Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 1
13 ottobre 2009

1. Sia $n \in \mathbb{N}$, $n > 1$.
   (a) Si determini l'insieme $\mathbb{Z}/n\mathbb{Z}^*$ degli elementi invertibili dell'anello $\mathbb{Z}/n\mathbb{Z}$.
   (b) Si deduca da (a) che l'anello $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è un numero primo.

2. (a) Si calcoli l'ordine di ogni elemento nel gruppo $\mathbb{Z}/12\mathbb{Z}^*$ e si decida se $(\mathbb{Z}/12\mathbb{Z}^*, \cdot)$ è un gruppo ciclico.
   (b) Si decida se l'anello $\mathbb{Z}/12\,\mathbb{Z}$ possiede divisori di zero.
   (c) Si determinino tutti gli ideali massimali di $\mathbb{Z}$ che contengono $12\,\mathbb{Z}$.

3. Sia $K = \mathbb{Z}/2\mathbb{Z}$. Si consideri l'anello quoziente $F = K[x]/(f)$ per $f = x^2 + x + 1 \in K[x]$.
   (a) Si verifichi che in F si ha $\overline{1} + \overline{1} = \overline{0}$, $\overline{x}^{\,2} = \overline{x} + \overline{1}$ e $\overline{x}^{\,3} = \overline{1}$.
   (b) Si deduca da (a) che F è costituito da 4 elementi.
   (c) Si determini la tavola dell'addizione e della moltiplicazione in F e si verifichi che F è un campo.
   (d) Si decida se l'anello quoziente $K[x]/(g)$ con $g = x^2 + 1$ è un campo.

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 2
21 ottobre 2009

4. (a) Si dimostri che in un dominio R un elemento $0 \neq p \in R$ è irriducibile se (p) è un ideale primo.
   (b) Sia R un dominio e sia $p \in R$ un elemento irriducibile. Si dimostri: $a \in R$ è irriducibile se a è associato a p.
   (c) Si dimostri che un dominio R è un campo se $R[x]$ è un PID.
   (d) Si dia un esempio di un dominio R con un elemento $p \in R$ tale che (p) è un ideale primo ma non massimale.

5. Siano $i = \sqrt{-1} \in \mathbb{C}$ e $R = \mathbb{Z}[i] = \{a + i\,b \,|\, a, b \in \mathbb{Z}\}$ l'insieme dei numeri *interi di Gauss*. Sia inoltre $\delta : R \to \mathbb{N}_0,\ x = a + i\,b \mapsto |\, x \,|^2 = a^2 + b^2$.
   (a) Si verifichi che R è un sottoanello di $\mathbb{C}$.
   (b) Per ogni $z \in \mathbb{C}$ si trovi $q \in \mathbb{Z}[i]$ tale che $|\, z - q \,|^2 \leq \frac{1}{2}$.
   (c) Si dimostri che (R, δ) è un anello euclideo.
   (d) Si determini l'insieme degli elementi invertibili R^*.
   (e) Si dimostri che $2 = (1+i)(1-i)$ è una scomposizione dell'elemento $2 \in R$ in fattori irriducibili.

6. Sia adesso $\tilde{R} = \mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}\,b \,|\, a, b \in \mathbb{Z}\}$. Si verifichi:
   (a) $\tilde{R}$ è un sottoanello di $\mathbb{C}$.
   (b) Gli elementi 2, 3, $1 + i\sqrt{5}$, $1 - i\sqrt{5}$ sono elementi irriducibili di $\tilde{R}$.
   (c) L'anello $\tilde{R}$ non è UFD.
   (d) L'ideale (2) non è un ideale primo di $\tilde{R}$.

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 3
28 ottobre 2008

7. Sia R un dominio. Si dimostrino i seguenti enunciati:
   (a) Il massimo comun divisore e il minimo comune multiplo di $a_1, \dots, a_n \in R$ sono unici a meno di associazione.
   (b) Dato un massimo comun divisore d di $a_1, \dots, a_n \in R$, gli elementi $b_1, \dots, b_n \in R$ sono coprimi se soddisfano $a_i = d \cdot b_i$ per $1 \leq i \leq n$.
   (c) Lemma di Euclide: Sia R un UFD. Dati $x, a, b \in R$, se x divide ab e a, x sono coprimi, allora x divide b.
   (d) Identità di Bézout: Se R è un PID, allora $a, b \in R$ sono coprimi se e solo se esistono $r, s \in R$ tali che $1 = ra + sb$.

