotto di A. Siano S, S' sottoinsiemi di A moltiplicativi.

a. Mostrare che
$$A_S = \left\{ \frac{a}{s} \in Q : \, a \in A, \, s \in S \right\}$$
è un sottoanello di Q.
b. Mostrare che se $S \subset S'$ e ogni elemento di S' è un divisore di qualche elemento di S allora $A_S = A_{S'}$.
c. Mostrare che se $A_S = A_{S'}$ allora ogni elemento di S' divide qualche elemento di S.

10 Febbraio 2017

Esercizio 1 Sia $\mathbb{L} = \mathbb{Q}[\sqrt{3}, \sqrt{7}]$.

a. Determinare una base di $\mathbb{L}$ come $\mathbb{Q}$-spazio vettoriale.
b. Stabilire se $\mathbb{L}$ è il campo di spezzamento di un polinomio $f \in \mathbb{Q}[X]$.
c. Determinare un elemento $\alpha \in \mathbb{L}$ tale che $\mathbb{L} = \mathbb{Q}[\alpha]$.
d. Mostrare che se $\beta \in \mathbb{L}$ è tale che $\beta^2 \in \mathbb{Q}$ allora esistono $q \in \mathbb{Q}$ e $d \in \{1, 3, 7, 21\}$ tali che $\beta = q\sqrt{d}$.
e. Determinare tutti i campi $\mathbb{K}$ tali che $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$.

Esercizio 2 Sia $A = \mathbb{Z}_6[X]$. Siano $f = \sum a_i X^i$ e $g = \sum b_j X^j$ polinomi in A di grado rispettivamente n e m tali che $fg = 1$.

a. Supponiamo $n + m > 0$ e $a_n = 3$. Mostrare che $b_m = 2, 4$.
b. Nelle ipotesi del punto [a.] mostrare che per ogni $k = 0, 1, \ldots, \min(n, m)$ si ha $a_{n-k} = 0, 3$ e $b_{m-k} = 0, 2, 4$.
c. Dedurre che $f = g = 1$ oppure $f = g = 5$.
d. Scrivere almeno tre elementi invertibili in $A[\sqrt{2}]$.

Esercizio 3 Sia A l'intersezione di tutti i sottoanelli di $\mathbb{C}$ che contengono $\mathbb{Z}$ e $\sqrt[3]{2}$.

a. Mostrare che A è un sottoanello di $\mathbb{C}$.
b. Mostrare che per ogni $\alpha \in A$ esistono unici $a, b, c \in \mathbb{Z}$ tali che $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$.
c. Descrivere esplicitamente l'ideale generato da $\sqrt[3]{2}$.
d. Descrivere esplicitamente il quoziente $A/(\sqrt[3]{2})$.

07 Giugno 2017

Esercizio 1 Sia $K \subset L$ un'estensione di campi di caratteristica $\neq 2$, con $[L : K] = 2$.

a. Mostrare che esiste $\alpha \in L$ tale che $\alpha^2 \in K$ e $L = K[\alpha]$;
b. Fissato un tale elemento α, mostrare che in generale il polinomio $X^4 - \alpha^2$ può essere riducibile su $K[X]$ (Sugg.: $K = \mathbb{Z}_3$);
c. Mostrare che se $K \subset L \subseteq \mathbb{R}$ allora il polinomio $X^4 - \alpha^2$ è irriducibile su $K[X]$;
d. Stabilire se esiste un campo $K \subset \mathbb{R}$ tale che $[\mathbb{R} : K] = 2$;

Esercizio 2 Sia $q \in \mathbb{Q}$ e

$$A_q := \left\{ \begin{bmatrix} a & b \\ qb & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}.$$

a. Mostrare che $(A_q, +, \cdot)$, dove $+$ e $\cdot$ indicano le usuali operazioni di somma e prodotto tra matrici, è un anello (commutativo unitario) per ogni q.
b. Mostrare che A_2 è un campo.
c. Mostrare che A_4 non è un dominio.
d. Descrivere esplicitamente l'ideale I di A_4 generato da $\begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix}$.
e. Mostrare che $A_4/I \cong \mathbb{Q}$.

Esercizio 3 Consideriamo le 7 possibili estensioni quadratiche di $\mathbb{Z}_7$, i.e. $\mathbb{Z}_7[\sqrt{d}]$ al variare di $d \in \mathbb{Z}_7$.

a. Per quali valori di d si ha che $\mathbb{Z}_7[\sqrt{d}]$ è un campo?
b. Per quali valori di d si ha che $\mathbb{Z}_7[\sqrt{d}]$ contiene elementi con quadrato nullo?
c. Per quali valori di d si ha che $\mathbb{Z}_7[\sqrt{d}]$ contiene almeno 3 elementi che al quadrato danno 1?
d. Dare condizioni necessarie e sufficienti su $d, d' \in \mathbb{Z}_7$ affinché $\mathbb{Z}_7[\sqrt{d}] \cong \mathbb{Z}_7[\sqrt{d'}]$.

04 Luglio 2017

Esercizio 1 Sia K un campo e consideriamo il polinomio $f = 4X^5 - 3X^3 + 2X^2 \in K[X]$.

a. Stabilire se $K[X]/(f)$ è un dominio.
b. Determinare, se esiste, un elemento $P \in K[X]/(f)$ nilpotente.
c. Determinare, se esiste, l'inverso di $P + 1$ in $K[X]/(f)$, dove P è l'elemento determinato nel punto precedente.
d. Sia A un dominio, $a, b \in A$ non nulli e non invertibili. Determinare un elemento nilpotente in $A/(a^2b)$.

Esercizio 2 Motivando le risposte, determinare il campo di spezzamento (e il suo grado) di $(X^2 - 2)(X^2 - 3)$

a. su $\mathbb{Q}$;
b. su $\mathbb{R}$
c. su $\mathbb{F}_7$
d. su $\mathbb{F}_9$;
e. su $\mathbb{F}_{169}$.
f. su $\mathbb{Z}_5[\sqrt{3}]$.

Esercizio 3 Consideriamo il polinomio $f = aX^4 + bX + c \in \mathbb{Z}[X]$, con $a, b, c \in \mathbb{Z}$ tutti dispari.

a. Determinare tutti i valori di a, b, c per cui $\mathbb{Q}[X]/(f)$ è un campo.
b. Determinare tutti i valori di a, b, c per cui $\mathbb{Z}[X]/(f)$ è un campo.
c. Determinare per quali valori di a, b, c l'elemento $aX^3 + b$ è invertibile in $\mathbb{Q}[X]/(f)$ e in tal caso determinarne l'inversa.
d. (difficile) Determinare per quali valori di a, b, c l'elemento $aX^3 + b$ è invertibile in $\mathbb{Z}[X]/(f)$ e in tal caso determinarne l'inversa.

05 Settembre 2017

Esercizio 1 Sia A un anello. Per ogni ideale I di A poniamo

$$\sqrt{I} := \{x \in A : \text{esiste } n \in \mathbb{N} \text{ per cui } x^n \in I\}.$$

a. Mostrare che $I \subset \sqrt{I}$:
b. Mostrare che $\sqrt{I}$ è ancora un ideale di A;
c. Mostrare che $\sqrt{\sqrt{I}} = \sqrt{I}$;
d. Per $A = \mathbb{Q}[X]$ e $I = (X^2)$ determinare $\sqrt{I}$.

Esercizio 2 Motivando le risposte, determinare un campo di spezzamento (e il suo grado) di $X^4 + 2$

a. su $\mathbb{Q}$ (Sugg.: mostrare in quest'ordine che i, $\sqrt{2}$ e $\sqrt[4]{2}$ appartengono al campo di spezzamento);
b. su $\mathbb{F}_3$;
c. su $\mathbb{F}_4$;
d. su $\mathbb{F}_5$.

Esercizio 3 Sia $A = \mathbb{Z}[\sqrt{-2}]$. Sia $\alpha = (1 + \varepsilon)^2$.

(1) Determinare un elemento $\beta \in A$ tale che $N(\beta) < 9$ e $\beta \equiv 3 \mod (\alpha)$;
(2) Mostrare che ogni elemento in $A/(\alpha)$ ha un rappresentante di norma < 9;
(3) Dedurre che $A/(\alpha)$ ha al più 17 elementi;
(4) Mostrare che $\varepsilon \equiv -4 \mod (\alpha)$;
(5) Mostrare che $1, 2, 3, 4, 5, 6, 7, 8$ non sono elementi di (α).
(6) Concludere che $A/(\alpha) \cong \mathbb{Z}_9$;

11 Gennaio 2018

Esercizio 1 Vogliamo studiare il campo si spezzamento di $X^3 - \sqrt{2}$ sui campi $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Z}_{11}[\sqrt{2}]$.

a. Determinare, se esistono, tutti i possibili omomorfismi $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_7$;
b. Utilizzare il punto precedente per stabilire se $X^3 - \sqrt{2}$ è irriducibile su $\mathbb{Q}[\sqrt{2}]$;
c. Determinare il grado del campo di spezzamento di $X^3 - \sqrt{2}$ su $\mathbb{Q}[\sqrt{2}]$.

Esercizio 2 Consideriamo l'anello $A = \mathbb{Z}_{17}[\sqrt{2}]$.

a. Stabilire se A è un dominio.
b. Determinare quanti sono gli elementi invertibili di A.
c. Mostrare che A possiede esattamente 4 classi di associatura.
d. Determinare tutti i possibili quozienti di A.

Esercizio 3 Sia A l'anello $\mathbb{Q}[X]$ e consideriamo le sue estensioni quadratiche $A[\sqrt{X}]$, $A[\sqrt{X^2}]$ e $A[\sqrt{X^3}]$.

a. Mostrare che $A[\sqrt{X}]$ è un dominio.
b. Mostrare che $A[\sqrt{X^2}]$ non è un dominio.
c. Mostrare che $A[\sqrt{X^3}]$ è un dominio ma non è un PID.
d. Mostrare che $A[\sqrt{X}]$ è isomorfo ad A e quindi è un dominio euclideo.

6 Febbraio 2018

Esercizio 1 Consideriamo il seguente insieme A di matrici 3×3:

$$A = \left\{ \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} : \ a, b, c \in \mathbb{Q} \right\}.$$

a. Mostrare che A è un anello commutativo (con le usuali operazioni) ed un $\mathbb{Q}$-spazio vettoriale di dimensione 3;
b. Mostrare che $I = \left\{ \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} : \ a+b+c=0 \right\}$ e $J = \left\{ \begin{bmatrix} a & a & a \\ a & a & a \\ a & a & a \end{bmatrix}, \ a \in \mathbb{Q} \right\}$ sono ideali non banali di A.
c. Determinare il nucleo dell'unico omomorfismo $\varphi : \mathbb{Q}[X] \to A$ tale che $\varphi(X) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ (Suggerimento: calcolare $\varphi(X^3)$).
d. Concludere che I e J sono gli unici ideali non banali di A.

Esercizio 2 Consideriamo il polinomio $f = X^5 - 3X^3 - 2X^2 - 1 \in \mathbb{Z}_7[X]$.

a. Stabilire se f è irriducibile.
b. Determinare il campo di spezzamento di f su $\mathbb{Z}_7$.
c. Determinare il campo di spezzamento di f su $\mathbb{F}_{7^4}$.
d. Stabilire quante radici ammette f in $\mathbb{F}_{7^5}$.

Esercizio 3 Consideriamo l'estensione quadratica A di $\mathbb{Z}_3$ data da $A = \mathbb{Z}_3[\sqrt{2}]$.

a. Mostrare che A è il campo con 9 elementi;
b. Determinare tutti i generatori di A^*;
c. Considerando l'ulteriore estensione quadratica $B = A[\sqrt{2}]$ stabilire se B è un campo;
d. Stabilire se esiste un ideale I di B tale che $B/I \cong \mathbb{F}_9$.

04 Giugno 2018

Esercizio 1 Sia $f = X^2 + X + 1 \in \mathbb{Q}[X]$ e

$$A = \left\{ \frac{g}{h} : g, h \in \mathbb{Q}[X],\ f \not| h \right\}.$$

a. Verificare che A è un anello;
b. Determinare gli elementi invertibili di A;
c. Mostrare che A ha un solo ideale massimale I;
d. Stabilire se il campo A/I è un'estensione finita di $\mathbb{Q}$.

Esercizio 2 Siano $\alpha, \beta \in \mathbb{Z}[i]$ tali che $\mathrm{MCD}(N(\alpha), N(\beta)) = 10$. Poniamo $I = (\alpha, \beta)$.

a. Mostrare che I è generato da un elemento la cui norma è un divisore di 10;
b. Stabilire se I può essere uguale a $\mathbb{Z}[i]$;
c. Stabilire se I può essere massimale;
d. Stabilire quanti elementi può avere l'anello $\mathbb{Z}[i]/I$.

Esercizio 3 Sia K un'estensione di $\mathbb{Q}$.

a. Mostrare che se $[K : \mathbb{Q}] = 2$ allora esiste $f \in \mathbb{Q}[X]$ tale che K è un campo di spezzamento per f.
b. Supponiamo che K sia il campo di spezzamento di un polinomio irriducibile f di grado 3. Sia $\varphi : K \to \mathbb{C}$ un omomorfismo tale che $\varphi(a) = a$ per ogni $a \in \mathbb{Q}$ e α una radice di f. Mostrare che anche $\varphi(\alpha)$ è una radice di f. Dedurre che $\varphi(K) \subseteq K$;
c. Mostrare che se $K = \mathbb{Q}[\sqrt[3]{2}]$ allora non esiste un polinomio f tale che K sia un campo di spezzamento per f su $\mathbb{Q}$.

9 Luglio 2018

Esercizio 1 Consideriamo l'anello $A = \mathbb{Z}[X]$.

a. Mostrare che per ogni $n \geq 2$ l'ideale (X, n) non è principale.
b. Posti $I = (X, 2)$ e $J = (X, 3)$ mostrare che $IJ = (X, 6)$.
c. Mostrare che $IJ \neq \{ab \mid a \in I,\, b \in J\}$.

Esercizio 2 Consideriamo l'anello $A = \mathbb{Z}[\sqrt{10}]$.

a. Determinare tutti i possibili omomorfismi $A \to \mathbb{Z}_2$
b. Determinare tutti gli ideali I di A tali che $A/I \cong \mathbb{Z}_3$.
c. Per ogni primo p mostrare che esistono al più due ideali I di A tale che $A/I \cong \mathbb{Z}_p$.
d. Stabilire se $\mathbb{F}_{49}$ è un quoziente di A.

Esercizio 3 Sia $f = X^3 + X^2 + 1 \in \mathbb{Z}_2[X]$ e α una radice di f in una qualche estensione di $\mathbb{F}_2$.

a. Mostrare che $K = \mathbb{Z}_2[\alpha]$ ha 8 elementi. Scelta una base di K su $\mathbb{Z}_2$ esprimere gli elementi $\alpha(\alpha + 1)^2$ e $(\alpha^2 + 1)^2$ come combinazione lineare degli elementi di questa base.
b. Dato un polinomio $g \in K[X]$ irriducibile di grado 4 sia β una radice di g e $L = K[\beta]$. Quanti elementi ha L?
c. Quanti sono i campi F tali che $K \subset F \subset L$?
d. Stabilire se β è un generatore del gruppo L^*.

