Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 1
14 ottobre 2008

1. Si verifichi che l'insieme End$G$ di tutti gli endomorfismi di un gruppo abeliano G forma un anello rispetto alla somma e alla composizione di applicazioni.

2. Sia I un insieme e sia R un anello.

   (a) Dato un sottoinsieme $N \subseteq I$, si verifichi che

   $$\mathcal{A}(N) = \{f \in R^I \mid f|_N = 0\}$$

   è un ideale dell'anello R^I.

   (b) Sia adesso R un campo e sia $x \in I$. Si dimostri che

   $$\mathcal{A}(x) = \{f \in R^I \mid f(x) = 0\}$$

   è un ideale massimale dell'anello R^I.

3. Sia $n \in \mathbb{N}$, $n > 1$.

   (a) Si determinino gli elementi di $\mathbb{Z}/n\mathbb{Z}^*$.

   (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.

4. Sia $(G, \cdot)$ un gruppo abeliano, e siano $a, b \in G$. Sia inoltre $n = mcm(\text{ord}(a), \text{ord}(b))$ il minimo comune multiplo dell'ordine di a e di b. Si dimostri che esiste un elemento $c \in G$ con $ord(c) = n$.

Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 2
5 novembre 2008

5. Sia K un campo e sia $R = K^{\mathbb{N}_0}$ l'anello delle successioni di elementi di K con l'addizione

$$(a_n) + (b_n) = (a_n + b_n)$$

e la moltiplicazione

$$(a_n) \cdot (b_n) = (a_n \cdot b_n)$$

Si dimostri:

(a) Il polinomio $f = X^2 - X \in R[X]$ ha un numero infinito di zeri in R.

(b) Le successioni (a_n) con $a_n = 0$ per quasi tutti gli n formano un ideale di R, e questo ideale non è principale.

6. Sia R un dominio e siano $a_1, \ldots, a_n \in R$.

(a) Si dimostri che il massimo comun divisore e il minimo comune multiplo di $a_1, \ldots, a_n$ sono unici a meno di associazione.

(b) Dato un massimo comun divisore d di $a_1, \ldots, a_n$, siano $b_1, \ldots, b_n \in R$ tali che $a_i = d \cdot b_i$ per $1 \leq i \leq n$. Si verifichi che $b_1, \ldots, b_n$ sono coprimi.

(c) Sia R un PID. Si trovi un elemento generatore per l'ideale $(a_1, \ldots, a_n)$.

7. Si dimostrino i seguenti enunciati:

(a) 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.

(b) 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. (a) Dato un anello R, si dimostri: Se $R[x]$ è un PID, allora R è un campo.

(b) In $\mathbb{Z}[x]$ si trovino due polinomi coprimi f, g tali che $1 \notin (f, g)$.

Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 3
12 novembre 2008

9. 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) un elemento generatore per l'ideale (f, g),
(b) un elemento generatore per l'ideale $(f) \cap (g)$.

10. Sia $K = \mathbb{Z}/3\mathbb{Z}$. Si scomponga il polinomio $f = x^4 + 2\,x^2 + 2\,x + 2 \in K[x]$ in polinomi irriducibili.

11. 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.

12. 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 $R = \mathbb{Z}[i]$.
(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, 2008/2009
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 4
19 novembre 2008

13. Si consideri l'anello quoziente $F = K[x]/(f)$ per $K = \mathbb{Z}/3\mathbb{Z}$ e $f = x^2 + 1 \in K[x]$.
    (a) Si elenchino gli elementi di F.
    (b) Si calcolino i prodotti $(\overline{1} + \overline{x}) \cdot (\overline{2} + \overline{x})$ e $(\overline{1} + \overline{x})^2$.
    (c) Si determini l'elemento inverso di $(\overline{1} + \overline{2x})$.