8. In $\mathbb{Q}[X]$ si considerino i polinomi

$$f(X) = X^4 - 1 \qquad g(X) = X^3 + X^2 - X - 1$$

   Si determinino
   (a) le scomposizioni di f e g in polinomi irriducibili,
   (b) un elemento generatore per l'ideale (f, g),
   (c) un elemento generatore per l'ideale $(f) \cap (g)$.

9. Si dimostri:
   (a) Il polinomio $f = x^2 + x + 1$ è irriducibile su $\mathbb{Z}/2\mathbb{Z}$ ma non su $\mathbb{Z}/3\mathbb{Z}$.
   (b) Il polinomio $f = 2x + 2$ è irriducibile in $\mathbb{Q}[x]$, ma non in $\mathbb{Z}[x]$.
   (c) Il polinomio $6x^2 + 5x + 1$ è riducibile di grado 2 in $\mathbb{Z}[x]$, pur non avendo zeri in $\mathbb{Z}$.
   (d) $\mathbb{R}[x]/(x^2 + 1)$ è un campo isomorfo a $\mathbb{C}$.

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 4
4 novembre 2009

10. Sia $K = \mathbb{Z}/3\mathbb{Z}$. Si scomponga in polinomi irriducibili il polinomio

$$f = x^4 + 2\,x^2 + 2\,x + 2 \in K[x].$$

11. Si dimostri che i seguenti polinomi sono irriducibili in $\mathbb{Q}[x]$.

    (a) $x^3 + 2x - 1$
    (b) $x^3 - 16$
    (c) $x^4 - 3x^3 - x^2 + 7x + 21$ (per riduzione)
    (d) $x^4 + 4x^3 + 6x^2 + 8x + 7$ (per sostituzione)

12. Si decida se sono veri o falsi i seguenti enunciati.

    (a) $\mathbb{Z}/2\mathbb{Z}[x]\,/(x^4 + x^2 + 1)$ è un campo di 4 elementi.
    (b) $\mathbb{Q} \subset \mathbb{Q}[x]/(2x^5 + 9x^4 + 6x^2 + 3)$ è un'estensione di campi di grado 5.
    (c) $x^{n-1} + x^{n-2} + \ldots + x + 1$, dove n è un numero pari con $n \geq 4$, è irriducibile su $\mathbb{Q}$.
    (d) $\overline{1} + 2\overline{x}$ è un elemento invertibile in $\mathbb{Z}/3\mathbb{Z}[x]/(x^2 + 1)$.
    (e) $x^5 + 2x + 1$ è irriducibile su $\mathbb{Z}/3\mathbb{Z}$.

NOTA: Termina qui la parte sulla quale verterà *l'esame integrativo* (per chi, nel passaggio al nuovo ordinamento, desidera farsi riconoscere i crediti di *Elementi di Algebra* come crediti di *Algebra*).

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 5
12 novembre 2009

13. (a) Si determinino il campo di riducibilità completa F di $x^4 - 5$ su $\mathbb{Q}$ e il grado dell'estensione $[F : \mathbb{Q}]$.

    (b) Siano $a = \sqrt[3]{7}, b = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$. Si calcolino i gradi $[\mathbb{Q}(a) : \mathbb{Q}]$, $[\mathbb{Q}(b) : \mathbb{Q}]$ e $[\mathbb{Q}(a, b) : \mathbb{Q}]$.

14. (a) Data un'estensione $K \subset F$, si verifichi che la chiusura algebrica $\overline{K}$ di K in F è un sottocampo di F.

    (b) Sia $\overline{\mathbb{Q}}$ l'insieme dei numeri algebrici, ovvero la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$. Si dimostri che $\mathbb{Q} \in \overline{\mathbb{Q}}$ è un'estensione algebrica di grado infinito.

    (c) Si dimostri che ogni elemento di $\mathbb{C} \setminus \overline{\mathbb{Q}}$ è trascendente su $\overline{\mathbb{Q}}$.