12 Settembre 2018

Esercizio 1

a. Siano $A_1, \dots, A_n$ anelli non banali e $A = A_1 \times \cdots \times A_n$. Mostrare che esistono $a_1, \dots, a_n \in A$ non nulli tali che $a_1 + \cdots + a_n = 1 \in A$ e $a_1^2 = a_1, \dots, a_n^2 = a_n$.
b. Sia ora B un anello e supponiamo che esistano $b_1, \dots, b_n \in B$ non nulli tali che $b_1 + \cdots + b_n = 1 \in B$ e $b_1^2 = b_1, \dots, b_n^2 = b_n$. Mostrare che $b_i B$ è un sottoanello di B per ogni $i = 1, \dots, n$.
c. Mostrare che esistono n anelli non non banali $B_1, \dots, B_n$ tali che $B \cong B_1 \times \cdots \times B_n$.

Esercizio 2 Si considerino gli anelli $A = \mathbb{Z}_3[X]/(X^2 + X + 2)$ e $B = \mathbb{Z}_3[Y]/(Y^2 + 2Y + 2)$.

a. Mostrare che A e B sono $\mathbb{Z}_3$-spazi vettoriali isomorfi e stabilire un isomorfismo esplicito tra essi.
b. Mostrare che A e B sono anelli isomorfi e stabilire un isomorfismo esplicito tra essi.
c. Mostrare che A e B sono campi isomorfi e stabilire un isomorfismo esplicito tra essi.

Esercizio 3 Sia $L = \{f \in \mathbb{Q}(X) : f(X) = f(X^{-1})\}$.

a. Mostrare che L è un campo.
b. Mostrare che $\varphi : \mathbb{Q}(X) \to L$ dato da $\varphi(f) = f(X + X^{-1})$ è un omomorfismo (iniettivo) di campi.
c. (*) Mostrare che $\varphi : \mathbb{Q}(X) \to L$ è anche suriettivo.

14 Gennaio 2019

Esercizio 1. Sia $\mathbb{D} = \mathbb{Z}[1/10] = \{\frac{a}{10^n} : a, n \in \mathbb{Z}\}$.

a. Mostrare che $\mathbb{D}$ ùn sottoanello di $\mathbb{R}$ che $\mathbb{D}$ è l'insieme dei numeri reali che ammettono un'espressione decimale finita.
b. Dato un ideale I di $\mathbb{D}$ sia a un generatore dell'ideale $I \cap \mathbb{Z}$ di $\mathbb{Z}$. Mostrare che a è anche un generatore di I e dedurre che $\mathbb{D}$ è un PID.
c. Descrivere gli elementi invertibili di $\mathbb{D}$.
d. Determinare, se esiste, MCD(0.42, 38500) in $\mathbb{D}$.

Esercizio 2 Consideriamo il polinomio $F = X^4 + 2$.

a. Mostrare che F é irriducibile in $\mathbb{Z}[X]$.
b. Dato un polinomio $G \in \mathbb{Z}[X]$, $G \notin (F)$, mostrare che l'ideale (F, G) contiene un polinomio non nullo di grado < 4.
c. Mostrare che l'ideale (F, G) contiene una costante non nulla.
d. Determinare un polinomio $G \notin (F)$ e tale che (F, G) è un ideale massimale.
e. Determinare un polinomio $H \notin (F)$ e tale che (F, H) non è un ideale massimale.

Esercizio 3 Siano $a, b \in \mathbb{Z}$ dispari tali che $a^3 = b^2 + 4$.

a. Mostrare che se p è primo allora p non divide $b + 2i$.
b. Mostrare che $MCD(b + 2i, b - 2i) = 1$ in $\mathbb{Z}[i]$.
c. Dedurre che $b + 2i$ e $b - 2i$ sono associati a due cubi in $\mathbb{Z}[i]$.
d. Mostrare che gli invertibili di $\mathbb{Z}[i]$ sono dei cubi e dedurre che anche $b + 2i$ e $b - 2i$ sono cubi in $\mathbb{Z}[i]$.

12 Febbraio 2019

Esercizio 1. Sia $\pi_5 = 1 + 2i \in \mathbb{Z}[i]$ e consideriamo l'insieme di numeri complessi

$$A = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in \mathbb{Z}[i],\ \beta \notin (\pi_5) \right\}.$$

a. Mostrare che A è un anello con le usuali operazioni di somma e prodotto;
b. Determinare gli elementi invertibili di A;
c. Stabilire se gli ideali di A generati rispettivamente da π_5 e da 7 sono massimali.
d. Determinare un ideale proprio non massimale I di A e determinare il nucleo dell'unico omomorfismo $\mathbb{Z} \to A/I$.

Esercizio 2 Sia K un campo e consideriamo il polinomio $F = X^2 + Y^2 + Z^2 \in K[X, Y, Z]$.

a. Mostrare che se K ha caratteristica 2 allora F è riducibile.
b. Se $\mathrm{car}(K) \neq 2$ consideriamo il campo $L = K(Y, Z)$. Mostrare che F è irriducibile in $L[X]$.
c. Concludere che se $\mathrm{car}(K) \neq 2$ allora F è irriducibile in $K[X, Y, Z]$.

Esercizio 3 Consideriamo il polinomio

$$F = X^9 + 3X^8 + 5X^3 - 3X^2 + 3X + 17 \in \mathbb{Z}[X].$$

Per ogni primo p denotiamo $\rho_p : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ la riduzione modulo p di un polinomio.

a. Mostrare che il polinomio $X^3 - X - 1$ è irriducibile in $\mathbb{Z}_3[X]$ e verificare che $\rho_3(F) = (X^3 - X - 1)^3$.
b. Mostrare che il polinomio $X^4 + X + 1$ è irriducibile in $\mathbb{Z}_2[X]$ e verificare che $\rho_2(F) = (X + 1)(X^4 + X + 1)^2$.
c. Dedurre che il polinomio F è irriducibile in $\mathbb{Z}[X]$ e quindi anche in $\mathbb{Q}[X]$.

4 Giugno 2019

Esercizio 1 Sia $A = \mathbb{Z}[\sqrt{10}]$.

a. Mostrare che $I = \{a + b\sqrt{10} : 2|a, 2|b\}$ è un ideale di A.
b. Stabilire se I è un ideale massimale.
c. Che anello è A/I?
d. Determinare un ideale non banale J di I e descrivere l'anello quoziente I/J.

Esercizio 2 Consideriamo l'anello $A = \mathbb{Z}[\sqrt{5}]$.

a. Scrivere i quadrati in $\mathbb{Z}_5$ e dedurre che non esistono elementi di norma ± 2 in A.
b. Mostrare che 2 non è associato né a $3 + \sqrt{5}$ né a $3 - \sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$.
c. Dedurre che $\mathbb{Z}[\sqrt{5}]$ non è un dominio a fattorizzazione unica.

Esercizio 3 Siano $f = X^3 - X - 1$ e $g = X^3 - X + 1$ polinomi in $\mathbb{F}_3[X]$.

a. Determinare i campi di spezzamento di f e di g si $\mathbb{F}_3$.
b. Determinare esplicitamente, se esiste, un isomorfismo

$$\varphi : \mathbb{F}_3[X]/(f) \to \mathbb{F}_3[X]/(g)$$

2 Luglio 2019

Esercizio 1 Sia $n \in \mathbb{Z}$, $n \neq 0$, e $A = \mathbb{Z}[X]/(nX - 1)$.

a. Mostrare che esiste un anello A' isomorfo ad A tale che $A \subseteq \mathbb{Z} \subseteq \mathbb{Q}$;
b. Per quali valori di n si ha $\mathbb{Z} = A'$?
c. Mostrare che A é un dominio a fattorizzazione unica.
d. Piú in generale, mostrare che se B é un dominio a fattorizzazione unica e $0 \neq b \in B$ allora $B/(bX - 1)$ é ancora un dominio a fattorizzazione unica.

Esercizio 2 Consideriamo la funzione $\rho : \mathbb{Z} \to \mathbb{Z}$ data da

$$\rho(m) = n \iff 2^n \leq |m| < 2^{m+1}$$

per ogni $m \neq 0$, e $\rho(0) = -1$.

a. Determinare q ed r con $\rho(r) < 3$ tali che $45 = q(-11) + r$.
b. Mostrare che ρ é una valutazione euclidea su $\mathbb{Z}$.
c. Mostrare se $a = qb + r$ con $\rho(r) < \rho(b)$ allora $|r| < |b|$ ma non é vero il viceversa.

Esercizio 3 Sia $f = X^5 - 5X^3 + 5 \in \mathbb{Q}[X]$

a. Mostrare che f é irriducibile.
b. Mostrare che f ha tre radici reali e due complesse coniugate.
c. Dedurre che il campo di spezzamento di f su $\mathbb{Q}$ ha grado divisibile per 10

$$\varphi : \mathbb{F}_3[X]/(f) \to \mathbb{F}_3[X]/(g)$$

9 Settembre 2019

Esercizio 1. Si consideri l'anello $A = \mathbb{Z}[X, Y]/(2XY - 1)$.

a. Stabilire se 2 é invertibile in A.
b. Mostrare che $2XY - 1$ é irriducibile in $\mathbb{Z}[X, Y]$.
c. Dedurre che A é un dominio.
d. Stabilire se le classi in A degli elementi X, X^2Y, $2X^2 - XY$ sono irriducibili

Esercizio 2 Consideriamo l'anello $A = \mathbb{Z}[i]/(2 + i)$

a. Stabilire se A é un dominio euclideo;
b. Determinare, se esiste, un omomorfismo di anelli $\mathbb{Z}_{25} \to A$;
c. determinare se esiste, un omomorfismo di anelli, $\mathbb{F}_{25} \to A$.

Esercizio 3 Consideriamo il polinomio $P = x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2 \in \mathbb{Q}[X]$ e sia K il campo di spezzamento di P su $\mathbb{Q}$.

a. Stabilire se il polinomio P é irriducibile.
b. Determinare il grado dell'estensione $[K : \mathbb{Q}]$.
c. Determinare, se esiste, un elemento $\alpha \in K$ tale che $K = \mathbb{Q}[\alpha]$.

9 Gennaio 2020

Esercizio 1. Sia $A = \mathbb{Z}[2/3]$ l'intersezione di tutti i sottoanelli di $\mathbb{Q}$ che contengono sia $\mathbb{Z}$ che $\frac{2}{3}$.

a. Determinare il gruppo $\mathcal{U}(A)$ degli elementi invertibili di A
b. Stabilire se $(\mathcal{U}(A), \cdot)$ è isomorfo al gruppo $(\mathbb{Z}, +)$
c. Stabilire se esiste un omomorfismo $\varphi : A \to \mathbb{Z}_6$.
d. Determinare un omomorfismo $\psi : A \to \mathbb{Z}_7$.
e. Stabilire se l'ideale $\ker \psi$ è massimale.
f. Stabilire se l'ideale $\ker \psi$ è principale.

Esercizio 2 In $\mathbb{Z}[i]$ consideriamo l'elemento $\alpha = -4 + 7i$.

a. Determinare la fattorizzazione in irriducibili si α.
b. Determinare la cardinalità di $A = \mathbb{Z}[i]/(\alpha)$.
c. Mostrare che A è prodotto cartesiano di due campi.
d. Stabilire se esiste un omomorfismo $A \to \mathbb{Z}_n$ per qualche n.

Esercizio 3 Sia $K = \mathbb{Q}[\sqrt[3]{3}]$.

a. Determinare $[K : \mathbb{Q}]$ e una base di K come $\mathbb{Q}$-spazio vettoriale.
b. Determinare tutti i campi L tali che $\mathbb{Q} \subseteq L \subseteq K$.
c. Mostrare che l'identità è l'unico automorfismo di K.
d. Dedurre che K non è un campo di spezzamento di un polinomio su $\mathbb{Q}$.

28 Gennaio 2020

Esercizio 1. Siano A e B due anelli (commutativi unitari) di caratteristica m, n rispettivamente, con $m, n \geq 0$ (eventualmente si può risolvere l'esercizio con $A = \mathbb{Z}_m$ e $B = \mathbb{Z}_n$ dove poniamo per convenzione $\mathbb{Z}_0 = \mathbb{Z}$).

a. Determinare la caratteristica di $A \times B$.
b. determinare, se esiste, un anello che non é un dominio di caratteristica 5.
c. determinare la caratteristica di A^A.
d. sia I un ideale di A. Mostrare che la caratteristica di A/I divide la caratteristica di A.

Esercizio 2 Sia $A = \mathbb{Z}[i]$.

a. Mostrare che l'ideale $I = (X, 5)$ di $A[X]$ non è principale;
b. Detto $J = (X, 3)$ sia
$$S = \{ab : a \in I, b \in J\}$$
e stabilire se gli elementi $5X, 3X, X$ appartengono ad S.
c. Stabilire se S è un ideale di $A[X]$ (potrà essere utile il punto precedente).
d. Mostrare che $IJ = (X, 15)$.

Esercizio 3 Stabilire se

a. $\mathbb{Z}_5[\sqrt{2}]$ è isomorfo a $\mathbb{Z}_5[\sqrt{3}]$;
b. $\mathbb{F}_{25}[\sqrt{2}]$ è isomorfo a $\mathbb{F}_{25}[\sqrt{3}]$ (sugg.: determinare quante radici ha il polinomio $X^2 - 2$ in $\mathbb{F}_{25}[\sqrt{3}]$).
c. $\mathbb{F}_{125}[\sqrt{2}]$ è isomorfo a $\mathbb{F}_{125}[\sqrt{3}]$;
d. $\mathbb{Q}[\sqrt{2}]$ è isomorfo a $\mathbb{Q}[\sqrt{3}]$.

09 Gennaio 2023

Esercizio 1

a. Sia $f \in \mathbb{Q}[X]$ irriducibile con $\deg f = 3$ e L il suo campo di spezzamento. Mostrare che se $[L : \mathbb{Q}] = 3$ allora f ha tre radici reali distinte.
b. Sia ora $f = X^3 - X^2 - 2X + 1 \in \mathbb{Q}[X]$. Mostrare che f é irriducibile.
c. Sia α una radice reale di f e sia $\beta = \alpha^2 - \alpha - 1$. Mostrare che $\alpha \neq \beta$.
d. Mostrare che β é una radice di f.
e. Detto L il campo di spezzamento di f concludere che $[L : \mathbb{Q}] = 3$.

