Corso di Laurea in Matematica A.A. 2024-2025
Docente: Stefano Bonzio

Esercizi sulla teoria degli anelli

1. Sia $\mathbb{H}$ l'insieme dei quaternioni, ovvero $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$. Si ricordi che, dato $q \in \mathbb{H}$, $q = a + bi + cj + dk$, $\overline{q} = a - bi - cj - dk$ e che $\|q\| = \sqrt{q\overline{q}}$.

   a) si provino le seguenti uguaglianze: $\overline{\overline{q}} = q$, $\overline{q + q_1} = \overline{q} + \overline{q_1}$, $\overline{q \cdot q_1} = \overline{q_1} \cdot \overline{q}$, $q\overline{q} = a^2 + b^2 + c^2 + d^2$, $\|q \cdot q_1\| = \|q\| \cdot \|q_1\|$.

   b) si verifichi che $\mathbb{H}$ forma un corpo (dove per $q \neq 0$, $q^{-1} = \|q\|^{-2} \cdot \overline{q}$).

2. Sul gruppo abeliano $A = (\mathbb{R}, +) \times (\mathbb{R}, +)$ si consideri la moltiplicazione definita da

$$(x, y) \cdot (x', y') = (xx' + yy', xy' + x'y).$$

   (a) Dimostrare che in questo modo $(A, +, \cdot)$ risulta un anello unitario e $\mathbb{R} \times \{0\}$ è un suo sottoanello.

   (b) Caratterizzare gli elementi invertibili ed i divisori dello zero di A.

   (c) Dire se esistono elementi che non sono né divisori dello zero né invertibili.

   (d) Trovare gli ideali massimali di A.

3. Sia A un anello commutativo unitario e I e J ideali di A. Definiamo

$$IJ = \{i_1 j_1 + \cdots + i_n j_n \mid n \in \mathbb{N},\ i_k \in I, j_k \in J,\ k = 1, \ldots, n\}.$$

   (a) Provare che IJ è un ideale di A contenuto nell'ideale $I \cap J$ e mostrare con un esempio che $IJ \neq I \cap J$.

   (b) Provare che se $A = I + J$ allora $IJ = I \cap J$.

   (c) Provare che l'affermazione in (b) non è vera se A non è un anello unitario.

   (d) se I e J sono due ideali massimali distinti, allora $IJ = I \cap J$;

   (e) se I e J sono ideali principali, $I = (a)$ e $J = (b)$, allora $IJ = (ab)$.

   (f) descrivere IJ e $I \cap J$ in $A = \mathbb{Z}$ e dedurre quando $IJ = I \cap J$.

4. Sia $A = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_3\}$. Provare che A è un sottocampo di $M_2(\mathbb{Z}_3)$. Dimostrare inoltre che $(A^*, \cdot)$ è un gruppo ciclico, determinare l'ordine di A^* e un suo generatore.

5. Sia $A = \{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$. Provare che A è un sottocampo di $M_2(\mathbb{R})$ isomorfo a $\mathbb{C}$.

6. Sia A un anello unitario e I un ideale bilatero di A. Dimostrare che l'insieme $U_I = \{x \in U(A) \mid x - 1 \in I\}$ è un sottogruppo normale di $U(A)$.

7. Sia $A = \{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$.

   (a) Provare che A è un anello commutativo unitario, ma non è un dominio.

   (b) Determinare l'ideale $N(A)$ degli elementi nilpotenti di A.

   (c) Mostrare che ogni ideale proprio di A è contenuto in $N(A)$ e dedurre che A è un anello locale.

   (d) Determinare tutti gli ideali di A.

8. Nell'anello $M_2(\mathbb{Z}_8)$, sia $A = \{ \begin{pmatrix} a & 5b \\ 4b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_8\}$.

   (a) Provare che A è un sottoanello commutativo di $M_2(\mathbb{Z}_8)$.

   (b) Dire se A è un dominio.

9. Sia p un primo e $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} \mid p \nmid n,\ (m, n) = 1\}$.

   (a) Provare che $\mathbb{Z}_{(p)}$ è un sottoanello di $\mathbb{Q}$.

   (b) Determinare gli elementi invertibili di $\mathbb{Z}_{(p)}$.

