ESERCIZI SU ANELLI

Anelli, sottoanelli, ideali.

Esercizio 1. Siano K un campo e $n \in \mathbb{N}$. Denotiamo con $K^{n,n}$ l'insieme delle matrici $n \times n$ su K e consideriamo su $K^{n,n}$ le usuali operazioni $+$ e $\cdot$ di addizione e moltiplicazione tra matrici. Provare che:

1. l'insieme $D^{n,n}$ delle matrici diagonali e l'insieme $T^{n,n}$ delle matrici triangolari superiori sono sottoanelli di $K^{n,n}$;
2. se $n > 1$, allora

$$B := \{f |\, f \in K^{n,n},\ \forall 1 \leq i,j \leq n\ :\ (i,j) \neq (1,1) \Rightarrow f_{ij} = 0\}$$

è un sottoanello unitario di $K^{n,n}$ con $1_B \neq 1_{K^{n,n}}$.

Esercizio 2. Per ogni $z \in \mathbb{C}$, denotiamo con $\bar{z}$ il complesso coniugato di z. Dimostrare che

$$\mathbb{H} := \left\{ f |\, f \in \mathbb{C}^{2,2},\ \exists x,y \in \mathbb{C} \quad f = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \right\}$$

è un corpo non commutativo, noto come il *corpo dei quaternioni*.

Esercizio 3. Siano $a, b \in \mathbb{R}$, $a < b$, e sia $\mathcal{C}[a,b]$ l'insieme delle funzioni continue definite sull'intervallo $[a,b]$ a valori in $\mathbb{R}$. Definiamo su $\mathcal{C}[a,b]$ le seguenti due operazioni $+$ e $\cdot$ ponendo, per ogni $f, g \in \mathcal{C}[a,b]$,

$$f+g : [a,b] \longrightarrow \mathbb{R},\ x \mapsto f(x)+g(x), \qquad f \cdot g : [a,b] \longrightarrow \mathbb{R},\ x \mapsto f(x) \cdot g(x)$$

1. Provare che $(\mathcal{C}[a,b], +, \cdot)$ è un anello commutativo unitario.
2. Se $S \subseteq [a,b]$, poniamo $\mathfrak{I}(S) := \{f |\, f \in \mathcal{C}[a,b]\ ,\ \forall x \in S\ \ f(x) = 0\}$. Dimostrare che $\mathfrak{I}(S)$ è un ideale di $\mathcal{C}[a,b]$.

Esercizio 4. Sia $\mathbb{T}^{2,2}$ l'anello delle matrici triangolari superiori 2×2 su un campo K. Consideriamo la funzione

$$f : \mathbb{T}^{2,2} \longrightarrow \mathbb{T}^{2,2}$$
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$$

1. Dimostrare che f è un omomorfismo di anelli.

2. Provare che l'insieme

$$I := \left\{ f | \, f \in \mathbb{T}^{2,2}, \; \exists \, b \in K \;\; f = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \right\}$$

è un ideale di A.

3. Dimostrare che $\mathbb{T}^{2,2}/I$ è isomorfo a $D^{2,2}$, dove $D^{2,2}$ è l'anello delle matrici diagonali 2×2 su K.

Esercizio 5. Siano A e B anelli commutativi unitari e sia $f : A \to B$ un omomorfismo di anelli.

1. Dimostrare che se A è un campo allora f è iniettiva oppure $f = 0$.

2. Si supponga f suriettiva. Provare che B è un campo se e solo se $\ker f$ è un ideale massimale di A.

Esercizio 6. Siano $a, b \in \mathbb{R}$, $a < b$, e sia $C[a, b]$ l'anello delle funzioni continue definite sull'intervallo $[a, b]$ a valori in $\mathbb{R}$ con le usuali operazioni di somma e prodotto tra funzioni. Sia poi $x \in [a, b]$.

1. Provare che l'applicazione $\phi_x : C[a, b] \to \mathbb{R}$, $f \mapsto f(x)$, è un epimorfismo di anelli.

2. Dimostrare che il sottoinsieme di $C[a, b]$ costituito dalle funzioni costanti è un sottoanello di $C[a, b]$ isomorfo a $\mathbb{R}$

3. Posto $S := \{x\}$, provare che l'ideale $\mathfrak{I}(S)$ è massimale.

Esercizio 7. Sia A un anello commutativo e J un ideale di A. Poniamo

$$\sqrt{J} := \{a | a \in A, \; \exists \, n \in \mathbb{N} \; a^n \in J\}.$$

Provare che $\sqrt{J}$ è un ideale di A contenuto nell'intersezione degli ideali primi di A contenenti J.