Esercizio 2 Sia $A = \mathbb{Z}[\sqrt{-2}]$.

a. Sia $n \in \mathbb{Z}$, $n > 0$. Mostrare che n é irriducibile in A se e solo se n é un numero primo e non é della forma $n = a^2 + 2b^2$, con a, b interi.
b. Sia p un numero primo tale che $p = a^2 + 2b^2 = c^2 + 2d^2$, con $a, b, c, d > 0$. Mostrare che $a = c$ e $b = d$.
c. Determinare quali n con $1 \leq n \leq 10$ sono irriducibili in A.
d. Sia $\alpha \in A$ tale che $N(\alpha)$ sia divisibile per 3. Mostrare che α é riducibile.
e. Determinare la fattorizzazione in irriducibili di $-11 + 5\varepsilon$ (dove $\varepsilon^2 = -2$).

Esercizio 3

a. Stabilire quanti e quali sono gli omomorfismi di anelli $\phi : \mathbb{Z}_{/6} \to \mathbb{Z}_{/3}$.
b. Determinare quanti sono gli omomorfismi $\varphi : \mathbb{Z}_{/6}[X] \to \mathbb{Z}_{/3}[X]$.
c. Consideriamo l'ideale di $\mathbb{Z}_{/6}[X]$ dato da $I = (X^2, 3)$. Determinare la cardinalitá di $\mathbb{Z}_{/6}[X]/I$.
d. Stabilire se $\mathbb{Z}_{/6}[X]/I$ é un dominio
e. Stabilire se $\mathbb{Z}_{/6}[X]/I$ é isomorfo ad un'estensione quadratica di un anello noto.

23 Gennaio 2023

Esercizio 1 Consideriamo il polinomio $f = X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$

a. Mostrare che f é irriducibile e determinare le sue radici;
b. dette α e β due radici di f con $\alpha \neq \pm\beta$ mostrare che $K_1 = \mathbb{Q}[\alpha] \neq K_2 = \mathbb{Q}[\beta]$;
c. mostrare che $K_1 \cap K_2 = \mathbb{Q}[\sqrt{3}]$.
d. mostrare che $\mathbb{Q}[\alpha, \beta]$ é un'estensione di grado 8 di $\mathbb{Q}$.
e. mostrare che l'estensione $\mathbb{Q}[\alpha, \beta]/\mathbb{Q}[\sqrt{3}]$ é un'estensione normale il cui gruppo di Galois é $\mathbb{Z}_{/2} \times \mathbb{Z}_{/2}$.

Esercizio 2 Sia $A = \mathbb{Z}[i]$. Per ogni $p \equiv 1 \mod 4$ indichiamo con $\pi_p = a + bi$ l'unico elemento di A tale che $N(\pi_p) = p$ con $0 < a < b$.

a. Determinare π_{41} e $c \in \mathbb{Z}$ tale che $4c \equiv 1 \mod 41$;
b. mostrare che $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{/41}$ dato da $\varphi(x + iy) = [x + 5cy]_{41}$ è un omomorfismo di anelli;
c. mostrare che $\ker \varphi = (\pi_{41})$
d. concludere che $A/(\pi_{41}) \cong \mathbb{Z}_{/41}$
e. generalizzando i punti precedenti mostrare che per ogni primo $p \equiv 1 \mod 4$ si ha $\mathbb{Z}[i]/(\pi_p) \cong \mathbb{Z}_{/p}$.

Esercizio 3 Sia $\omega \in \mathbb{C}$ una radice primitiva terza dell'unitá e $A = \{a + b\omega : a, b \in \mathbb{Z}\}$.

a. Mostrare che A é un sottoanello di $\mathbb{C}$;
b. mostrare che $\overline{a + b\omega} = a - b - b\omega$ (dove la barra indica il coniugio complesso) e determinare la norma complessa di un generico elemento $a + b\omega \in A$;
c. sia $c \in \mathbb{Z}$ tale che $c \in (2 - 5\omega)$: mostrare che $39|c$;
d. mostrare che il sottoanello fondamentale di $A/(2 - 5\omega)$ é $\mathbb{Z}_{/39}$;
e. stabilire se $2 - 5\omega$ é primo in A.

13 Febbraio 2023

Esercizio 1 Sia A un anello unitario. Un ideale I di A si dice primo se per ogni $x, y \in A$ tali che $xy \in I$ si ha $x \in I$ oppure $y \in I$.

a. mostrare che un ideale massimale é sempre un ideale primo;
b. sia $Nil(A) = \{a \in A : a^n = 0 \text{ per qualche } n > 0\}$ l'insieme degli elementi nilpotenti di A. Mostrare che $Nil(A)$ é un ideale di A;
c. mostrare che se I é un ideale primo di A allora $Nil(A) \subseteq I$;
d. determinare $Nil(\mathbb{Z}_{/6})$ e $Nil(\mathbb{Z}_{/8})$;
e. mostrare che $Nil(A/Nil(A)) = \{0\}$

Esercizio 2 Sia $K \subseteq L \subseteq \mathbb{C}$ un'estensione di campi, $f \in K[X]$ irriducibile e L il campo di spezzamento di f. Siano α, β radici di f e $G = Gal(L/K)$;

a. richiamando un risultato visto mostrare che esiste $\tau \in G$ tale che $\tau(\alpha) = \beta$;
b. usando il punto (a) mostrare che i sottogruppi $Gal(L/K[\alpha])$ e $Gal(L/K[\beta])$ di G sono coniugati tra loro (due sottogruppi H, K di un gruppo G si dicono coniugati se esiste $g \in G$ tale che $g^{-1}Hg = K$) ;
c. dedurre che se G é abeliano allora $K[\alpha] = K[\beta]$;
d. concludere che se G é abeliano allora $L = K[\alpha]$;
e. mostrare con un esempio che senza l'ipotesi "G abeliano" non é detto che $L = K[\alpha]$.

Esercizio 3

a. Mostrare che se $\cos\alpha$ e $\cos\beta$ sono costruibili con riga e compasso allora lo é anche $\cos(\alpha + \beta)$.
b. Sia $\omega = e^{\frac{2\pi i}{9}}$. Determinare $[\mathbb{Q}[\omega] : \mathbb{Q}]$ e dedurre che $\cos(40°)$ non é costruibile con riga e compasso;
c. mostrare che con riga e compasso é possibile costruire $\cos(9°)$ e $\cos(30°)$;
d. usare (a) e (c) per mostrare che é possibile costruire $\cos(3°)$;
e. mostrare che, per $n > 0$, $\cos(n°)$ é costruibile con riga e compasso se e solo se n é un multiplo di 3.

05 Giugno 2023

Esercizio 1 Sia A un dominio d'integritá e I un ideale di A tale che A/I sia a sua volta un dominio d'integritá. Consideriamo l'insieme dei "simboli"

$$B = \left\{ \frac{x}{y} : x, y \in A,\ y \notin I \right\}$$

e consideriamo su B la relazione $\sim$ data da

$$\frac{x}{y} \sim \frac{x'}{y'} \quad se\ \ xy' = x'y.$$

a. mostrare che $\sim$ é una relazione d'equivalenza su B;
b. mostrare che l'insieme quoziente $B/\sim$ ha in modo naturale una struttura di anello;
c. determinare gli elementi invertibili di $B/\sim$;
d. mostrare che gli elementi non invertibili formano un ideale e spiegare perché questo é l'unico ideale massimale di $B/\sim$;
e. con $A = \mathbb{Z}$ e $I = p\mathbb{Z}$ descrivere esplicitamente l'anello $B/\sim$.

Esercizio 2 Sia $\alpha = -3 + 9i \in \mathbb{Z}[i]$ e poniamo $A = \mathbb{Z}[i]/(\alpha)$.

a. fattorizzare α in irriducibili;
b. stabilire se A é un dominio;
c. stabilire se A contiene elementi nilpotenti;
d. determinare il sottoanello fondamentale di A;
e. stabilire se A contiene piú di 30 elementi.

Esercizio 3 Sia $\alpha \in \mathbb{C}$ un numero algebrico di grado 3 su $\mathbb{Q}$.

a. Determinare il grado di α^2 su $\mathbb{Q}$;
b. mostrare che il grado di α^3 é 1 o 3: mostrare un esempio in cui α^3 ha grado 1 e un esempio in cui ha grado 3;
c. supponiamo inoltre che $\mathbb{Q}[\alpha]$ sia un'estensione di Galois di $\mathbb{Q}$ e siano β e γ le altre due radici del polinomio minimo di α. Mostrare che $\alpha^2 + \beta^2 + \gamma^2 \in \mathbb{Q}$ (sugg.: ricordare che $\mathbb{Q} = \mathbb{Q}[\alpha]^G$ dove $G = Gal(\mathbb{Q}[\alpha]/\mathbb{Q})$;
d. determinare $[Q[\alpha\beta] : \mathbb{Q}]$;
e. Sia $\delta \in \mathbb{C}$ tale che $\mathbb{Q}[\alpha] \neq \mathbb{Q}[\delta]$. Mostrare che $\mathbb{Q}[\alpha] \ncong \mathbb{Q}[\delta]$.

27 Giugno 2023

Esercizio 1. Sia $f = X^3 - 2$ e F il campo di spezzamento di f su $\mathbb{Q}$.

a. Determinare $[F : \mathbb{Q}]$;
b. determinare se esiste un elemento $\alpha \in \mathbb{C}$ tale che $F = \mathbb{Q}[\alpha]$;
c. determinare il polinomio minimo di α su $\mathbb{Q}$;
d. dato un campo $K \subseteq \mathbb{C}$ sia L il campo di spezzamento di f su K: mostrare che $[L : K]$ é un divisore di 6;
e. per $d = 1, 2, 3, 6$ determinare, se esiste, un campo K_d tale che il campo di spezzamento L_d per f su K_d soddisfi $[L_d : K_d] = d$.

Esercizio 2 Consideriamo i seguenti sottoinsiemi di $\mathbb{Z}[X]$

$$I = \{f \in \mathbb{Z}[X] : \tilde{f}(0) \text{ é pari}\}, \quad J = \{f \in \mathbb{Z}[X] : \tilde{f}(0) \text{ é multiplo di } 3\}$$

(dove $\tilde{f}$ indica la funzione polinomiale associata ad f).

a. Mostrare che I e J sono ideali di $\mathbb{Z}[X]$;
b. stabilire se I e J sono ideali massimali;
c. stabilire se I e J sono ideali coprimi;
d. determinare esplicitamente l'ideale prodotto IJ;
e. determinare esplicitamente l'ideale quoziente $\mathbb{Z}[X]/IJ$.

Esercizio 3

Dato un anello A e un sottoinsieme $I \subseteq A$ poniamo $\sqrt{I} = \{x \in A : \exists n > 0 \text{ tale che } x^n \in I\}$. Sia inoltre $\varphi : A \to B$ un omomorfismo di anelli.

a. Mostrare che se I é un ideale di A allora $\sqrt{I}$ é ancora un ideale di A;
b. mostrare che $\varphi(\sqrt{I}) \subseteq \sqrt{\varphi(I)}$;
c. mostrare che se φ é suriettiva e $\ker \phi \subseteq I$ allora $\sqrt{\varphi(I)} = \varphi(\sqrt{I})$;
d. Sia $A = B = \mathbb{Z}[X]$, $\varphi(f(X) = f(X^2)$, $I = (X^3)$. Determinare $\sqrt{I}$ e $\varphi(I)$.
e. Nelle stesse notazioni del pnuto precedente determinare $\varphi(\sqrt{I})$ e $\sqrt{\varphi(I)}$.

12 Luglio 2023

Esercizio 1. Siano $\alpha = \sqrt[5]{3}$, e $\varepsilon = e^{\frac{2\pi i}{5}}$ una radice primitiva quinta dell'unitá.

a. Determinare il polinomio minimo di α e il polinomio minimo di ε;
b. mostrare che $\mathbb{Q}[\varepsilon] = \mathbb{Q}[\varepsilon^2]$;
c. mostrare che $L = \mathbb{Q}[\alpha, \varepsilon]$ é un'estensione normale di $\mathbb{Q}$;
d. mostrare che se $\sigma \in Gal(L/\mathbb{Q})$ ha ordine 5 allora $\sigma(\varepsilon) = \varepsilon$;
e. concludere che $\mathbb{Q}[\varepsilon]$ é l'unica estensione di grado 4 di $\mathbb{Q}$ contenuta in L.

Esercizio 2 Siano A_1 e A_2 due anelli non banali e $R = A_1 \times A_2$.

a. Mostrare che R non é un dominio d'integritá;
b. mostrare che se I_1 e I_2 sono rispettivamente ideali di A_1 e A_2 allora $I_1 \times I_2$ é un ideale di R;
c. mostrare che se I é un ideale di R allora esistono I_1 e I_2 ideali rispettivamente di A_1 e A_2 tali che $I = I_1 \times I_2$;
d. quanti sono gli ideali di $\mathbb{Z}_{/90}$?
e. stabilire se $(A_1 \times A_2)/(I_1 \times I_2) \cong A_1/I_1 \times A_2/I_2$.

Esercizio 3 Sia A un anello unitario e consideriamo l'insieme

$$R(A) = \left\{ \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} : a, b \in A. \right\} \subset M_{2,2}(A).$$

a. mostrare che $R(A)$ é un anello unitario rispetto alle usuali operazioni di somma e prodotto di matrici;
b. mostrare che $R(\mathbb{R})$ é un campo;
c. mostrare che $R(\mathbb{Z}_{/5}) \cong \mathbb{F}_{25}$;
d. stabilire quanti sono gli elementi invertibili di $R(\mathbb{Z}_{/7})$;
e. mostrare che $R(\mathbb{Z}_{/7}) \cong \mathbb{Z}_{/7}[\sqrt{4}]$.

11 Settembre 2023

Esercizio 1. Siano A, B anelli unitari con A sottoanello di B. Dire se le seguenti affermazioni sono vere o false spiegandone la motivazione

a. se B é un campo allora anche A é un campo;
b. se A é un campo di caratteristica 0 allora anche B é un campo;
c. se A é un campo e B é uno spazio vettoriale di dimensione finita su A allora B é un campo.
d. se A é un dominio euclideo allora anche B lo é
e. se B é un UFD allora anche A lo é.

Esercizio 2 Sia L/K un'estensione finita con $[L : K] = 4$ e $\gamma \in L$ tale che $L = K[\gamma]$.

a. mostrare che per ogni $\alpha \in L$ l'applicazione $f_\alpha : L \to L$ data da $f_\alpha(\beta) = \alpha\beta$ per ogni $\beta \in L$ é un endomorfismo di L come K-spazio vettoriale. É anche un omomorfismo di anelli?
b. descrivere una base di L come K-spazio vettoriale;
c. scrivere la matrice M_γ associata a f_γ rispetto alla base determinata nel punto precedente (in funzione dei coefficienti del polinomio minimo di γ);
d. mostrare che $\det(XI - f_\gamma) \in K[X]$ é il polinomio minimo di γ su K;
e. per quali $\alpha \in L$ si ha che $\det(XI - f_\alpha)$ é il polinomio minimo di α su K?