14. Si decida se i seguenti polinomi sono irriducibili in $\mathbb{Q}[x]$.
    (a) $2x^5 + 9x^4 + 6x^2 + 3$
    (b) $x^4 - 3x^3 - x^2 + 7x + 21$
    (c) $x^{n-1} + x^{n-2} + \ldots + x + 1$ dove n è un numero pari con $n \geq 4$
    (d) $x^3 + 2x - 1$
    (e) $x^4 + 4x^3 + 6x^2 + 8x + 7$ (sostituendo x con $x - 1$)
    (f) $x^5 + 8x + 16$ (attraverso riduzione modulo 3)

15. Sia $a = \sqrt{2} + i \in \mathbb{C}$, e sia $f = x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$. Si verifichi:
    (a) $f(a) = 0$
    (b) $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[a]$ è un'estensione propria di campi.
    (c) $[\mathbb{Q}[a] : \mathbb{Q}] = 4$ e f è il polinomio minimo di a su $\mathbb{Q}$.
    (d) Si determini il polinomio minimo di a su $\mathbb{Q}[\sqrt{2}]$.

16. Dati $n \geq 2$ numeri primi distinti $p_1, \ldots, p_n$, si dimostri che $\sqrt[n]{p_1, \ldots, p_n}$ è irrazionale.

Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 5
26 novembre 2008

17. Si determinino il campo di riducibilità completa F di x^4-2 su $\mathbb{Q}$ e il grado dell'estensione $[F:\mathbb{Q}]$.

18. (a) Si verifichi che i sottocampi $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{2})$ di $\mathbb{C}$ sono isomorfi come spazi vettoriali su $\mathbb{Q}$, ma non come campi.
    (b) Sia $\bar{\mathbb{Q}}$ l'insieme dei numeri algebrici, ovvero la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$. Si dimostri che ogni elemento di $\mathbb{C} \setminus \bar{\mathbb{Q}}$ è trascendente su $\bar{\mathbb{Q}}$.

19. Sia $K \subset F$ un'estensione di campi finita. Si dimostri:
    (a) Se $[F:K]$ è un numero primo, allora $K \subset F$ è un'estensione semplice, cioè non esistono campi intermedi propri $K \subset L \subset F$ con $K \neq L$ e $L \neq F$.
    (b) 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.

20. Siano p e q due numeri primi distinti e $\alpha = \sqrt{p} + \sqrt{q}$. Si determini il polinomio minimo di α su $\mathbb{Q}$ (procedendo come nell'Esercizio 15).

Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 6
3 dicembre 2008

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.

22. (a) Quali delle seguenti estensioni sono normali?
    - $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$
    - $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$
    - $\mathbb{Q} \subset \mathbb{Q}(z)$, dove $z = e^{\frac{2i\pi}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

    (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 e si decida se anche $K \subset L$ è sempre normale.

23. (a) Siano $r, n \in \mathbb{N}$ e sia $\pi = (x_1, \ldots, x_r)$ un ciclo nel gruppo delle permutazioni 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 del gruppo alterno A_4, detto *gruppo di Klein*.
    (c) Si usi (a) per dimostrare che il gruppo di Klein è un sottogruppo normale di A_4.

24. 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).
    (d) $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ è un'estensione di Galois.

Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di Algebra

Foglio 7
10 dicembre 2008

25. Sia K un campo di caratteristica $\neq 2$. Si dimostri che ogni estensione di campi $K \subset F$ di grado 2 è un'estensione di Galois.

26. Sia G un gruppo risolubile. Si dimostri che sono risolubili anche ogni sottogruppo $H \leq G$ e ogni gruppo quoziente G/N (dove N è un sottogruppo normale).

27. Si determini (a meno di isomorfismo) il campo di riducibilitá completa dei polinomi

    (a) $x^4 + x + 1$ su $K = \mathbb{Z}/2\mathbb{Z}$.
    (b) $x^3 + x^2 + x + 1$ su $K = \mathbb{Z}/3\mathbb{Z}$.
    (c) $x^4 + 2\,x^2 + 2\,x + 2$ su $K = \mathbb{Z}/3\mathbb{Z}$.

28. Sia F un campo di p^n elementi con un numero primo p e un numero naturale $n \in \mathbb{N}$. Si dimostri:

    (a) Se L è sottocampo di F, allora $\mid L \mid = p^m$ dove m è un divisore di n.
    (b) Per ogni divisore positivo m di n esiste uno e un solo sottocampo

    $$L = \{x \in F \mid x^{p^m} = x\}$$

    di F di p^m elementi.