   (c) Determinare gli ideali di $\mathbb{Z}_{(p)}$.

   (d) Determinare gli ideali primi e massimali di $\mathbb{Z}_{(p)}$.

   (e) Provare che $\mathbb{Z}_{(p)}$ è un anello locale.

10. Dimostrare che:

    (a) ogni campo è un anello locale senza elementi nilpotenti non nulli;

    (b) se $\mathbb{Z}_m$ è locale e non ha elementi nilpotenti non nulli allora $\mathbb{Z}_m$ è un campo;

    (c) dare un esempio di anello locale senza elementi nilpotenti non nulli che non sia un campo.

11. Un anello commutativo unitario si dice *regolare* se per ogni $x \in A$ esiste $y \in A$ tale che $x = yx^2$. Dimostrare che:

    (a) ogni campo è un anello regolare e se A è un dominio regolare allora A è un campo;

(b) l'anello quoziente di un anello regolare è regolare;

(c) in un anello regolare ogni ideale primo e massimale;

(d) in un anello regolare ogni ideale principale è generato da un idempotente;

(e) se I e J sono due ideali di un anello regolare allora $IJ = I \cap J$;

(f) per ogni insieme non vuoto S e per ogni campo K, l'anello K^S è regolare.

12. Sia G un gruppo abeliano ed $\mathrm{End}(G)$ l'insieme degli endomorfismi di G. Siano $f, g \in \mathrm{End}(G)$ e si definisca $(f+g)(x) = f(x) + g(x)$, per $x \in G$. Sia $\circ$ l'usuale composizione di funzioni, cioèè $(f \circ g)(x) = f(g(x))$ per $x \in G$.

    (a) Si dimostri che $(\mathrm{End}(G), +, \circ)$ è un anello unitario.

    (b) Sia A un anello unitario. Si dimostri che A si può identificare con un sottoanello di $\mathrm{End}(G)$ per qualche gruppo abeliano G.

13. Sia G un gruppo abeliano e $f \in A = \mathrm{End}(G)$.

    (a) Dimostrare che se f è suriettivo, allora f non è divisore destro dello zero in A.

    (b) Dimostrare che se f è iniettivo, allora f non è divisore sinistro dello zero in A.

    (c) Trovare un anello dove esistono divisori sinistri dello zero che non sono divisori destri dello zero (suggerimento: considerare l'anello $\mathrm{End}(\mathbb{Z}^{\mathbb{N}})$).

14. Sia $A = \{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}\}$.

    (a) Dimostrare che A è un sottoanello di $M_2(\mathbb{C})$.

    (b) Sia $q = a + bi + cj + dk$ un elemento del corpo dei quaternioni $\mathbb{H}$. Si dimostri che l'applicazione $\varphi : \mathbb{H} \to A$ definita da

    $$\varphi(q) = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \ \alpha = a + ib, \ \beta = c + id \in \mathbb{C}$$

    è un isomorfismo di anelli e pertanto di corpi.

    (c) Si verifichi che

    $$\det(\varphi(q)) = \|q\|^2 = a^2 + b^2 + c^2 + d^2.$$

    Si deduca che $\|q_1 q_2\| = \|q_1\|\|q_2\|$, per ogni $q_1, q_2 \in \mathbb{H}$.

    (d) Si verifichi che l'insieme dei quaternioni di norma 1 è un sottogruppo del gruppo moltiplicativo $(\mathbb{H}^*, \cdot)$.

15. Determinare l'insieme degli endomorfismi unitari dei seguenti anelli: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{n}]$.

16. Sia $f : A_1 \to A_2$ un omomorfismo di anelli unitari.

    (a) Provare che $f(U(A_1)) \subseteq U(A_2)$.

    (b) Considerando l'omomorfismo canonico $f : \mathbb{Z} \to \mathbb{Z}_n$, mostrare che in (a) non vale l'uguaglianza se $n > 6$.

17. Sia A l'anello $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$

    (a) Trovare la caratteristica di A.

    (b) Descrivere gli ideali (primi, massimali e principali) di A.

    (c) Determinare a quale degli anelli $\mathbb{Z}_4 \times \mathbb{Z}_{15}$, $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ e $\mathbb{Z}_{60}$ è isomorfo l'anello A.

    (d) Descrivere quali sono gli elementi invertibili e gli elementi nilpotenti di A.