Esercizio 3

a. sia A un anello e $a \in A$ nilpotente. Mostrare che $1 + a$ é invertibile e dedurre che la somma di un invertible e un nilpotente é sempre invertibile;
b. dare un esempio di un polinomio invertibile di grado 1 in $\mathbb{Z}_{/4}[X]$;
c. sia ora $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ invertibile e $g = b_0 + b_1X + \cdots + b_mX^m$ l'inverso di f (con $n > 0$, $a_n, b_m \neq 0$). Mostrare che a_0 é invertibile;
d. mostrare che $a_n^{r+1}b_{m-r} = 0$ per ogni $r \leq m$ e dedurre che a_n é nilpotente
e. concludere dai punti precedenti che $a_1, \ldots, a_n$ sono tutti nilpotenti.

Soluzioni 09 Gennaio 2017

Esercizio 1 a. Se α è una radice di f abbiamo $\alpha^4+6\alpha^2+4=0$ da cui $\alpha^2=-3\pm\sqrt{5}$ e quindi $\pm\sqrt{5}=\alpha^2+3\in L$ perché $\alpha\in L$.

b. Osserviamo che f non ha radici reali (e in particolare non ha radici in K o in $\mathbb{Q}$) e quindi in $\mathbb{R}[X]$ si fattorizza nel prodotto di due polinomi irriducibili di secondo grado: questa fattorizzazione è data da $f=(X^2+3+\sqrt{5})(X^2+3-\sqrt{5})$. Questa fattorizzazione è valida anche in $K[X]$ (chiaramente i due polinomi rimangono irriducibili in $K[X]$. Osserviamo che f non può avere una fattorizzazione in $\mathbb{Q}[X]$ come prodotto di due polinomi di secondo grado irriducibili, altrimenti questa sarebbe una fattorizzazione in $K[X]$ (o in $\mathbb{R}[X]$) contraddicendo la precedente e quindi f è irriducibile in $\mathbb{Q}[X]$.

c. Siccome f è irriducibile su $\mathbb{Q}$, α ha grado 4 su $\mathbb{Q}$ e quindi anche α^{-1} ha grado 4 (questo perché, ad esempio, $\mathbb{Q}[\alpha]=\mathbb{Q}[\alpha^{-1}]$). Abbiamo quindi $\alpha^4+6\alpha^2+4=0$ e dividendo per α^4 otteniamo $1+6\alpha^{-2}+4\alpha^{-4}=0$ e quindi α^{-1} è radice del polinomio $1+6X^2+4X^4$ da cui il polinomio minimo di α^{-1} è $X^4+\frac{3}{2}X^2+\frac{1}{4}$.

d. Sia α una radice di $X^2+3+\sqrt{5}$. Abbiamo che $\mathbb{Q}[\sqrt{5},\alpha]\subseteq L$ e vogliamo mostrare che in realtà vale l'uguaglianza. Per questo è sufficiente mostrare che $\mathbb{Q}[\sqrt{5},\alpha]$ contiene una radice di $X^2+3-\sqrt{5}$. E infatti $2/\alpha$ è una radice di $X^2+3-\sqrt{5}$. Questo deriva dal fatto che se $d=-3-\sqrt{5}$ e $d'=-3+\sqrt{5}$ abbiamo $dd'=4$ e quindi $d'=4/d$ e quindi una radice quadrata di d' è data da $2/\alpha$.

Un altro modo di vedere questo fatto (seguendo più fedelmente il suggerimento) è il seguente. Se K è un campo e d non è un quadrato in K consideriamo l'estensione $K[\sqrt{d}]$. Ci chiediamo quali elementi di K sono quadrati in $K[\sqrt{d}]$. Abbiamo $(a+b\varepsilon)^2=a^2+b^2d+2ab\varepsilon$. Questo quadrato sta in K se e solo se $a=0$ oppure $b=0$. Nel primo caso otteniamo elementi del tipo a^2 nel secondo del tipo b^2d. Nel nostro caso ci chiediamo quindi se d' è della forma b^2d o, equivalentemente, se d'/d è un quadrato di K e abbiamo già osservato che $d'/d=4/d^2$, che è chiaramente un quadrato.

Esercizio 2

a. Abbiamo, posto $\alpha=1+2\sqrt{3}$

$$\alpha^{-1}=\frac{\bar{\alpha}}{N(\alpha)}=\frac{1-2\sqrt{3}}{-11}=-\frac{1}{11}+\frac{2}{11}\sqrt{3}.$$

b. Osserviamo che i 3 elementi hanno tutti la stessa norma in valore assoluto (condizione necessaria affinchè possano essere associati). Due elementi sono associati se il loro rapporto (in $\mathbb{Q}[\sqrt{3}]$) è invertibile in A. Abbiamo $8+5\sqrt{3}/\alpha=2+\sqrt{3}$ (che è invertibile in A avendo norma 1), mentre $17+10\sqrt{3}/\alpha=\frac{43}{11}+\frac{24}{11]\sqrt{3}}$ (che non sta in A).

c. L'elemento $2+\sqrt{3}$ ottenuto nel punto b. è invertibile (ha norma 1). Essendo un numero reale diverso da >1 tutte le sue potenze sono distinte e saranno tutte invertibili in A.

Esercizio 3

Osserviamo che $665 = 5 \cdot 7 \cdot 19$ e quindi dobbiamo risolvere il sistema modulo 5,7 e 19 per il teorema cinese del resto.

Il polinomio $X^3 + 13X^2 + 48X + 36$ si fattorizza nella forma $(X+1)(X+6)^2$ in $\mathbb{Z}[X]$ e quindi anche in $\mathbb{Z}_p[X]$ per ogni primo p. Risolviamo quindi il sistema nei tre moduli 5,7,19.
– Modulo 5
La seconda equazione diventa $(X+1)^3$ e quindi l'unica soluzione è -1. Questa chiaramente soddisfa anche la prima equazione.
– Modulo 7
La seconda equazione ha soluzione -1 e $-6 = 1$ e queste chiaramente soddisfano la prima equazione.
– Modulo 19
La seconda equazione ha soluzione -1 e -6 e osservando che ogni elemento di $\mathbb{Z}_{19}$ soddisfa la prima equazione (per il piccolo Fermat) concludiamo che sono entrambe accettabili.

Otteniamo quindi 4 soluzioni combinando le varie possibilità modulo 5,7 e 19: (-1,-1,-1), (-1,1,-6),(-1,-1,-6), (-1,1,-1) . Le prime due triple danno le soluzioni -1 e -6 che già conoscevamo dalla fattorizzazione di $X^3 + 13X^2 + 48X + 36$. La terza tripla dà il sistema

$$\begin{cases} X \equiv -1 \mod 35 \\ X \equiv -6 \mod 19 \end{cases}$$

da cui $X = -1 + 35k$ e quindi $-1 + 35k \equiv -6 \mod 19$. Osservando che $35 = -3 \mod 19$ e moltiplicando per 6 l'equazione otteniamo $-6 - 18k = 2 \mod 19$ e quindi $-6 + k = 2$ e infine $k = 8$. Concludiamo che $X = -1 + 35 \cdot 8 = 279$ è la terza soluzione.

L'altra soluzione si può calcolare analogamente e dovrebbe essere 379.

Soluzioni 23 Gennaio 2017

Esercizio 1

a. Basta osservare che $\alpha^4 f(\alpha^{-1}) = f(\alpha)$ e quindi se α è radice anche α^{-1} lo è.

b. Verifichiamo che f è irriducibile su $\mathbb{Q}$. Senz'altro non ha radici (le uniche possibili sono ± 1) e se proviamo a fattorizzarlo in $\mathbb{Z}[X]$ otteniamo

$$X^4 - 8X^2 + 1 = (X^2 + aX \pm 1)(X^2 - aX \pm 1)$$

da cui $\pm 2 - a^2 = -8$ che non ammette soluzione in $\mathbb{Q}$.

Dal punto precedente, e osservando che f è biquadratico, abbiamo che se α è una radice allora $-\alpha$, α^{-1} e $-\alpha^{-1}$ sono radici. Queste sono tutte distinte in quanto $\alpha \neq 0, \pm 1, \pm i$ e quindi sono tutte le radici di f. Ne segue che

$$K = \mathbb{Q}[\alpha, -\alpha, \alpha^{-1}, -\alpha^{-1}] = \mathbb{Q}[\alpha]$$

e quindi $[K : \mathbb{Q}] = 4$ perché f è il polinomio minimo di α.

c. Osserviamo ora che $K \subset \mathbb{R}$. Cercando infatti le radici di f (sfruttando il fatto che è biquadratico) otteniamo $\pm\sqrt{4 \pm \sqrt{15}}$ che sono tutte reali. Osserviamo ora che

$$L = K[\sqrt{-2}]$$

e quindi che $[L : K] = 2$ visto che K, essendo reale, non può contenere $\sqrt{-2}$. Concludiamo che $[L : \mathbb{Q}] = 8$ e quindi $[L : \mathbb{Q}[\sqrt{-2}]] = 4$ sfruttando la moltiplicatività del grado delle estensioni (lemma della torre).

d. Su $\mathbb{Z}_{11}$ il polinomio f si fattorizza nel seguente modo:

$$f = (X^2 - 2)(X^2 - 6)$$

e osserviamo che 2 e 6 non sono quadrati in $\mathbb{Z}_{11}$. Ricordando che $\mathbb{F}_{11^2}$ contiene le radici quadrate di tutti gli elementi di $\mathbb{Z}_{11}$ abbiamo che il campo di spezzamento è proprio $\mathbb{F}_{121}$.

Esercizio 2

a. Abbiamo $\alpha = 5(4 - \varepsilon)$ e osserviamo che 5 è irriducibile perchè non esistono elementi di norma 5. Abbiamo inoltre $N(4 - \varepsilon) = 18$ e quindi i possibili divisori di $4 - \varepsilon$ devono avere norma che divide 18. Di norma 2 abbiamo solo ε (e associati) e proviamo a vedere se ε è un divisore di $4 - \varepsilon$. Abbiamo

$$(4 - \varepsilon)\frac{(-\varepsilon)}{2} = -1 - 2\varepsilon$$

e quindi $(4 - \varepsilon) = \varepsilon(-1 - 2\varepsilon)$. Proviamo quindi a fattorizzare $(-1 - 2\varepsilon)$ che ha norma 9. Gli elementi di norma 3 sono $1 - \varepsilon$ e $1 + \varepsilon$) (e associati). Proviamo a vedere se $1 - \varepsilon$ divide $(-1 - 2\varepsilon)$: otteniamo $-1 - 2\varepsilon = (1 - \varepsilon)^2$ e quindi la fattorizzazione in irriducibili di α è

$$\alpha = 5\varepsilon(1 - \varepsilon)^2.$$

b. $A/(\alpha)$ è un anello finito (ogni classe ha un rappresentante di norma minore di $N(\alpha)$ e chiaramente esistono un numero finito di elementi che hanno norma minore di $N(\alpha)$) e quindi ha un numero finito di ideali. In alternativa possiamo anche descrivere questi ideali esplicitamente: sappiamo che gli ideali di un quoziente $A/(\alpha)$ sono dati da $J/(\alpha)$ dove J è un ideale di A che contiene (α). Ne segue che J é generato da un divisore di α e questi

sono in numero finito (e sono 1, 5, ε, $1-\varepsilon$, $(1-\varepsilon)^2$, 5ε, $5(1-\varepsilon)$, $\varepsilon(1-\varepsilon)$, e α).
c. Gli ideali massimali sono dati dagli ideali massimali che contengono α: sono quindi quelli generati dai fattori irriducibili di α e sono quindi

$$\frac{(5)}{(\alpha)}, \frac{(\varepsilon)}{(\alpha)}, \frac{(1-\varepsilon)}{(\alpha)}.$$

d. Un quoziente A/I di un anello è un campo se e solo se I è massimale. Nel nostro esempio abbiamo che i possibili campi sono

$$\frac{A/(\alpha)}{(5)/(\alpha)} \cong \frac{A}{(5)} \cong \mathbb{F}_{25}$$

dove abbiamo usato il terzo teorema di omomorfismo e il fatto che questo campo ha caratteristica 5 (infatti $5 = 0$) e/o che ha 25 elementi: infatti, in questo quoziente, $a+b\varepsilon = a'+b\varepsilon$ se e solo se $a \equiv a'$ e $b \equiv b' \mod 5$. Similmente si ottengono gli altri due possibili quozienti

$$\frac{A/(\alpha)}{(\varepsilon)/(\alpha)} \cong \frac{A}{(\varepsilon)} \cong \mathbb{Z}_2$$

e

$$\frac{A/(\alpha)}{(1-\varepsilon)/(\alpha)} \cong \frac{A}{(1-\varepsilon)} \cong \mathbb{Z}_3.$$

Esercizio 3 a. Basta mostrare che

- A_S è un sottogruppo additivo di Q: infatti $0 = \frac{0}{1} \in A_S$. Se $\frac{a}{s} \in A_S$ anche il suo opposto $\frac{-a}{s} \in A_S$ e se $\frac{a}{s}, \frac{a'}{s'} \in A_S$ allora $\frac{a}{s} + \frac{a'}{s'} = \frac{as'+a's}{ss'} \in A_S$.
- $1 = \frac{1}{1} \in A_S$ perché $1 \in S$;
- A_S è chiuso rispetto al prodotto: se $\frac{a}{s}, \frac{a'}{s'} \in A_S$ allora $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'} \in A_S$.

b. Si ha chiaramente $A_S \subset A_{S'}$ perché $S \subset S'$. Mostriamo l'inclusion opposta e sia quindi $\frac{a}{s'} \in A_{S'}$ per ipotesi sappiamo che esistono $s \in S$ e $b \in A$ tali che $s = bs'$ ma allora

$$\frac{a}{s'} = \frac{ab}{s} \in A_S.$$

c. Sia $s' \in S'$. Per ipotesi abbiamo che $\frac{1}{s'} \in A_S$ per cui esistono $a \in A$ e $s \in S$ tali che $\frac{1}{s'} = \frac{a}{s}$ da cui $s'a = s$ e quindi s' divide s.