15. Sia $K \subset F$ un'estensione di campi finita. Si dimostri:

    Se $[F : K] = 2^n$ con $n \in \mathbb{N}$, allora ogni polinomio $f \in K[X]$ di grado $\deg f = 3$ con uno zero in F possiede già uno zero in K.

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 6
18 novembre 2009

16. Sia $F \subset \mathbb{C}$ il campo di riducibilità completa di $f(X) = X^3 - 3X - 1$ su $\mathbb{Q}$.
    (a) Si verifichi: se $\alpha \in \mathbb{C}$ è uno zero di f, anche $\frac{-1}{\alpha+1}$ è uno zero di f.
    (b) Si dimostri che $F = \mathbb{Q}(\alpha)$, dove α è uno zero di f in $\mathbb{C}$.
    (c) Si calcoli $[F : \mathbb{Q}]$.

17. (a) Sia $z = e^{\frac{2i\pi}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$. Si dimostri che $\mathbb{Q} \subset \mathbb{Q}(z)$ è un'estensione normale.
    (b) Sia $K \subset F$ un'estensione normale e sia $K \subset L \subset F$ un campo intermedio. Si dimostri che $L \subset F$ è normale. Anche $K \subset L$ è sempre normale?
    (c) Sia $f \in \mathbb{Q}[x]$ un polinomio irriducibile di grado 3 che possiede un unico zero reale. Sia L il campo di riducibilità completa di f su $\mathbb{Q}$. Si determini $[L : \mathbb{Q}]$.

18. Siano p, q due numeri primi, sia $\alpha = \sqrt{p} + \sqrt{q}$, e sia $f = x^4 - 2(p+q)x^2 + (p-q)^2$.
    Si verifichi:
    (a) $f(\alpha) = 0$
    (b) $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\alpha)$ è un'estensione propria di campi.
    (c) $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 4$ e f è il polinomio minimo di α su $\mathbb{Q}$.

    e si determini il polinomio minimo di α su $\mathbb{Q}(\sqrt{p})$.

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 7
25 novembre 2009

19. Nel gruppo delle permutazioni S_n, indichiamo con A_n il sottogruppo delle permutazioni pari, detto *gruppo alterno*. Si noti che A_n è un sottogruppo normale di S_n (un sottogruppo H di un gruppo G è detto *normale* se per $x \in G$ e $y \in H$ si ha sempre $xyx^{-1} \in H$).

    (a) Siano $r, n \in \mathbb{N}$ e sia $\pi = (x_1, \ldots, x_r)$ un ciclo in S_n.
    Si verifichi che per ogni permutazione $\sigma \in S_n$ si ha
    $$\sigma \circ \pi \circ \sigma^{-1} = (\sigma(x_1), \ldots, \sigma(x_r))$$

    (b) Si verifichi che l'insieme
    $$\mathcal{V} = \{\mathrm{id},\ (12)(34),\ (13)(24),\ (14)(23)\} \subset S_4$$
    è un sottogruppo abeliano di A_4, detto *gruppo di Klein*.

    (c) Si usi (a) per dimostrare che il gruppo di Klein è un sottogruppo normale di A_4.

20. Siano p e q due numeri primi distinti e $\alpha = \sqrt{p} + \sqrt{q}$. Si dimostri:

    (a) $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

    (b) $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ è una base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$.

    (c) $\mathrm{Aut}F = \{\mathrm{id}, \varphi_1, \varphi_2, \varphi_3\}$ con ${\varphi_i}^2 = \mathrm{id}$ per ogni $i = 1, 2, 3$
    (quindi $\mathrm{Aut}F$ è isomorfo al gruppo di Klein).

21. (a) Sia $K \subset F$ un'estensione separabile, e sia $K \subset L \subset F$ un campo intermedio. Si dimostri che $K \subset L$ e $L \subset F$ sono separabili.

    (b) Si dimostri: Se $f_1, \ldots, f_n \in K[x]$ sono polinomi non costanti su un campo K, allora $f = f_1 \cdot \ldots \cdot f_n$ è separabile se e solo se lo sono tutti gli f_i.

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 8
2 dicembre 2009

22. Si decida se i seguenti enunciati sono veri o falsi (motivando la risposta):
    (a) Se K un campo di caratteristica $\neq 2$, allora ogni estensione $K \subset F$ di grado 2 è un'estensione di Galois.
    (b) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{4})$ è un'estensione di Galois.
    (c) Se $F = \mathbb{Q}(i, \sqrt{7})$, allora $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{7}))$ è sottogruppo normale di $\mathrm{Gal}(F/\mathbb{Q})$.