Esercizio 8. Sia J un ideale di $\mathbb{Z}$. Fornire una descrizione esplicita dell'ideale $\sqrt{J}$ definito come nell'esercizio precedente.

Esercizio 9. Sia A un anello commutativo unitario e M un ideale proprio di A. Dimostrare che le seguenti affermazioni sono equivalenti:

1. M è ideale massimale,

2. $\forall a \in A \backslash M \;\; \exists x \in A \;\; 1 - ax \in M$.

Esercizio 10. Sia A un dominio di integrità e siano $a, b \in A$. Provare che le seguenti affermazioni sono equivalenti:

1. gli ideali generati a e b in A coincidono;
2. esiste $u \in A$, u invertibile, tale che $b = ua$.

Esercizio 11. Provare che l'anello $\mathbb{Z}/\mathbb{Z}15$ ha due soli ideali non banali e che tali ideali sono massimali.

Esercizio 12. Siano A e B anelli commutativi unitari e sia $f : A \to B$ un epimorfismo di anelli. Provare che:

1. se P è un ideale primo di A contenente $\ker f$ allora $f(P)$ è un ideale primo di B;
2. se Q è un ideale primo di B allora l'antimmagine di Q tramite f è un ideale primo di A contenente $\ker f$.

Anello dei polinomi. Domini Euclidei.

Esercizio 13. Dato un anello A ed un elemento $a \in A$, si consideri l'omomorfismo $\varphi : A[x] \to A$ dato da $P(x) \mapsto P(a)$.

1. Si dimostri che φ è suriettivo con nucleo $(x-a) \subset A[x]$.
2. Si dimostri che vale l'isomorfismo di anelli $A[x]/(x-a) \simeq A$.

Esercizio 14. Siano C un campo, A un sottoanello proprio e non banale di C e D il campo dei quozienti di A. Un elemento $c \in C$ è detto *algebrico* su A se esiste un polinomio non nullo $P(x) \in A(x)$ tale che $P(c) = 0$. Provare che $c \in C$ è algebrico su A se e solo se è algebrico su D.

Esercizio 15. Siano A un anello commutativo unitario, $a \in A$ e I un ideale di A. Poniamo

$$\mathcal{I} := \{f |\ f \in A[x] \quad f(a) \in I\}.$$

Provare che:

1. $\mathcal{I}$ è un ideale di $A[x]$;
2. I è un ideale primo di A se, e solo se, $\mathcal{I}$ è un ideale primo di $A[x]$.

Esercizio 16. (a) Si consideri l'anello $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Trovare tutti gli elementi invertibili di$\mathbb{Z}[i]$.

(b) Ricordiamo che due elementi x e y dell'anello A si dicono *associati* se vale $y = ux$ per elemento invertibile $u \in A^*$. Provare che $x = a + ib$ e $y = a - ib$ sono associati in $\mathbb{Z}[i]$ se, e solo se, $ab = 0$ oppure $a \in \{b; -b\}$.

Esercizio 17. Determinare un massimo comun divisore α dei polinomi $f := 3x^3 - x^2 + 6x - 2$ e $g := x^2 - x + 1$ in $(\mathbb{Z}/Z7)[x]$ ed elementi $\beta, \gamma \in (\mathbb{Z}/Z7)[x]$ tali che $\alpha = \beta f + \gamma g$.

Esercizio 18. Determinare un massimo comun divisore α dei numeri complessi $4 + 13i$ e $8 + i$ in $\mathbb{Z}[i]$ ed elementi $\beta, \gamma \in \mathbb{Z}[i]$ tali che $\alpha = \beta(4 + 13i) + \gamma(8 + i)$.

Esercizio 19. Stabilire se i seguenti polinomi sono irriducibili in $\mathbb{Q}[x]$:

1. $2x^3 - 5x + 2$;
2. $2x^2 - 5x + 2$.

Esercizio 20. Si provi che ciascuno dei polinomi

1. $x^2 + 3$,
2. $x^2 - 2$.

non è irriducibile in $(\mathbb{Z}/\mathbb{Z}7)[x]$.

Esercizio 21. Sia $f := x^3 + x + 1 \in \mathbb{Q}[x]$ ed I l'ideale di $\mathbb{Q}[x]$ generato da f. Dimostrare che $\mathbb{Q}[x]/I$ è un campo e determinare l'inverso di $I + x$.