Soluzioni 10 Febbraio 2017

Esercizio 1 a. Sappiamo che $\{1, \sqrt{3}\}$ è una base di $\mathbb{Q}[\sqrt{3}]$ su $\mathbb{Q}$. Osserviamo inoltre che $\sqrt{7} \notin Q[\sqrt{3}]$ e quindi $\{1, \sqrt{7}\}$ è una base di $\mathbb{L}$ su $\mathbb{Q}[\sqrt{3}]$. Per il teorema sulla base di un'estensione di un'estensione deduciamo che una base di $\mathbb{L}$ su $\mathbb{Q}$ è data da $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$.
b. Basta considerare $f = (X^2 - 3)(X^2 - 7)$. Le sue radici sono $\pm\sqrt{3}$ e $\pm\sqrt{7}$ da cui il cui campo di spezzamento di f è $\mathbb{Q}[\sqrt{3}, -\sqrt{3}, \sqrt{7}, -\sqrt{7}] = \mathbb{L}$.
c. Basta porre $\alpha = \sqrt{3} + \sqrt{7}$. Infatti $\mathbb{Q}[\alpha] \subseteq \mathbb{L}$ per ovvie ragioni. Per l'inclusione opposta consideriamo $\alpha^3 = 10 + 9\sqrt{7} + 21\sqrt{3}$ da cui $\alpha^3 - 10 - 9\alpha = 12\sqrt{3}$ e quindi $\sqrt{3} \in \mathbb{Q}[\alpha]$ e quindi anche $\sqrt{7} = \alpha - \sqrt{3} \in \mathbb{Q}[\alpha]$.
d. Ogni elemento $\beta \in \mathbb{L}$ si scrive nella forma $a + b\sqrt{7}$ con $a, b \in \mathbb{Q}[\sqrt{3}]$. Se $\beta^2 \in \mathbb{Q}$ abbiamo $a^2 + 7b^2 + 2ab\sqrt{7} \in \mathbb{Q}$ da cui $ab = 0$ e $a^2 + 7b^2 \in \mathbb{Q}$. Se $a = 0$ abbiamo $b^2 \in \mathbb{Q}$ e se $b = 0$ abbiamo $a^2 \in \mathbb{Q}$. Nel primo caso $b = r + \sqrt{3}s$ con $r, s \in \mathbb{Q}$ e deduciamo che $r = 0$ e quindi $\beta = b\sqrt{7} = s\sqrt{21}$, oppure $s = 0$ e otteniamo $\beta = r\sqrt{7}$. Nel secondo caso avremmo $\beta = t + v\sqrt{3}$ con $t, v \in \mathbb{Q}$ da cui $\beta = t \in \mathbb{Q}$ oppure $\beta = v\sqrt{3}$.
e. Se $\mathbb{K}$ è un campo intermedio tra $\mathbb{Q}$ ed $\mathbb{L}$ allora $\mathbb{K}$ è della forma $\mathbb{K}[\gamma]$ con $\gamma \in \mathbb{L}$, γ di grado 2. Ora, se il discriminante del polinomio minimo di γ è Δ abbiamo $\mathbb{K}[\gamma] = \mathbb{K}[\sqrt{\Delta}]$. Per il punto precedente abbiamo che $\sqrt{\Delta} = q\sqrt{d}$ e quindi

$$\mathbb{K} = \mathbb{Q}[\gamma] = \mathbb{Q}[\sqrt{\Delta}] = \mathbb{Q}[q\sqrt{d}] = \mathbb{Q}[\sqrt{d}].$$

Abbiamo quindi che le estensioni intermedie sono $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{7}]$, $\mathbb{Q}[\sqrt{21}]$.
Esercizio 2 a. Il coefficiente di X^{n+m} in fg è $a_n b_m$. Siccome $n + m > 0$ tale coefficiente deve essere 0 e quindi, sapendo che $a_n = 3$, abbiamo $b_m = 0, 2, 4$. Ma $b_m \neq 0$ perché g ha grado m.
b. Procediamo per induzione su k. Il caso $k = 0$ è stato risolto nel punto precedente. Osserviamo che $n + m - k > 0$ e quindi il coefficiente di fg di grado $n + m - k$ deve annullarsi. Tale coefficiente è dato da:

$$a_n b_{m-k} + a_{n-1} b_{m-(k-1)} + \cdots + a_{n-(k-1)} b_{m-1} + a_{n-k} b_m = 0 \in \mathbb{Z}_6.$$

Per ipotesi induttiva tutti i termini intermedi si annullano e quindi otteniamo

$$a_n b_{m-k} + a_{n-k} b_m = 0 \in \mathbb{Z}_6.$$

Siccome il primo addendo è 0 o 3 lo stesso deve accadere al secondo e siccome $b_m = 2, 4$ l'unica possibilità è che a_{n-k} sia 0 o 3. Similmente siccome il secondo addendo è 0,2,4 lo stesso deve accadere al primo addendo e siccome $a_n = 3$ abbiamo che necessariamente $b_{m-k} = 0, 2, 4$.
c. Supponiamo per assurdo $n + m > 0$. Siccome $a_n b_m = 0$ e sia a_n che b_m sono diversi da 0, almeno uno dei due deve essere 3 e possiamo suppore $a_n = 3$. Per il punto precedente abbiamo che tutti i coefficienti di f sono multipli di 3 o tutti i coefficienti di g sono multipli di 2. In ogni caso otteniamo un assurdo perché 2 e 3 non sono invertibili. Deduciamo che f e g hanno grado 0 e quindi $f = g = 1$ oppure $f = g = 5$.
d. Gli elementi invertibili di $A\sqrt{2}]$ sono tutti gli elementi di norma invertibile, cioè 1 o 5

per il punto precedente. Un elemento generico $f + g\sqrt{2}$ è quindi invertibile se e solo se

$$f^2 - 2g^2 = 1, 5 \in \mathbb{Z}_6[X].$$

Ad esempio tutti gli elementi con $f = 1$ e g polinomio con tutti i coefficienti divisibili per 3 sono invertibili.

Esercizio 3 a. L'intersezione di una famiglia non vuota di sottoanelli è sempre un sottoanello: tutte le verifiche sono banali. Basta quindi osservare che esiste un sottoanello di $\mathbb{C}$ che contiene sia $\mathbb{Z}$ che $\sqrt[3]{2}$ e questo è proprio $\mathbb{C}$.
b. Sia $B = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{C}\}$. Si verifica facilmente che B è un sottoanello di $\mathbb{C}$ che chiaramente contiene sia $\mathbb{Z}$ che $\sqrt[3]{2}$ e quindi è uno degli anelli che andiamo ad intersecare per ottenere A. Basta ora osservare che ogni sottoanello che contiene sia $\mathbb{Z}$ che $\sqrt[3]{2}$ contiene anche B. Infatti un tale anello contiene anche $\sqrt[3]{2}^2 = \sqrt[3]{4}$ e quindi contiene tutti gli elementi che si ottengono facendo somme e prodotti di elementi in $\mathbb{Z}$, $\sqrt[3]{2}$ e $\sqrt[3]{4}$ e quindi in particolare tutti gli elementi di B.
L'unicità viene ad esempio dal fatto che A è contenuto in $\mathbb{Q}[\sqrt[3]{2}]$ che è un $\mathbb{Q}$-spazio vettoriale con base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.
c. Abbiamo

$$(\sqrt[3]{2}) = \{\alpha\sqrt[3]{2} : \alpha \in A\} = \{\sqrt[3]{2}(a+b\sqrt[3]{2}+c\sqrt[3]{4}),\ a, b, c1 \in \mathbb{Z}\} = \{2c+a\sqrt[3]{2}+b\sqrt[3]{4},\ a, b, c \in \mathbb{Z}\}.$$

d. Dal punto precedente abbiamo che l'omomorfismo

$$\varphi : A \to \mathbb{Z}_2$$

dato da $\varphi(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a \in \mathbb{Z}_2$ ha per nucleo $(\sqrt[3]{2})$ e quindi, essendo suriettivo, abbiamo

$$\frac{A}{(\sqrt[3]{2})} \cong \mathbb{Z}_2.$$

Soluzione 07 Giugno 2017

Esercizio 1 a. Se $\beta \in L \setminus K$ allora $L = K[\beta]$. Il polinomio minimo di β su K avrà grado 2 e sarà quindi del tipo

$$X^2 + 2bX + c$$

con $b, c \in K$. Ma allora $(\beta + b)^2 = b^2 - c$ e quindi basterà porre $\alpha = \beta + b$. In altre parole stiamo prendendo come α una radice quadrata del discriminante del polinomio minimo di β.

b. In $\mathbb{Z}_3$ abbiamo bisogno di un elemento che non sia un quadrato già in $\mathbb{Z}_3$: l'unico tale elemento è -1 e in effetti prendendo $L = \mathbb{Z}_3[\sqrt{-1}]$ otteniamo un'estensione quadratica ma il polinomio

$$X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$$

non è irriducibile in $\mathbb{Z}_3$.

c. Se K e L sono campi reali, senza perdita di generalità assumiamo $\alpha > 0$ e abbiamo

$$X^4 - \alpha^2 = (X^2 - \alpha)(X^2 + \alpha)$$

in $L[X]$ e in questa fattorizzazione il polinomio $X^2 + \alpha$ è irriducibile. In $K[X]$ il polinomio $X^4 + \alpha^2$ non ha radici (altrimenti conterrebbe una radice quadrata di α^2). Se fosse il prodotto di due polinomi irriducibile disecondo grado in $K[X]$ uno dei due dovrebbe essere necessariamente $X^2 + \alpha$ per la compatibilità delle fattorizzazioni e questo è assurdo perché $\alpha \notin K$.

d. Un tale campo non può esistere. Supponiamo per assurdo che esista un tale K. Per il punto a. avremmo un elemento $\alpha \in \mathbb{R}$ (che possiamo assumere > 0) tale che $\mathbb{R} = K[\alpha]$. Per il punto c. il polinomio $X^4 - \alpha^2$ è irriducibile e quindi estendendolo con una sua radice (ad esempio $\sqrt{\alpha}$) otterremmo un'estensione di grado 4 di K. Ma $\sqrt{\alpha} \in \mathbb{R}$ che è un'estensione di grado 2, e questa è una contraddizione.

Esercizio 2

a. A è contenuto nell'anello delle matrici a coefficienti in $\mathbb{Q}$. Il fatto che A sia un sottogruppo additivo è evidente (o di facile verifica). La matrice identità appartiene ad A e quindi l'unica proprietà da verificare è che A è chiuso rispetto al prodotto. Si ha

$$\begin{bmatrix} a & b \\ qb & a \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ qb' & a' \end{bmatrix} = \begin{bmatrix} aa' + qbb' & ab' + ba' \\ q(ab' + ba') & aa' + qbb' \end{bmatrix}$$

da cui si evince che il prodotto è un'operazione binaria su A commutativa.

b. Dobbiamo mostrare che con $q = 2$ ogni matrice non nulla ammette inversa in A, cioè, visto come funziona il prodotto nel punto precedente, che dati $a, b \in \mathbb{Q}$ non entrambi nulli esistono $a', b' \in \mathbb{Q}$ tali che

$$\begin{cases} aa' + 2bb' = 1 \\ ab' + ba' = 0 \end{cases}$$

E questo sistema ammette (un'unica) soluzione in $\mathbb{Q}$ per il teorema di Rouché-Capelli visto che la matrice dei coefficienti ha determinante $a^2 - 2b^2 \neq 0$.

c. Procedendo in modo analogo al caso precedente dobbiamo risolvere il sistema

$$\begin{cases} aa' + 4bb' = 0 \\ ab' + ba' = 0 \end{cases}$$

Una possibile soluzione è data da $a = a' = 2$, $b = -b' = 1$ e infatti

$$\begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

d. Abbiamo che l'ideale I generato da $\begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix}$ è costituito da tutti i multipli (in A_4!) di questa matrice per cui abbiamo

$$\begin{aligned} I &= \left\{ \begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 4b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\} \\ &= \left\{ \begin{bmatrix} 2(a+2b) & a+2b \\ 4(a+2b) & 2(a+2b) \end{bmatrix} : a, b \in \mathbb{Q} \right\} \\ &= \left\{ \begin{bmatrix} 2c & c \\ 4c & 2c \end{bmatrix} : c \in \mathbb{Q} \right\} \end{aligned}$$

e. Vista la forma degli elementi di I consideriamo la funzione $\varphi : A_4 \to \mathbb{Q}$ data da

$$\varphi \begin{bmatrix} a & b \\ 4b & a \end{bmatrix} = a - 2b.$$

Si ha chiaramente che φ è un omomorfismo di gruppi additivi. Vediamo che è anche un omomorfismo di anelli unitari. Intanto manda 1 in 1. Inoltre

$$\begin{aligned} \varphi\left(\begin{bmatrix} a & b \\ 4b & a \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ 4b' & a' \end{bmatrix} \right) &= \varphi \begin{bmatrix} aa' + 4bb' & ab' + ba' \\ 4(ab' + ba') & aa' + qbb' \end{bmatrix} \\ &= aa' + 4bb' - 2(ab' + ba') \\ &= (a - 2b)(a' - 2b') \\ &= \varphi \begin{bmatrix} a & b \\ 4b & a \end{bmatrix} \varphi \begin{bmatrix} a' & b' \\ 4b' & a' \end{bmatrix} \end{aligned}$$

Esercizio 3

a. Sappiamo che $\mathbb{Z}_7[\sqrt{d}]$ è un campo se e solo se d non è un quadrato in $\mathbb{Z}_7$. I quadrati in $\mathbb{Z}_7$ sono 0,1,2,4 e quindi $\mathbb{Z}_7[\sqrt{d}]$ è un campo se e solo se $d \in \{3, 5, 6\}$.

b. Consideriamo il generico elemento $a + \varepsilon b \in \mathbb{Z}_7[\sqrt{d}]$. Abbiamo

$$(a + b\varepsilon)^2 = a^2 + db^2 + 2ab\varepsilon.$$

Questo è 0 se e solo se $a^2 + db^2 = 0$ e $2ab = 0$. Soluzioni non banali si ottengono solo con $d = 0$ e infatti in questo caso abbiamo $\varepsilon^2 = 0$.

c. Similmente al punto precedente dobbiamo risolvere il sistema

$$\begin{cases} a^2 + db^2 = 1 \\ 2ab = 0 \end{cases}$$

Per $d = 3, 5, 6$ non possiamo avere 3 soluzioni perché abbiamo dei campi.
Per $d = 0$ abbiamo anche solo le soluzioni banali ± 1.
Per $d = 1$ abbiamo le soluzioni non banali $\pm\varepsilon$.
Per $d = 2$ abbiamo le soluzioni non banali $\pm 2\varepsilon$.
Per $d = 4$ abbiamo le soluzioni non banali $\pm 3\varepsilon$.

d. Di ottengono campi per $d = \{3, 5, 6\}$ e questi sono i somorfi perché sono campi finiti con la stessa cardinalità. L'estensione con $d = 0$ non è isomorfa alle altre per il punto b. (è l'unica con un elemento che al quadrato dà 0. Le estensioni con $d = 1, 2, 4$ sono isomorfe tra di loro e gli isomorfismi si ottengono sfruttando il punto c. e in particolare abbiamo che $(a + b\sqrt{1}) \mapsto (a + 2b\sqrt{2})$ è un isomorfismo tra $\mathbb{Z}[\sqrt{1}]$ e $\mathbb{Z}[\sqrt{2}]$ e che $(a + b\sqrt{1}) \mapsto (a + 3b\sqrt{4})$ è un isomorfismo tra $\mathbb{Z}[\sqrt{1}]$ e $\mathbb{Z}[\sqrt{4}]$.