18. Sia $\mathbb{K}$ un campo e $A = \mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}$ (n fattori). Trovare gli ideali primi e massimali di A e dire quanti sono.

19. Nell'anello $A = \mathbb{Z}[\sqrt{2}]$ si considerino gli ideali $I = (2)$ e $J = (3)$. Dire se gli anelli quoziente A/I e A/J sono campi.

20. Nell'anello $A = \mathbb{Z}[\sqrt{5}]$ sia $I = (5)$ e si consideri l'anello quoziente A/I.

    (a) Provare che se $a \equiv 0 \mod 5$, allora l'elemento $a + b\sqrt{5} + I$ èè nilpotente.

    (b) Provare che se $a \not\equiv 0 \mod 5$, allora l'elemento $a + b\sqrt{5} + I$ èè invertibile.

    (c) Determinare gli ideali di A/I.

21. Sia $A = \mathbb{Z}[\sqrt{5}]$. Per $\alpha = x + \sqrt{5}y \in A$ definiamo la norma di α come $N(\alpha) = x^2 - 5y^2$. Dimostrare che $M = \{\alpha \in A \mid N(\alpha) \text{ pari}\}$ è un ideale massimale di A.

Esercizi sui reticoli

1. Dimostrare che se un elemento di un reticolo distributivo e limitato ammette complemento, tale complemento è unico e che se $a \wedge b = 0$ e $a \vee b = 1$ allora $b = \overline{a}$.

2. Dimostrare che in ogni algebra di Boole B vale che $\overline{\overline{x}} = x$ e valgono le leggi di De Morgan, ovvero: $\overline{x \wedge y} = \overline{x} \vee \overline{y}$ e $\overline{x \vee y} = \overline{x} \wedge \overline{y}$, per ogni $x, y \in B$.

3. Dimostrare che l'insieme degli ideali di un reticolo limitato L forma un reticolo completo (suggerimento: mostrare che l'insieme è chiuso per intersezioni arbitrarie).

4. Un anello commutativo unitario A si dice *Booleano*, se, per ogni $a \in A$, vale $a^2 = a$.

   (a) Provare che la caratteristica di A è 2 e che A è un anello commutativo;

   (b) Provare che A ha divisori dello zero qualora $|A| > 2$;

   (c) Ogni ideale primo di A è massimale.

5. Sia $(B, \vee, \wedge, ^-, 0, 1)$ un'algebra di Boole: si dimostri che, definendo $a+b := (a \wedge \overline{b}) \vee (\overline{a} \wedge b)$ e $a \cdot b := a \wedge b$, $(B, +, \cdot)$ è un anello Booleano.
   Viceversa, sia A un anello Booleano e si definiscano $a \vee b := a + b + a \cdot b$, $a \wedge b = a \cdot b$ e $\overline{a} = 1 + a$: si dimostri che $(A, \vee, \wedge, ^-, 0, 1)$ è un'algebra di Boole.

6. Sia I un ideale di un reticolo distributivo e limitato L. Dimostrare che esiste un ideale massimale che estende I (per massimale si intende la stessa nozione data per gli anelli).

7. Sia $f \colon L_1 \to L_2$ un omomorfismo di reticoli limitati. Dimostrare che l'insieme $I = \{x \in L_1 \mid f(x) = 0\}$ è un ideale di L_1.

8. Sia L un reticolo distributivo e limitato. Un sottoinsieme non vuoto $F \subseteq L$ si dice un *filtro* di L se soddisfa le seguenti proprietà:

   1) $a \wedge b \in F$, per ogni $a, b \in F$;

   2) se $a \in F$ e $a \leq x$, per qualche $x \in L$, allora $x \in F$.

   Dimostrare che:

   (a) $1 \in F$;

   (b) per ogni $a \in L$, l'insieme $\uparrow a = \{x \in L \mid a \leq x\}$ è un filtro di L;

   (c) se L è finito ogni filtro è della forma $\uparrow a$;

   (d) se L è un'algebra di Boole, allora un sottoinsieme F di L è un filtro se e solo se l'insieme $I = \{\overline{x} \mid x \in F\}$ è un ideale di L, dove $\overline{x}$ è l'unico complemento dell'elemento $x \in L$.