Esercizio 22. Provare che il polinomio $f := x^4 + x + 1 \in (\mathbb{Z}/\mathbb{Z}2)[x]$ è irriducibile e, indicato con J l'ideale di $(\mathbb{Z}/\mathbb{Z}2)[x]$ generato da f, determinare la cardinalità di $(\mathbb{Z}/\mathbb{Z}2)[x]/J$.

Esercizio 23. Sia $g := x^3 + x - 1 \in (\mathbb{Z}/3\mathbb{Z})[x]$. Dimostrare che

1. l'ideale principale $(g) \subset (\mathbb{Z}/3\mathbb{Z})[x]$ non è un ideale primo;
2. la classe di resto $[x^2 - x - 1]$ in $(\mathbb{Z}/3\mathbb{Z})[x]/(g)$ è un divisore dello zero.

Domini Euclidei, domini a ideali principali, e domini a fattorizzazione unica. Fattorizzazione di polinomi.

Esercizio 24. Sia D un dominio euclideo di funzione euclidea δ e sia $u \in D \setminus \{0\}$. Provare che sono equivalenti:

(i) u è invertibile;

(ii) $\forall a \in D \setminus \{0\}$ $\delta(u) \leq \delta(a)$;

(iii) $\delta(u) = \delta(1)$.

Esercizio 25. Sia D un dominio euclideo di funzione euclidea δ e siano $a, b \in D \setminus \{0\}$. Provare che a e b sono associati se, e solo se, $a \mid b$ e $\delta(a) = \delta(b)$.

Esercizio 26. Sia D un dominio a ideali principali e siano $a, b \in D$. Provare che, se a e b sono coprimi, allora si ha $(a)_D \cap (b)_D = (ab)_D$.

Esercizio 27. Si provi che ciascuno dei seguenti polinomi è irriducibile in $(\mathbb{Z}/\mathbb{Z}5)[x]$:

1. $x^3 + x + 1$;
2. $x^2 + 3$;
3. $x^2 + 2$;
4. $x^3 + 3x + 2$.

Esercizio 28. Provare che $x^4 + 3x^3 + 2x + 4$ non è irriducibile in $(\mathbb{Z}/\mathbb{Z}5)[x]$.

Esercizio 29. Sia C un campo e sia $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, con $a_0 \neq 0$ e $a_n \neq 0$, un polinomio irriducibile in $C[x]$. Provare che è irriducibile (in $C[x]$) anche il polinomio $g = a_n + a_{n-1}x + a_{n-2}x^2 + \cdots + a_0x^n$.

Esercizio 30. Provare che i seguenti polinomi sono irriducibili in $\mathbb{Q}[x]$:

1. $x^3 + 3x^2 + 9x + 6$;
2. $4x^4 + 5x + 10$;
3. $x^3 + 2x + 1$;
4. $x^4 - 2x^2 + 8x + 1$;

5. $3x^4 + 2x^3 + 4x^2 + 5x + 1$;

6. $x^5 + 5x^2 - 5x + 15$;

7. $x^4 - 10x^2 + 1$;

8. $-3x^4 + 27x^3 - 3x^2 + 9x + 1$;

9. $x^4 - 6x^3 + 12x^2 - 3x + 9$.

Esercizio 31. Provare che per ogni numero primo p il polinomio

$$f = 1 + x + x^2 + \cdots + x^{p-1}$$

è irriducibile in $\mathbb{Q}[x]$. Esibire un esempio di polinomio del tipo

$$f = 1 + x + x^2 + \cdots + x^{n-1}$$

(con n non primo) che sia riducibile in $\mathbb{Q}[x]$.

Esercizio 32. Siano $F := \mathbb{Z}/\mathbb{Z}3$, $g := x^3 + x + 1 \in F[x]$ e sia $J = gF[x]$. Dimostrare che

1. J non è un ideale primo;

2. $J + (2x + 2)$ è un elemento invertibile di $F[x]/J$.

Esercizio 33. Si consideri l'anello $A = \mathbb{K}[x_1, x_2, x_3, \dots]/J$, dove J è l'ideale generato dagli elementi

$$x_1 - x_2^2\ ,\quad x_2 - x_3^2\ ,\quad x_3 - x_4^2\ ,\quad x_4 - x_5^2\ , \dots\ .$$

(a) Dimostrare che A è l'unione degli anelli di polinomi $\mathbb{K}[x_n] \simeq \mathbb{K}[x]$.