Soluzioni 04 Luglio 2017

Esercizio 1

a. $K[X]/(f)$ non è un dominio in quanto $X^2 \cdot (4X^3 - 3X + 2) = 0$ per cui X^2 è un divisore dello zero (osserviamo che $X^2 \neq 0 \in K[X]/(f)$ perché X^2 non può essere multiplo di f.

b. Abbiamo $(4X^4 - 3X^2 + 2X)^2 = 0$ per cui $4X^4 - 3X^2 + 2X$ è nilpotente.

c. Siccome $P^2 = 0$ abbiamo $(P + 1)(P - 1) = P^2 - 1 = -1$ e quindi l'inverso di $P + 1$ è $-P + 1$ cioè $-4X^5 + 3X^3 - 2X^2 + 1$.

d. Basta considerare ab. Tale elemento non è un multiplo di a^2b, altrimenti avremmo $a^2bx = ab$ da cui, siccome siamo in un dominio e quindi vale la legge di cancellazione, avremmo $ax = 1$ e quindi a sarebbe invertibile. Quindi $ab \neq 0 \in A/(a^2b)$, ma $(ab)^2 = 0$ e quindi ab è nilpotente.

Esercizio 2

a. Su $\mathbb{Q}$ il polinomio f non ha radici. Iniziamo estendendo con una radice di $X^2 - 2$,cioè con $\sqrt{2}$: otteniamo $\mathbb{Q}[\sqrt{2}]$ che è un'estensione di grado 2. Si vede facilmente che in $\mathbb{Q}[\sqrt{2}]$ non ci sono soluzioni di $X^2 - 3$ per cui dobbiamo effettuare un'ulteriore estensione di grado 2. Il campo di spezzamento è quindi $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ che ha grado 4 su $\mathbb{Q}$.

b. Su $\mathbb{R}$ il polinomio si spezza giá e quindi il campo di spezzamento è $\mathbb{R}$ stesso.

c. Su $\mathbb{F}_7 = \mathbb{Z}_7$ abbiamo che $X^2 - 2$ si spezza già, mentre $X^2 - 3$ non ha soluzioni: dobbiamo quindi effettuare un'estensione di grado 2, ottenendo $\mathbb{F}_{49}$.

d. $\mathbb{F}_9$ è un'estensione di grado 2 del campo finito $\mathbb{Z}_3$ e sappiamo quindi dalla teoria che contiene tutte le radici dei polinomi (irriducibili) di grado 2 su $\mathbb{Z}_3$. In particolare contiene sicuramente le radici di $X^2 - 2$ e di $X^2 - 3$ per cui il campo di spezzamento è $\mathbb{F}_9$ stesso.

e. f. Lo stesso argomento del punto d. permette di concludere.

Esercizio 3

a. La riduzione di f in $\mathbb{Z}_2[X]$ è $X^4 + X + 1$ e si verifica facilmente che tale polinomio è irriducibile in $\mathbb{Z}_2[X]$ per cui f è irriducibile in $\mathbb{Q}[X]$ e quindi $\mathbb{Q}[X]/(f)$ è sempre un campo, quali che siano a, b, c (purché tutti dispair!)

b.Viceversa $\mathbb{Z}[X]/(f)$ non è mai un campo: consideriamo infatti l'elemento 2: se fosse invertibile avremmo un polinomio P tale che $2P = 1 \in \mathbb{Z}[X]/(f)$ e quindi $2P = 1 + Qf$. Riducendo questa identità in $\mathbb{Z}_2[X]$ avremmo $Qf = -1$ che è chiaramente assurda visto che f non è di certo invertibile in $\mathbb{Z}_2[X]$.

c. Per il punto a. è sempre invertibile. L'inversa si trova facilmente considerando che $X(aX^3 + b) = -c \in \mathbb{Q}[X]$ e quindi l'inversa di $(aX^3 + b)$ è $-\frac{1}{c}X$.

d. Quanto visto nel punto c. vale anche in questo caso se $c = \pm 1$ e quindi in questo caso il polinomio è invertibile e l'inversa è $-\frac{1}{c}X = -cX$. Se $c \neq \pm 1$ l'esercizio si complica assai.

- Se $aX^3 + b$ è invertibile allora f è primitivo. Infatti, se f non fosse primitivo, sia $d > 1$ un divisore comune di a, b, c; abbiamo che $d \neq 0 \in \mathbb{Z}[X]/(f)$ e che quindi d è un divisore dello 0 in $\mathbb{Z}[X]/(f)$, in quanto $d \cdot \frac{f}{d} = 0$. Ne segue che $aX^3 + b$ è un multiplo di un divisore dello 0 e quindi non può essere invertibile.
- Se $aX^3 + b$ è invertibile allora $c|a$. Sfruttiamo il fatto che se $P \in \mathbb{Z}[X]$ è un qualunque polinomio allora è possibile effettuare la divisione con resto di aP per f

in $\mathbb{Z}[X]$ e quindi abbiamo che aP è congruo modulo f ad un polinomio a coefficienti interi di grado al più 4. Supponiamo ora che aX^3+b sia invertibile in $\mathbb{Z}[X]/(f)$ e sia P un polinomio a coefficienti interi che rappresenta una sua inversa. Allora la classe del polinomio aP si può rappresentare con un polinomio Q di grado al più 3. Abbiamo quindi che $\frac{1}{a}Q$ è l'inverso di aX^3+b in $\mathbb{Q}[X]/(f)$ ed ha grado al più 3 e quindi $\frac{1}{a}Q = -\frac{1}{c}X$ e quindi $Q = -\frac{a}{c}X$. Siccome Q ha coefficienti interi abbiamo che $c|a$

- Infine, se f non è primitivo e a è multiplo di c allora aX^3+b è invertibile. Infatti in tali ipotesi abbiamo che b è primo con c e quindi esistono due interi b' e h tali che $bb'+ch=1$ e un intero k tale che $a=kc$. Abbiamo in questo caso

$$-\frac{1}{c}X+\frac{b'}{c}(kcX^4+bX+c) = -\frac{1}{c}X+kb'X^4+\frac{1}{c}X-hX+b' = kb'X^4-hX+b'$$

e quindi quest'ultimo è l'inverso di aX^3+b in $\mathbb{Z}[X]/(f)$.

Soluzioni 11 Gennaio 2018

Esercizio 1

a. Ricordando che esiste un unico omomorfismo $\mathbb{Z} \to A$ per ogni anello A rimane da individuare le possibili immagini di $\sqrt{2}$. L'immagine di $\sqrt{2}$ deve essere un elemento che al quadrato dà 2 (perché ϕ è un omomorfismo) e quindi le uniche possibilità sono $3, 4$. Abbiamo quindi due possibili omomorfismi

$$\phi_1(a + b\sqrt{2}) = a + 3b$$

$$\phi_2(a + b\sqrt{2}) = a + 4b.$$

È immediato verificare che sono entrambi omomorfismi.

b. Sia $\varphi : \mathbb{Z}[\sqrt{2}][X] \to \mathbb{Z}_7[X]$ l'unico omomorfismo che estende ϕ_1 e tale che $\varphi(X) = X$. Se $X^3 - \sqrt{2}$ è riducibile in $\mathbb{Z}[\sqrt{2}]$ lo sarebbe anche la sua immagine $X^3 - 3 \in \mathbb{Z}_7[X]$: ma questo polinomio è irriducibile non avendo radici. Siccome $\mathbb{Z}[\sqrt{2}]$ è euclideo e quindi a fattorizzazione unica possiamo applicare il lemma di Gauss e concludere che $X^3 - \sqrt{2}$ è irriducibile anche in $(\mathbb{Q}[\sqrt{2}])[X]$.

c. Se α è una radice reale di $X^3 - \sqrt{2}$ abbiamo che $[\mathbb{Q}[\sqrt{2}, \alpha] : \mathbb{Q}[\sqrt{2}]] = 3$ per il punto precedente. Tuttavia questo campo non può contenere tutte le radici di $X^3 - \sqrt{2}$ perché è un campo reale e quindi è necessario effettuare un'altra estensione di grado 2. Il campo di spezzamento ha quindi grado 6.

Esercizio 2

a. Osserviamo che $6 + \varepsilon$ ha norma 0 e quindi A non è un dominio.

b. Gli elementi invertibili sono quelli che hanno norma invertibile: siccome l'anello dei coefficienti è un campo è più semplice calcolare quelli non invertibili, cioè quelli di norma 0. Sia quindi $\alpha = a + b\varepsilon$ tale che $N(\alpha) = 0$; abbiamo

$$N(\alpha) = a^2 - 2b^2 = a^2 - (6b)^2 = (a + 6b)(a - 6b).$$

per cui $N(\alpha) = 0$ se e solo se $a = \pm 6b$: gli elementi che soddisfano questa condizione sono 33 (due scelte per a per ogni valore di $b \neq 0$) e quindi gli invertibili sono $17^2 - 33$.

c. Una classe è formata da 0 e una classe dagli elementi invertibili. Le altre due classi sono date da

$$C_1 = \{a + \varepsilon b : \ a = 6b, \, a \neq 0\}$$

e

$$C_2 = \{a + \varepsilon b : \ a = -6b, \, a \neq 0\}.$$

d. Vediamo i possibili ideali di A.
Osserviamo che un ideale è necessariamente unione di classi di associatura. Se un ideale I contiene un invertibile allora $I = A$ e quindi $A/I = \{0\}$. Se I contiene sia un elemento di C_1 che di C_2 allora sia C_1 che C_2 e quindi un invertibile e quindi ricadiamo nel caso precedente. Le uniche possibilità rimaste sono $C_1 \cup \{0\}$, $C_2 \cup \{0\}$ e $\{0\}$ e questi sono effettivamente ideali. Se $I = C_1 \cup \{0\}$ allora A/I è un campo (perché I è massimale) con 17 elementi...

Esercizio 3

a. Basta mostrare che nessun elemento non nullo ha norma nulla. Se $N(f+\varepsilon g)=0$ con $f,g\in A$ abbiamo $f^2=Xg^2$ non è possibile perché X avrebbe molteplicità pari in f^2 e dispari in Xg^2 (se questi sono nulli).
b. Infatti l'elemento $X-\varepsilon$ ha norma mulla.
c. Per mostare che $A[\sqrt{X^3}]$ è un dominio si procede come nel punto (a). Per mostrare che non è un PID è sufficiente mostrare, ad esempio, che l'ideale $(X,\sqrt{X^3})$ non è principale oppure che $X^3=X\cdot X\cdot X=\varepsilon^2$ ammette due distinte scomposizioni in irriducibili
d. Basta osservare che $A[\sqrt{X}]$ altri non è che l'anello dei polinomi a coefficienti in $\mathbb{Q}$ nella variabile $\sqrt{X}$ e infatti si verifica facilmente che l'applicazione $\varphi : A[\sqrt{X}]\to A$ data da

$$\varphi(a_0+a_1X+\cdots+a_nX^n+\varepsilon(b_0+b_1X+\cdots+b_mX^m)=a_0+a_1X^2+\cdots+a_nX^{2n}+X(b_0+b_1X^2+\cdots+b_mX^{2m}$$

è un isomofismo di anelli.

Soluzioni 06 Febbraio 2018

Esercizio 1

a. Si ha chiaramente che A è il sottospazio dello spazio vettoriale di tutte le matrici 3×3 generato dalle 3 matrici

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Siccome queste 3 matrici sono linearmente indipendenti abbiamo che A è un $\mathbb{Q}$-spazio vettoriale di dimensione 3 e in particolare un gruppo abeliano rispetto alla somma. La matrice identità appartiene ad A e quindi rimane da verificare solo che A è chiuso e commutativo rispetto al prodotto. Si ha

$$\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} \cdot \begin{bmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{bmatrix} = \begin{bmatrix} \tilde{a} & \tilde{b} & \tilde{c} \\ \tilde{c} & \tilde{a} & \tilde{b} \\ \tilde{b} & \tilde{c} & \tilde{a} \end{bmatrix}$$

con $\tilde{a} = a\alpha + b\gamma + c\beta$, $\tilde{b} = a\beta + b\alpha + c\gamma$ e $\tilde{c} = a\gamma + b\beta + c\alpha$ per cui A è chiusio rispetto al prodotto. Osservando la simmetria di $\tilde{a}, \tilde{b}, \tilde{c}$ rispetto alle due terne (a, b, c) e (α, β, γ) abbiamo anche la commutatività del prodotto.

b. Sia I che J sono chiaramente sottospazi vettoriali di A per cui basta verificare la proprietà di "assorbimento" rispetto al prodotto. Per I basta osservare che

$$\tilde{a} + \tilde{b} + \tilde{c} = (a + b + c)(\alpha + \beta + \gamma)$$

per cui se $a+b+c = 0$ allora $\tilde{a}+\tilde{b}+\tilde{c} = 0$. Per J osserviamo invece che se $a = b = c$ allora $\tilde{a} = \tilde{b} = \tilde{c} = a(\alpha + \beta + \gamma)$. Che siano non banali è evidente.

c. Abbiamo

$$\varphi(X) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \ \varphi(X^2) = \varphi(X)^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \ \varphi(X^3) = \varphi(X)^3 = I$$

. Segue che φ è suriettiva e quindi

$$\mathbb{Q}[X]/\ker(\varphi) \cong A;$$

di conseguenza $\ker(\varphi)$ è generato dal un polinomio di grado 3. Ma $X^3-1 \in \ker(\varphi)$ e concludiamo che $\ker(\varphi) = (X^3-1)$. Oppure, avendo osservato che $X^3-1 \in \ker(\varphi)$ abbiamo che il nucleo di φ è necessariamente generato da un divisore di X^3-1, ma nessun divisore proprio di X^3-1 sta nel nucleo...

d. Dall'isomorfismo del punto precedente basta osservare che $\mathbb{Q}[X]/(X^3-1)$ ha esattamente due ideali non banali. Ma gli ideali di questo quoziente sono generati dai divisori non banali di X^3-1 che sono $X-1$ e X^2+X+1 e sono quindi 2.

Esercizio 2

a. Effettuando il raccoglimento parziale per f abbiamo
$$X^5 - 3X^3 - 2X^2 - 1 = X^3(X^2 - 3) - 2(X^2 - 3) = (X^3 - 2)(X^2 - 3)$$
per cui f è riducibile in $\mathbb{Z}_7[X]$. Osserviamo anche che i due fattori $X^2 - 3$ e $X^3 - 3$ sono irriducibili non avendo radici.
b. Se α è una radice di $X^2 - 3$ nel campo di spezzamento abbiamo $\mathbb{Z}_7[\alpha] = \mathbb{F}_{7^2}$ e se β è una radice di $X^3 - 2$ abbiamo $\mathbb{Z}_7[\beta] = \mathbb{F}_{7^3}$. Per l'unicitá dei sottocampi di data cardinalità di un campo finito abbiamo che $\mathbb{Z}_7[\beta]$ contiene tutte le radici di $X^3 - 3$ e quindi il campo di spezzamento sarà il campo finito più piccolo che contiene $\mathbb{F}_{7^2}$ e $\mathbb{F}_{7^3}$, cioè $\mathbb{F}_{7^6}$.
c. Abbiamo in questo caso $\mathbb{F}_{7^{12}}$.
d. In $\mathbb{F}_{7^5}$ non esistono radici di f perché $\mathbb{F}_{7^5}$ non ha sottocampi isomorfi a $\mathbb{F}_{7^2}$ o a $\mathbb{F}_{7^3}$.