23. Sia $F = \mathbb{Q}(i, \sqrt[4]{2})$.
    (a) Si determinino gli elementi di $H = \mathrm{Gal}(F/\mathbb{Q}(\sqrt[4]{2}))$.
    (b) Si determinino gli elementi di $H' = \mathrm{Gal}(F/\mathbb{Q}(i))$ e si verifichi che $H' \cong \mathbb{Z}/4\mathbb{Z}$.
    (c) Si decida se $G = \mathrm{Gal}(F/\mathbb{Q})$ è un gruppo abeliano.
    (d) Si calcoli il polinomio minimo di $\alpha = i + \sqrt[4]{2}$ su $\mathbb{Q}(\sqrt[4]{2})$.

24. Sia $K \subset F$ un'estensione di Galois con gruppo di Galois $G = \mathrm{Gal}(F/K) = \{\varphi_1, \ldots, \varphi_n\}$. Siano inoltre $\alpha \in F$ e $f \in K[x]$ il polinomio minimo di α su K.

    Si dimostri

$$(x - \varphi_1(\alpha)) \cdot \ldots \cdot (x - \varphi_n(\alpha)) = f^t \quad \text{dove} \quad t = [F : K(\alpha)]$$

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 9
9 dicembre 2009

25. Siano p, q due primi distinti. Si verifichi che $x^2 - (p + q + 2\sqrt{pq})$ è il polinomio minimo di $\alpha = \sqrt{p} + \sqrt{q}$ su $L_3 = \mathbb{Q}(\sqrt{pq})$.

26. Si decida se i seguenti enunciati sono veri o falsi:
    (a) $E_7(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/7\mathbb{Z}$.
    (b) Il campo di riducibilità completa di $x^3 + x^2 + x + 1$ su $\mathbb{Z}/3\mathbb{Z}$ è isomorfo a $GF(27)$.
    (c) $\mathbb{Z}/3\mathbb{Z}[x]/(x^2 + x + 2) \cong \mathbb{Z}/3\mathbb{Z}[x]/(x^2 + 1)$.

27. (a) Si calcolino le radici ottave dell'unità $z_0, z_1, \ldots, z_7 \in \mathbb{C}$ e si trovi un elemento primitivo di $\mathbb{Q} \subset \mathbb{Q}_8$ (dove $\mathbb{Q}_8$ è il campo di riducibilità completa di $x^8 - 1$ su $\mathbb{Q}$).
    (b) Si determini a meno di isomorfismo il campo di riducibilità completa $(\mathbb{Z}/2\mathbb{Z})_5$ di $x^5 - 1$ su $\mathbb{Z}/2\mathbb{Z}$.

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 10
16 dicembre 2009

28. Sia K un campo infinito e sia $K \subset L$ un'estensione finita e separabile. Si dimostri il *Teorema dell'elemento primitivo* verificando i seguenti enunciati:

    (a) Esistono elementi $\alpha_1, \ldots, \alpha_n \in L$ separabili su K tali che $L = K(\alpha_1, \ldots, \alpha_n)$.

    (b) Per ogni $1 \leq i \leq n$ consideriamo il polinomio minimo f_i di α_i su K. Allora $K \subset L \subset F$, dove F è il campo di riducibilità completa di $f = f_1 \ldots f_n$ su K.

    (c) Esiste solo un numero finito di campi intermedi $K \subset L' \subset L$.

    (d) Se $n = 2$, ovvero $L = K(\alpha_1, \alpha_2)$, allora $K \subset L$ possiede un elemento primitivo di forma $\alpha_1 + k\alpha_2$ con $0 \neq k \in K$.

    (e) $K \subset L$ possiede un elemento primitivo.

29. Sia F il campo di riducibilità completa del polinomio $f = x^3 - 7$ su $\mathbb{Q}$.

    (a) Si dimostri che $G = \mathrm{Gal}(F/\mathbb{Q}) \cong S_3$.

    (b) Si determinino un elemento primitivo α di $\mathbb{Q} \subset F$ e il suo polinomio minimo su $\mathbb{Q}$.