Esercizi su polinomi, domini fattoriali, principali ed euclidei

1. Sia A un anello commutativo unitario. Dimostrare che un polinomio $p(x) \in A[x]$ è nilpotente sse tutti i coefficienti di p sono nilpotenti.

2. Sia A un anello commutativo unitario e $p(x) \in A[x]$ con coefficiente direttivo invertibile e di grado $n > 0$. Dato l'ideale principale $I = (p(x))$, si dimostri che esiste una bigezione tra l'anello quoziente $A[x]/I$ e le classi laterali $r(x)+I$, dove $r(x)$ è un polinomio di grado minore di n oppure $r(x) = 0$.

3. Sia A un dominio. Dimostrare che $U(A[x]) = U(A)$. L'uguaglianza è vera anche nel caso in cui A non sia un dominio?

4. Sia A un anello commutativo unitario e I un ideale di A. Sia J l'insieme di tutti i polinomi che hanno coefficienti in I. Dimostrare che J è un ideale di $A[x]$ e che $A[x]/J \cong A/I[x]$.

5. Si consideri l'anello dei polinomi $\mathbb{Z}[x]$. Sia I l'insieme dei polinomi di $\mathbb{Z}[x]$ il cui termine di grado zero è pari. Verificare che I è un ideale di $\mathbb{Z}[x]$ e che non è principale.

6. Siano A un dominio e B un anello unitario isomorfo ad A quale anello unitario. Si dimostri che:

   (a) B è un dominio;

   (b) se A è fattoriale, allora anche B è fattoriale;

   (c) se A è principale, allora anche B è principale;

   (d) se A è euclideo, allora anche B è euclideo.

7. Sia A un dominio euclideo e $a, b \in A^*$. Se $b|a$ e $\delta(a) = \delta(b)$ allora a è associato a b.

8. Si fornisca una dimostrazione diretta del fatto che ogni dominio euclideo è fattoriale. (Suggerimento: considerare δ^* e ragionare per induzione).

9. Sia A un dominio a ideali principali e sia I un ideale di A non banale. Dimostrare che ogni elemento non invertibile del quoziente A/I è divisore dello zero.

10. Dimostrare che per $f(x), g(x) \in A[x]$ si ha $\text{cont}(f \cdot g) = \text{cont}(f) \cdot \text{cont}(g)$.

11. Sia K un campo, $f(x) \in K[x]$ un polinomio di grado 2 o 3. Allora $f(x)$ è riducibile (non irriducibile) se e solo se $f(x)$ ha radici in K.

12. Sia A un dominio principale e a un elemento di A che ha un divisore primo $p \in A$ tale che p^2 non divide a. Allora il polinomio $f(x) = x^n + a$ è irriducibile in $A[x]$ per ogni $n > 0$.

13. Si dimostri che i polinomi $x^5 - 6x + 3$ e $x^7 - 60$ in $\mathbb{Z}[x]$ sono irriducibili.

14. Sia p un numero primo. Dimostrare che non esiste alcun omomorfismo di anelli unitari $\mathbb{Q}[x] \to \mathbb{Z}_p[x]$.

15. Dimostrare che il polinomio $x^4 + x^3 + 1 \in \mathbb{Z}[x]$ è irriducibile.

16. Calcolare il quoziente e il resto della divisione euclidea di $f(x)$ per $g(x)$ per i polinomi:

    a) $f(x) = x^5 - x^3 + 1$, $g(x) = x^2 + 1$ in $\mathbb{Z}[x]$;

    b) $f(x) = 3x^4 + 2x^3 + 2x + 5$, $g(x) = 2x^2 + 5x - 1$ in $\mathbb{Z}_7[x]$.

17. Sia $f(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$.

    a) Provare che $f(x)$ è irriducibile in $\mathbb{Z}_5[x]$;

    b) Costruire un campo quoziente di $\mathbb{Z}_5[x]$ con 125 elementi;

    c) Costruire un campo quoziente di $\mathbb{Z}_5[x]$ con 25 elementi.

18. Dire se i polinomi $f(x) = x^4 + 830x^3 + 1002x^2 + 213x + 71$ e $g(x) = x^4 + x^3 + 2x^2 + x + 4$ sono riducibili in $\mathbb{Q}[x]$.