(b) Trovare una catena ascendente di ideali principali in A che non stabilizza mai.

(c) Mostrare che non esiste una fattorizzazione di x_1 come prodotto di irriducibili.

Esercizio 34. Siano $a, b \in \mathbb{K}$, con $b \neq 0$. Dimostrare che un polinomio $f(x) \in \mathbb{K}[x]$ è irriducibile se e solo se $f(a + bx)$ è irriducibile.

Esercizio 35. Dimostrare che il nucleo dell'omomorfismo $\mathbb{Z}[x] \to \mathbb{R}$ che mappa $x \mapsto 1 + \sqrt{2}$ è un ideale principale, e trovare un generatore per tale ideale.

Esercizio 36. Sia p un numero primo. Dimostrare che, per ogni $n \geq 1$, il polinomio $x^n - p$ è irriducibile in $\mathbb{Z}[x]$.

Esercizio 37. In questo esercizio dimostriamo che il polinomio $x^4 + 1$ è irriducibile in $\mathbb{Z}[x]$, ma la sua immagine in $\mathbb{F}_p[x]$ è riducibile per ogni intero primo p.

(a) Dimostrare che $x^4 + 1$ è irriducibile in $\mathbb{Z}[x]$.

(b) Vogliamo ora dimostrare che il polinomio $x^4 + 1$ è riducibile in $\mathbb{Z}/p[x]$ per ogni primo p. Lo facciamo seguendo i seguenti punti. Innanzitutto, dimostrare l'affermazione per $p = 2$. Da ora in poi possiamo dunque suppore che p è un primo dispari.

(c) Dimostrare le seguenti identità:

$$x^4 + 1 = (x^2)^2 - (-1) = (x^2 + 1)^2 - 2x^2 = (x^2 - 1)^2 - (-2)x^2 \,. \quad (1)$$

(d) Consideriamo la funzione $\rho : \mathbb{F}_p^* \to \mathbb{F}_p^*$ data da $\rho(x) = x^2$. Chiamiamo gli elementi nell'immagine di ρ *quadrati* modulo p, e gli elementi che non sono nell'immagine di ρ *non-quadrati* modulo p. Dimostrare che ci sono esattamente $\frac{p-1}{2}$ quadrati modulo p in $\mathbb{F}_p^*$ (e $\frac{p-1}{2}$ non-quadrati modulo p).

(e) Dimostrate che i quadrati modulo p sono precisamente gli elementi $x \in \mathbb{F}_p^*$ tali che $x^{\frac{p-1}{2}} \equiv -1(p)$. In particolare, dedurre che il prodotto di due non-quadrati modulo p è un quadrato modulo p.

(f) Dimostrare che tra i tre numeri -1, 2, -2 almeno uno è un quadrato modulo p.

(g) Dedurre (usando le identità (1)) che $x^4 + 1$ è riducibile in $\mathbb{F}_p[x]$.

Esercizio 38. Dato il polinomio $f := x^4 - x^2 - 12 \in \mathbb{Q}[x]$ e denotato con J l'ideale generato da f in $\mathbb{Q}[x]$, descrivere gli ideali dell'anello $\mathbb{Q}[x]/J$ e dire quali tra di essi sono massimali.

Esercizio 39. Dire per quali valori di $a \in \mathbb{Z}$ il polinomio $3x^3 + 20ax^2 + 50a^2x + 60$ sia irriducibile, rispettivamente, in $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x]$

Esercizio 40. Provare che gli elementi irriducibili in $\mathbb{Z}[i]$ sono:

1. gli associati di un numero primo p con $p = 3 \bmod(4)$;

2. i numeri $z = a + ib \in \mathbb{Z}[i]$ tali che $a^2 + b^2$ è un primo (necessariamente uguale a 2 o congruo a 1 mod(4)).

Esercizio 41. Sono assegnati in $\mathbb{Z}[i]$ i due interi di Gauss $z := 4 + 2i, w := 3 - i$.

1. Determinare un massimo comun divisore di z e w;
2. Scrivere z come prodotto di interi di Gauss irriducibili.

Esercizio 42. Descrivere l'anello quoziente $\mathbb{Z}[i]/(p)$ nei seguenti casi:

(a) $p = 2$,

(b) $p \equiv 1 \mod (4)$,

(c) $p \equiv 3 \mod (4)$.