    (c) Si determini il gruppo di Galois $H = \mathrm{Gal}(F/\mathbb{Q}_3)$, dove $\mathbb{Q}_3$ è il campo di riducibilità completa del polinomio $g = x^3 - 1$ su $\mathbb{Q}$. È un sottogruppo normale di G?

30. Siano $K = \mathbb{Z}/5\mathbb{Z}$ e $f = x^4 - 2 \in K[x]$.

    (a) Si verifichi che K contiene tutte le radici quarte dell'unità.

    (b) Si verifichi che f è irriducibile su K.

    (c) Si determini a meno di isomorfismo il gruppo di Galois $\mathrm{Gal}(f/K)$.

Buone vacanze e auguri per il 2010!

Prof. Lidia Angeleri
Università di Verona, 2009/2010
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 11
13 gennaio 2010

Questo foglio è dedicato alle *formule di Cardano-Tartaglia-Del Ferro* per la risoluzione di un'equazione cubica. Su un campo K di caratteristica zero che contenga una radice primitiva terza dell'unità $z \in E_3(K)$, consideriamo il polinomio

$$f = x^3 + px + q \in K[x].$$

Siano E un campo di riducibilità completa di f su K e $\alpha_1, \alpha_2, \alpha_3 \in E$ gli zeri di f.
Siano inoltre

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in E$$

e

$$\Delta = \delta^2 = -4p^3 - 27q^2 \in K$$

il discriminante di f. Si verifichi:

31. (a) Le funzioni elementari simmetriche $\tilde{s_1}, \tilde{s_2}, \tilde{s_3}$ nelle variabili $\alpha_1, \alpha_2, \alpha_3$ soddisfano
$\tilde{s_1} = \alpha_1 + \alpha_2 + \alpha_3 = 0$
$\tilde{s_2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$
$\tilde{s_3} = \alpha_1\alpha_2\alpha_3 = -q$
(b) $\delta = {\alpha_1}^2\alpha_2 + {\alpha_2}^2\alpha_3 + {\alpha_3}^2\alpha_1 - {\alpha_1}^2\alpha_3 - {\alpha_2}^2\alpha_1 - {\alpha_3}^2\alpha_2$
(c) $3(z-z^2)\delta - 3\sum_{i\neq j} {\alpha_i}^2\alpha_j = 6z({\alpha_1}^2\alpha_2 + {\alpha_2}^2\alpha_3 + {\alpha_3}^2\alpha_1) + 6z^2({\alpha_1}^2\alpha_3 + {\alpha_2}^2\alpha_1 + {\alpha_3}^2\alpha_2)$

32. Consideriamo gli elementi

$$\alpha = \alpha_1 + z\alpha_2 + z^2\alpha_3, \quad \beta = \alpha_1 + z^2\alpha_2 + z\alpha_3 \in E.$$

(a) $2\alpha^3 + 27q = 3(z - z^2)\delta, \quad 2\beta^3 + 27q = -3(z - z^2)\delta$ e $\alpha\beta = -3p.$
(b) Gli elementi $a = \frac{\alpha^3}{27}$, $b = \frac{\beta^3}{27}$ appartengono a $K(\delta)$ e sono gli zeri del polinomio

$$g = x^2 + qx - (\tfrac{p}{3})^3 \in K[x].$$

(c) Esistono $u, v \in E$ tali che l'elemento u è una radice terza di $a \in K(\delta)$, l'elemento v una radice terza di $b \in K(\delta)$ e $3uv = -p$. In tal caso $u + v$ è uno zero di f e

$$\{\alpha_1, \alpha_2, \alpha_3\} = \{u + v,\ z^2u + zv,\ zu + z^2v\}$$

33. (a) Un polinomio $f \in \mathbb{R}[x]$ ha tre zeri distinti in $\mathbb{R}$ se $\Delta > 0$, al più due zeri distinti in $\mathbb{R}$ se $\Delta = 0$, uno zero in $\mathbb{R}$ e due zeri coniugati in $\mathbb{C} \setminus \mathbb{R}$ se $\Delta < 0$.
(b) Si trovino gli zeri del polinomio $x^3 - 2x + 4 \in \mathbb{Q}[x]$ e si determini $\mathrm{Gal}(f/\mathbb{Q})$.