Esercizio 3

a. Sappiamo già che $A = \{x + \varepsilon y : , x, y \in \mathbb{Z}_3$ ha $3^2 = 9$ elementi. Per dimostrare che è un campo basta osservare ce 2 non è un quadrato in A.
b. Il gruppo A^* è ciclico di ordine 8 per cui ha $\phi(8) = 4$ generatori. Osservando che $1, -1, \varepsilon e - \varepsilon$ hanno ordine rispettivamente 1,2,4,4 abbiamo che i generatori sono proprio gli altri 4 elementi, cioè $\pm 1 \pm \varepsilon$.
c. $B = \{a + b\eta,\ a, b \in A\}$ dove η soddisfa $\eta^2 = 2$. Tuttavia B non è un campo perché 2 è un quadrato in A: infatti $2 = \varepsilon^2$.
d. Basta mostrare che esiste un omomorfismo suriettivo $\varphi : B \to A$. Un tale omomorfismo è dato da
$$\varphi(a + b\eta) = a + b\varepsilon.$$

Soluzioni 04 Giugno 2018

Esercizio 1

a. A è un sottoinsieme di $\mathbb{Q}(X)$ il campo delle frazioni di $\mathbb{Q}[X]$ per cui è sufficiente verificare le seguenti proprietà:

- $0 = \frac{0}{1} \in A$;
- Se $\frac{g}{h}, \frac{g'}{h'} \in A$ allora $\frac{g}{h} - \frac{g'}{h'} = \frac{gh'-g'h}{hh'} \in A$. Infatti, siccome f è irriducibile, $f \not| hh'$.
- $1 = \frac{1}{1} \in A$;
- Se $\frac{g}{h}, \frac{g'}{h'} \in A$ allora $\frac{g}{h}\frac{g'}{h'} = \frac{gg'}{hh'} \in A$. Infatti, siccome f è irriducibile, $f \not| hh'$.

b. Mostriamo che

$$\mathcal{U}(A) = \{\frac{g}{h} : f \not| g, h\}.$$

Infatti, se $\frac{g}{h} \in \mathcal{U}(A)$ allora esiste $\frac{g'}{h'} \in A$ tale che $\frac{gg'}{hh'} = 1$, cioè $gg' = hh'$. Siccome $f \not| hh'$ allora $f \not| gg'$ e quindi $f \not| g$. Viceversa, se $f \not| g, h$ allora chiaramente $\frac{g}{h}$ è invertibile essendo il suo inverso $\frac{h}{g} \in A$.

c. $I = \{\frac{fg}{h} : f \not| h\}$ è un ideale. I è l'unico massimale perché gli elementi che non stanno in A sono precisamente gli elementi invertibili.

d. In A/I abbiamo $f = 0$ e quindi ... $\frac{g}{h}$ si può scrivere nella forma $aX + b$ e quindi abbiamo un'estensione finita di $\mathbb{Q}$.

Esercizio 2

a. Sia $\gamma = MCD(\alpha, \beta)$. Dalla teoria sappiamo che $I = (\gamma)$. E siccome $\gamma | \alpha, \beta$, dalla moltiplicatività della norma abbiamo $N(\gamma) | N(\alpha), N(\beta)$ e quindi $N(\gamma) | MCD(N(\alpha), N(\beta)) = 10$.

b. Questo accade se solo se γ è invertibile e dobbiamo capire se questo è possibile. Esiste un unico elemento a meno di associati, cioè $1 + i$, di norma 2 e quindi $1 + i$ divide sia α che β. Di conseguenza $1 + i$ divide γ e quindi γ non è invertibile.

c. Dal punto precedente I può essere massimale se e solo se $\gamma = 1 + i$ (sempre a meno di associati). Questo può capitare se $\alpha = (1 + i)(1 + 2i)$ e $\beta = (1 + i)(1 - 2i)$. In questo caso le condizioni sono tutte soddisfatte.

d. Da punti precedenti abbiamo solo 3 possibilità:

- $\gamma = 1 + i$ e in questo caso $\mathbb{Z}[i]/I \cong \mathbb{Z}_2$;
- $\gamma = (1 + i)(1 + 2i)$ (ad esempio se $\alpha = \beta = (1 + i)(1 + 2i)$. In questo caso, usando ad esempio il teorema cinese del resto abbiamo

$$\mathbb{Z}[i]/I \cong \frac{\mathbb{Z}[i]}{(1+i)} \times \frac{\mathbb{Z}[i]}{1+2i} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10}.$$

- $\gamma = (1 + i)(1 - 2i)$ (ad esempio se $\alpha = \beta = (1 + i)(1 - 2i)$). Come nel caso precedente $\mathbb{Z}[i]/I \cong \mathbb{Z}_{10}$.

Esercizio 3

a. Sia $\alpha \in K \setminus \mathbb{Q}$. Allora α è algebrico di grado 2 su $\mathbb{Q}$ e sia quindi f il suo polinomio minimo. Se β è l'altra radice di f abbiamo $\beta \in \mathbb{Q}[\alpha]$ e quindi $K = \mathbb{Q}[\alpha] = \mathbb{Q}[\alpha, \beta]$ è il campo si spezzamento di f su $\mathbb{Q}$.

b. Se $f = a_0 + a_1 X + a_2 X^2 + X^3$ è il polinomio minimo di α abbiamo

$$0 = \varphi(0) = \varphi(a_0 + a_1\alpha + a_2\alpha^2 + \alpha^3) = a_0 + a_1\varphi(\alpha) + a_2\varphi(\alpha)^2 + \varphi(\alpha)^3$$

dove abbiamo usato le proprietà di omomorfismo di φ e il fatto che $\varphi(a) = a$ per ogni $a \in \mathbb{Q}$. Ne segue che $\varphi(\alpha)$ é anche una radice di f.

Siccome K è generato su $\mathbb{Q}$ dalle radici di f concludiamo che $\varphi(K) \subseteq K$.

c. Sia β una radice non reale di $X^3 - 2$. Sappiamo dalla teoria che $\varphi : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\beta]$ dato da

$$\varphi(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2) = a_0 + a_1\beta + a_2\beta^2$$

è un isomorfismo di anelli (campi, in questo caso). Questo φ contraddice il punto (b.) in quanto $\varphi(K) \not\subseteq K$ e quindi K non può essere un campo di spezzamento.

Soluzioni 14 Gennaio 2019

Esercizio 1.

a. Possiamo sempre assumere che l'esponente di 10 al denominatore sia ≥ 0. Abbiamo
   - $1 = \frac{1}{10^0} \in \mathbb{D}$.
   - $\frac{a}{10^n} - \frac{b}{10^m} = \frac{10^m a - 10^n b}{10^{n+m}} \in \mathbb{D}$;
   - $\frac{a}{10^n}\frac{b}{10^m} = \frac{ab}{10^{n+m}}$

   e quindi $\mathbb{D}$ è un sottoanello di $\mathbb{Q}$. La seconda parte segue osservando che un numero reale α ha espressione decimale finita se e solo se esiste $n \geq 0$ tale che $\alpha 10^n \in \mathbb{Z}$.

b. Sia I un ideale di $\mathbb{D}$ e sia a tale che $I \cap \mathbb{Z} = (a)_{\mathbb{Z}} = \{ka : k \in \mathbb{Z}\}$. Mostriamo che $I = \{qa : q \in \mathbb{D}\}$ con la doppia inclusione.
   $\supseteq$: Sia $\frac{b}{10^n} \in I$: allora $b = \frac{b}{10^n}10^n \in I \cap \mathbb{Z}$ e quindi esiste $k \in \mathbb{Z}$ tale che $b = ka$ e quindi $\frac{b}{10^n} = \frac{k}{10^n}a \in \{qa : q \in \mathbb{D}\}$. $\subseteq$: ovvia.

c. Mostriamo che $\mathcal{U}(\mathbb{D}) = \{\frac{2^h 5^k}{10^n} : h, k \geq 0\}$. Infatti $\frac{2^h 5^k}{10^n}\frac{2^k 5^h}{10^{k+h-n}} = 1$ e quindi $\frac{2^h 5^k}{10^n}$ è invertibile. Viceversa, se $\frac{a}{10^n}$ è invertibile allora esistono b e m tali che $ab = 10^{n+m}$ e quindi gli unici divisori primi possibili di a sono 2 e 5.

d. Vediamo la scomposizione in fattori irriducibili. Abbiamo $0.42 = \frac{2}{100} \times 3 \times 7$ e $38500 = 500 \times 7 \times 11$ da cui, osservando che $\frac{2}{100}$ e 500 sono invertibili e che 3, 7 e 11 sono irriducibili e non associati tra loro, il MCD è 7.

Esercizio 2

a. Segue da Eisenstein con $p = 2$.

b. Possiamo effettuare la divisione euclidea di G per F perché F è monico e quindi abbiamo $G = qF + r$ con $\deg r < 4$ e $r \in (F, G)$.

c. F e G sono coprimi in $\mathbb{Q}[X]$ per il lemma di Gauss. Allora esistono $A, B \in \mathbb{Q}[X]$ tali che $AF + BG = 1$. Se n è il mcm di tutti i denominatori che compaiono nei polinomi A e B abbiamo quindi $(nA)F + (nB)G = n \in (F, G)$.

d. Scegliendo $G = X$ abbiamo $I = (F, G) = (2, X)$, l'ideale contenente tutti i polinomi con termine noto pari. I é massimale perché l'unico ideale contenente I e un qualunque polinomio con termine noto dispari è $\mathbb{Z}[X]$.

e. Scegliendo $H = X^2$ abbiamo $J = (X^2, F)$ è un ideale non massimale perché strettamente contenuto in I (ad esempio non può contenere X).

Esercizio 3

a. Se $p|b + 2i$ allora $p|b$ e $p|2$ e queste condizioni sono incompatibili perché b è dispari.

b. Sia $\alpha \in \mathbb{Z}[i]$ irriducibile tale che $\alpha|b + 2i$. Abbiamo
   - $\alpha \neq 1 + i$ perché $b + 2i$ ha norma dispari.
   - $\alpha \neq p$ con $p \equiv 3 \mod 4$ per il punto precedente.
   - se $\alpha = \pi_p, \bar{\pi}_p$ con $p \equiv 1 \mod 4$ mostriamo che α non divide $b - 2i$. Altrimenti $\bar{\alpha}|\overline{b - 2i} = b + 2i$ e quindi $p|b + 2i$ contraddicendo il punto precedente.

   Concludiamo che $b + 2i$ e $b - 2i$ non possono avere fattori irriducibili in comune e quindi $MCD(b + 2i, b - 2i) = 1$.

c. Sia α un fattore irriducibile di $b+2i$. Allora α compare con molteplicità $3k$ in a^3. Siccome $b+2i$ e $b-2i$ sono coprimi abbiamo che α compare con molteplicità $3k$ anche in $b+2i$. Ogni fattore di $b+2i$ compare quindi con molteplicità multipla di 3 e quindi, a meno di associati é un cubo.
d. Gli invertibili di $\mathbb{Z}[i]$ sono ± 1, $\pm i$ e quindi sono dei cubi. Se $b+2i = uz^3$ con u invertibile allora, siccome u è un cubo, abbiamo che anche $b+2i$ è un cubo.

Soluzioni 09 Gennaio 2023

Esercizio 1

(a) Siccome $\deg f$ é dispari esiste una radice $\alpha \in \mathbb{R}$ di f. Il campo $\mathbb{Q}[\alpha]$ é un'estensione di grado 3 ed é contenuta in un campo di spezzamento di f. Siccome tale campo ha anche grado 3 abbiamo che $\mathbb{Q}[\alpha]$ é un campo di spezzamento di f e quindi le radici sono tutte reali. Le radici sono distinte perché f é irriducibile su un campo di caratteristica 0.

(b) La riduzione di f in $\mathbb{Z}_{/2}[X]$ é $X^3 + X^2 + 1$ che é irriducibile (perché non ha radici). f é quindi irriducibile anche su $\mathbb{Q}$.

(c) $\beta \neq \alpha$ perché $\{1, \alpha, \alpha^2\}$ é una base di $\mathbb{Q}[\alpha]$

(d) Con Ruffini otteniamo $f = (X - \alpha)(X^2 + (\alpha - 1)X + \alpha^2 - \alpha - 2)$. Mostriamo quindi $\beta^2 + (\alpha - 1)\beta + \alpha^2 - \alpha - 2 = 0$. Abbiamo $\alpha^3 = \alpha^2 + 2\alpha - 1$ da cui $\alpha^4 = \alpha(\alpha^2 + 2\alpha - 1) = \alpha^3 + 2\alpha^2 - \alpha = 3\alpha^2 + \alpha - 1$ da cui deduciamo

$$\beta^2 = -\alpha + 2$$

e

$$\alpha\beta = \alpha - 1$$

e concludiamo quindi

$$\beta^2 + (\alpha - 1)\beta + \alpha^2 - \alpha - 2 = 0.$$

(e) Siccome $\mathbb{Q}[\alpha]$ contiene le due radici α e β di f necessariamente contiene la terza e quindi $\mathbb{Q}[\alpha]$ é il campo di spezzamento di f.

Esercizio 2 (a) Sia n irriducibile in A. Se n non fosse un numero primo una sua fattorizzazione non banale in $\mathbb{Z}$ sarebbe una fattorizzazione non banale in A. Inoltre, se fosse $n = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$ questa sarebbe anche una fattorizzazione non banale di n in A: entrambi i fattori hanno infatti la stessa norma $\sqrt{n}$ e quindi non sono invertibili

Viceversa, se $n = p$ é un numero primo sia $p = \alpha\beta$ una fattorizzazione in A. Se questa é non banale allora $N(\alpha) = N(\beta) = p$ e quindi, se $\alpha = a + b\sqrt{-2}$ avremmo $p = a^2 + 2b^2$;

(b) abbiamo $p = (a + b\sqrt{-2})(a - b\sqrt{-2}) = (c + d\sqrt{-2})(c - d\sqrt{-2})$. Siccome A é un ED é anche un UFD e quindi queste due fattorizzazioni in irriducibili (tutti i fattori hanno norma p) devono coincidere a meno dell'ordine e di associati. Ma siccome gli elementi invertibili di A sono solo ± 1 abbiamo che $a = \pm c$ e $b = \pm d$: siccome tutti i numeri coinvolti sono positivi il risultato segue.

(c) Basta considerare i numeri primi: $2 = 0^2 + 2 \cdot 1^2$ non é irriducibile, $3 = 1^2 + 2 \cdot 1^2$ nemmeno. 5 e 7 sono invece irriducibili perché non si possono scrivere nella forma $a^2 + 2b^2$.

(d)abbiamo $3 = (1 + \sqrt{-2})(1 - \sqrt{-2}) = 3 | N(\alpha) = \alpha\bar{\alpha}$. Siccome $1 + \sqrt{-2})$ ha norma 3 é irriducibile e quindi primo e quindi é un divisore di α o di $\bar{\alpha}$. Nel primo caso concludiamo, nel secondo deduciamo che $(1 - \sqrt{-2})$ é un divisore di α (osservando che il coniugio é un automorfismo di A.

(e)$\alpha = -11 + 5\varepsilon$ ha norma $9 \cdots 19$. Per il punto precedenti α é divisibile per $1 + \varepsilon$ o per $1 - \varepsilon$, ma non per entrambi, altrimenti i suoi coefficienti sarebbero divisibili per 3. Di

conseguenza é divisibile per $(1+\varepsilon)^2$ o per $(1-\varepsilon)^2$. Vediamo: moltiplichiamo α per l'inverso di $(1+\varepsilon)^2$ (nel campo dei quozienti): abbiamo

$$\alpha(1+\varepsilon)^{-2} = (-11+5\varepsilon)\frac{(1-\varepsilon)^2}{9} = \frac{1}{9}(-11+5\varepsilon)(-1-2\varepsilon) = \frac{1}{9}(31+17\varepsilon) \notin A.$$

evidentemente l'altra possibilitá é quella giusta:

$$\alpha(1-\varepsilon)^{-2} = (-11+5\varepsilon)\frac{(1+\varepsilon)^2}{9} = \frac{1}{9}(-11+5\varepsilon)(-1+2\varepsilon) = \frac{1}{9}(-9-27\varepsilon) = -1-3\varepsilon \in A$$

e quindi abbiamo la fattorizzazione

$$\alpha = (1-\varepsilon)^2(-1-3\varepsilon).$$

Esercizio 3

(a) Un omomorfismo ϕ é tale che $\phi(1) = 1$ e quindi l'unica possibilitá é $\phi([a]_6) = [a]_3$ che chiaramente é ben posta perché $3|6$.

(b) Questi sono infiniti perché $\varphi(X)$ puó essere scelto arbitrariamente

(c) Abbiamo che I é costituito dai polinomi con termine e coefficiente di primo grado multiplo di 3. Di conseguenza ogni classe ha un rappresentante della forma $aX + b$ con $a, b = 0, 1, 2$. D'altra parte, per la descrizione di I abbiamo $[aX + b] = [a'X + b']$ se e solo se $a \equiv a' \mod 3$ e $b \equiv b' \mod 3$ e quindi questi rappresentanti stanno tutti in classi distinte. Di conseguenza abbiamo esattamente 9 elementi in questo quoziente

(d) Non é un dominio perche $[X] \cdot [X] = [0]$ ma $[X] \neq [0]$.

(e) L'unica possibilitá é che $A = \mathbb{Z}_{/6}[X]/I$ sia una estensione quadratica di $\mathbb{Z}_{/3}$ il fatto che $X^2 = 0$ in A ci suggerisce che questa estensione sia $\mathbb{Z}_{/3}[\sqrt{0}]$. Infatti se consideriamo l'omomorfismo

$$\varphi : \mathbb{Z}_{/6}[X] \to \mathbb{Z}_{/3}[\sqrt{0}]$$

dato sulle costanti da $\varphi([a]_6) = [a]_3$ e tale che $\varphi(X) = \varepsilon$ possiamo osservare che questo omomorfismo é suriettivo e che $ker(\varphi) = I$ e il risultato segue dal primo teorema di omomorfismo.

Soluzioni 23 Gennaio 2023

Esercizio 1

(a) Il polinomio f é irriducibile per il criterio di Eisenstein. Le radici sono $\pm\sqrt{1+\sqrt{3}}$ e $\pm i\sqrt{\sqrt{3}-1}$.

(b) Prendiamo $\alpha = \sqrt{1+\sqrt{3}}$ e $\beta = i\sqrt{\sqrt{3}-1}$. Si ha $K_1 \neq K_2$ perché il primo é un campo reale, il secondo no

(c) $K_1 \cap K_2$ é un'estensione di grado al piú 2 di $\mathbb{Q}$ (perché K_1 e K_2 hanno grado 4 e l'intersezione é propria per il punto precedente). Bata quindi mostrare che $\sqrt{3} \in K_1 \cap K_2$. Questo segue dal fatto che $\alpha^2 - 1 = \sqrt{3}$ e $-\beta^2 + 1 = \sqrt{3}$

(d) Dal punto (b) sappiamo che $\mathbb{Q}[\alpha, \beta]$ é un'estensione di grado almeno 2 di K_1. D'altra parte β, per il punto precedente, soddisfa il polinomio

$$X^2 + \sqrt{3} - 1 \in K_1[X]$$

e quindi $\mathbb{Q}[\alpha, \beta]$ é un'estensione di grado 2 di K_1. Il risultato segue dal lemma della torre.

(e)$\mathbb{Q}[\alpha, \beta]$ é un'estensione normale perché é il campo di spezzamento di f (su $\mathbb{Q}$, ma anche su $K_1 \cap K_2$). Il gruppo di Galois ha quindi ordine 4 e siccome abbiamo almeno due campi intermedi K_1 e K_2 il gruppo di Galois ha almeno due sottogruppi proprio e quindi é necessariamente il gruppo di Klein $\mathbb{Z}_{/2} \times \mathbb{Z}_{/2}$.

Esercizio 2

(a) Si ha $\pi_{41} = 4 + 5i$ perché $4^2 + 5^2 = 41$ e $c = -10$.

(b) Basta mostrare che $(5c)^2 \equiv -1 \mod 41$. In alternativa l'unica verifica da fare é la moltiplicativitá

(c) Abbiamo $\varphi(\pi_{41}) = [4 - 5 \cdot 10 \cdot 5]_{41} = [0]_{41}$ per cui $\pi_{41} \in \ker\varphi$. D'altra parte π_{41} é irriducibile e quindi l'ideale (π_{41}) é massimale e quindi $ker(\varphi)$ coincide on (π_{41}) non potendo essere tutto A.

(d)Questo segue direttamente dal primo teorema di omomorfismo: φ é suriettiva perché $\mathbb{Z}_{/41}$ é generato da 1.

(e) Sia $\pi_p = a + ib$, quindi tale che $a^2 + b^2 = p$ e sia c un intero tale che $ac \equiv 1 \mod p$. Osserviamo che $(bc)^2 = p^2c^2 - a^2c^2 \equiv -1 \mod p$ per cui l'omomorfismo $\varphi : A \to \mathbb{Z}_{/p}$ dato da $\varphi(x + iy) = [x + bcy]_p$ é ben definito. Osserviamo che $\pi_p \in \ker\varphi$: infatti

$$\varphi(\pi_p) = a + cb^2$$

che moltiplicata per a dá $a^2 + b^2 \equiv 0 \mod p$. Il risultato segue ancora dal teorema di omomorfismo.

Esercizio 3 (a) bisogna solo mostrare che A é chiuso rispetto al prodotto: questo deriva direttamente dal fatto che $1 + \omega + \omega^2 = 1$ e quindi $\omega^2 = -1 - \omega$;

(b) abbiamo $\overline{\omega} = \omega^2 = -1 - \omega$ e quindi

$$\overline{a + b\omega} = a + b(-1 - \omega) = a - b - b\omega$$

e quindi

$$N(a + b\omega) = (a + b\omega)(\overline{a + b\omega}) = a^2 + b^2 - ab$$

(c) dal punto precedente abbiamo $N(2-5\omega)=39$ per cui se $c\in(2-5\omega)$ esiste $\alpha\in A$ tale che

$$c=(2-5\omega)\alpha$$

e passando alle norme abbiamo

$$c^2=39N(\alpha)$$

dove $N(\alpha)$ é anche un numero intero. Da questo deriva $39|c$;

(d) Dal punto precedente abbiamo che se $c=0\in A/(2-5\omega)$ allora c é un multiplo di 39. D'altra parte $39=0\in A/(2-5\omega)$ per cui la caratteristica di $A/(2-5\omega)$ é proprio 39.

(e) abbiamo $(2-5\omega)|39=3\cdot 13$. Se $2-5\omega$ fosse primo avremmo $(2-5\omega)|3$ oppure $(2-5\omega)|13$, a entrambe le condizioni sono impossibili per la moltiplicativitá delle norma.

Soluzioni 13 Febbraio 2023

Esercizio 1

a. Sia I massimale e $x, y \in A$ tali che $xy \in I$. Allora nel quoziente A/I abbiamo $[x][y] = [0]$ e siccome il quoziente é un campo (e quindi un dominio) abbiamo $[x] = 0$ oppure $[y] = 0$, cioé $x \in I$ oppure $y \in I$.
b. Siano $x, y \in A$ nilpotenti, diciamo $x^n =$ e $y^m = 0$. Allora $(x-y)^{m+n} = 0$ e $(ax)^n = 0$ per ogni $a \in A$. $Nil(A)$ é quindi un ideale.
c. Sia $a \in Nil(A)$ e quindi $a^n = 0$. Per definizione di ideale primo , siccome $a \cdot a^{n-1} = 0 \in I$ abbiamo $a \in I$ oppure $a^{n-1} \in I$. Il risultato segue quindi per induzione.
d. Abbiamo $Nil(\mathbb{Z}_{/6}) = \{[0]_6\}$ e $Nil(\mathbb{Z}_{/8}) = ([2]_8)$.
e. Se $[a] \in Nil(A/Nil(A))$ allora esiste n tale che $[a]^n = [a^n] = [0]$ cioé abbiamo a^n nilpotente. Ma se a^n é nilpotente anche a lo é e quindi $[a] = [0]$.

Esercizio 2

a. L é campo di spezzamento per f sia su $K[\alpha]$ che su $K[\beta]$. Identificando questi ultimi con l'isomorfismo $\phi : K[\alpha] \to K[\beta]$ che fissa gli elementi di K e manda α in β abbiamo, per il teorema di unicitá dei campi di spezzamento, che esiste un isomorfismo $\tau : L \to L$ che ristretto a $K[\alpha]$ sia ϕ.
b. Basterà mostrare che se $h \in Gal(L/K[\alpha])$ allora $\tau h \tau^{-1} \in Gal(L/K[\beta])$ e per questo basta mostrare che $\tau h \tau^{-1}$ fissa β. Infatti:

$$\tau h \tau^{-1}(\beta) = \tau h(\alpha) = \tau(\alpha) = \beta.$$

c. Se G é abeliano allora $Gal(L/K[\alpha]) = Gal(L/K[\beta])$ e quindi, per la corrispondenza di Galois, $K[\alpha] = K[\beta]$.
d. Sostituendo β con una qualunque altra radice di f abbiamo che $K[\alpha]$ contiene tutte le radici di f e quindi $L = K[\alpha]$.
e. Basta scegliere $f = X^3 - 2$ (irriducibile per Eisenstein) con $K = \mathbb{Q}$. Sicuramente $\mathbb{Q}[\sqrt[3]{2}]$ non puó essere il campo di spezzamento perché non contiene le radici non reali di f.

Esercizio 3

a. Ricordando che i numeri costruibili formano un campo chiuso rispetto all'estrazione di radice quadrata abbiamo che $\sin(\alpha) = \pm\sqrt{1-\cos^2\alpha}$ e $\sin\beta$ sono costruibili. Di conseguenza anche $\cos(\alpha+\beta)$ é costruibile.
b. $[\mathbb{Q}[\omega] : \mathbb{Q}] = \phi(9) = 6$ che non é potenza di 2 e quindi ω non é costruibile e di conseguenza neanche la sua parte reale che é $\cos(40°)$.

c. $\cos(30^\circ) = \frac{\sqrt{3}}{2}$ é chiaramente costruibile. Ricordando che il pentagono é costruibile possiamo costruire l'angolo di 72° e quindi, bisecandolo tre volte, otteniamo l'angolo di 9°. In alternativa basta osservare che $\phi(40) = \phi(5)\phi(8) = 16$ é una potenza di 2.
d. Possiamo costruire $\cos(9 + 9)$ e quindi anche $\cos(27)$ e quindi anche $\cos(30 - 27)$
e. Se n é multiplo di 3 possiamo costruire $\cos(n^\circ)$ per i punti $a.$ e $d.$. Supponiamo ora di poter costruire $\cos(n^\circ)$ con n non multiplo di 3. Allora se $n \equiv \pm 1 \mod 3$ possiamo costruire $\cos(\pm 1^\circ) = \cos(1^\circ)$. Ma allora potremmo costruire anche $\cos(40^\circ)$, assurdo.

Soluzioni 12 Luglio 2023

Esercizio 1.

a. Il polinomio minimo di α é X^5-3 (irriducibile per Eisenstein), mentre il polinomio minimo di ε é il quinto polinomio ciclotomico $\phi_5(X) = 1 + X + X^2 + X^3 + X^4$.
b. É chiaro che $\varepsilon^2 \in \mathbb{Q}[\varepsilon]$. Osserviamo inoltre che $\varepsilon = \varepsilon^6 = (\varepsilon^2)^3$ per cui $\varepsilon \in \mathbb{Q}[\varepsilon^2]$.
c. Le radici di $X^5 - 3$ sono $\alpha\varepsilon^i$, $i = 1, \dots, 5$ per cui si verifica direttamente per doppia inclusione che L é il campo di spezzamento di $X^5 - 3$ su $\mathbb{Q}$ per cui é anche un'estensione normale;
d. Siccome σ permuta le radici del polinomio minimo di ε abbiamo che $\sigma(\varepsilon) = \varepsilon^i$ per qualche $i = 1, 2, 3, 4$. L'ipotesi ci fornisce $\varepsilon = \sigma^5(\varepsilon) = \varepsilon^{i^5}$ per cui $i^5 \equiv 1 \mod 5$ da cui si deduce $i = 1$;
e. Sia H un sottogruppo del gruppo di Galois di ordine 5. Necessariamente H é generato da un elemento σ di ordine 5 e il campo L^H é un'estensione di grado 4 di $\mathbb{Q}$. Dal punto precedente abbiamo $\mathbb{Q}[\varepsilon] \subseteq L^H$. Per motivi di gradi abbiamo l'uguaglianza.

Esercizio 2

a. Siano a_1 e a_2 elementi non nulli di A_1 e A_2. Allora
$$(a_1, 0) \cdot (0, a_2) = (0, 0)$$
per cui $A_1 \times A_2$ non é un dominio.
b. Se $(x_1, x_2), (y_1, y_2) \in I_1 \times I_2$ allora
$$(x_1, x_2) - (y_1, y_2) = (x_1 - x_2, y_1 - y_2) \in I_1 \times I_2$$
per cui $I_1 \times I_2$ é un sottogruppo additivo. Inoltre per ogni $(a_1, a_2) \in A_1 \times A_2$ abbiamo $(a_1, a_2) \cdot (x_1, x_2) = (a_1x_1, a_2x_2) \in I_1 \times I_2$.

Esercizio 3