ESERCIZI DI ALGEBRA I
Canale M-Z – A.A. 2015-16

Insiemi e funzioni

Esercizio 1. Siano R, S, T insiemi. Si dimostri che

(a) $R \cap S \subseteq T \iff R \subseteq T \cup (R \setminus S)$;

(b) $R \cap T = \emptyset \iff R \setminus (S \setminus T) \subseteq (R \setminus S) \setminus T$.

Esercizio 2. Siano A, B insiemi. Si dimostri che

$$A \subseteq B \qquad \iff \qquad \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

Esercizio 3. Siano S, T insiemi. Si dimostri se è vero che

(a) $\mathcal{P}(S \cap T) = \mathcal{P}(S) \cap \mathcal{P}(T)$;

(b) $\mathcal{P}(S \cup T) = \mathcal{P}(S) \cup \mathcal{P}(T)$.

Siano X, Y insiemi e R una relazione tra X e Y. Definiamo *relazione inversa di* R

$$R^{-1} := \{(y, x) |\, (x, y) \in R\}.$$

Se H, Z sono insiemi con $Y \subseteq H$ e S una relazione tra H e Z, definiamo *relazione composta*

$$S \circ R := \{(x, z) |\, x \in X,\ z \in Z \quad \exists y \in Y\ (x, y) \in R \quad \text{e} \quad (y, z) \in S\}.$$

Esercizio 4. Siano

$$A := \{(x, y) |\, x, y \in \mathbb{N}_+ \quad y = x(x+1)\},$$

$$B := \{(x, y) |\, x, y \in \mathbb{N}_+ \quad x \,\text{pari}\},$$

$$C := \{(x, y) |\, x, y \in \mathbb{Z} \quad 4 \text{ divide } x^2 - y^2\}.$$

(a) Per ciascuno degli insiemi $A, B, C, A \cap B, C \circ A, C^{-1} \circ A, C^{-1}$ dire se si tratta di funzioni e, in tal caso, stabilire se sono iniettive e/o suriettive.

(b) Determinare $A \cap B \cap C$ e dire se è vuoto.

Esercizio 5. Sia X un insieme e R, S, T relazioni su X. Si dimostri se sono vere le seguenti affermazioni:

(a) $R^{-1} \subseteq R \Longrightarrow R^{-1} = R$;

(b) $R \circ R \subseteq R \Longrightarrow R \circ R = R$;

(c) $(S \circ R)^{-1} = S^{-1} \circ R^{-1}$;

(d) $(R \setminus S)^{-1} = R^{-1} \setminus S^{-1}$.

Esercizio 6. Siano S, T insiemi, $f : S \longrightarrow T$, $A \subseteq S$ e $B \subseteq T$. Provare che

(a) $A \subseteq f^{-1}(f(A))$ e $A = f^{-1}(f(A))$ se f è iniettiva;

(b) $f(f^{-1}(B)) \subseteq B$ e $B = f(f^{-1}(B))$ se f è suriettiva.

Esercizio 7. Siano S, T insiemi finiti, $f : S \longrightarrow T$. Provare che

(a) se $|S| = |T|$ e f è suriettiva, allora f è iniettiva;

(b) se $|S| = |T|$ e f è iniettiva, allora f è suriettiva.

Esercizio 8. Sia X un insieme non vuoto con n elementi e $f : \mathcal{P}(X) \longrightarrow \{1, \ldots, n\}$.

(a) Si dimostri che esistono $A, B \in \mathcal{P}(X)$ con $A \neq B$ tali che

$$f(A) = f(B) = f(A \cup B) = f(A \cap B).$$

(b) Discutere il caso in cui $X = \emptyset$.

Esercizio 9. Sia A l'insieme dei numeri pari e B quello dei numeri dispari in $\mathbb{Z}$. Sia

$$f : A \times B \longrightarrow B, \qquad (a, b) \longmapsto a - b,$$
$$g : A \times B \longrightarrow A \times B, \qquad (a, b) \longmapsto (ab, a + b).$$

(a) Dire se f è iniettiva e/o suriettiva (su B).

(b) Dire se g è iniettiva e/o suriettiva (su $A \times B$).

Esercizio 10. Sia P l'insieme dei numeri interi pari e D quello dei numeri interi dispari. Si stabilisca una biezione tra:

(a) $\mathbb{N}$ e $\mathbb{Z}$;

(b) $\mathbb{N}_+$ e P;

(c) $\mathbb{N}_+$ e D.

Esercizio 11. Siano X, Y, Z insiemi, $f \in Y^X$ e $g \in Z^Y$. Dimostrare se sono vere le seguenti:

(a) $g \circ f$ iniettiva $\Longrightarrow$ f iniettiva;

(b) $g \circ f$ suriettiva $\Longrightarrow$ f suriettiva;

(c) $g \circ f$ iniettiva e f suriettiva $\Longrightarrow$ g iniettiva;

(d) $g \circ f$ suriettiva e g iniettiva $\Longrightarrow$ f suriettiva.

Esercizio 12. Siano A, B insiemi tali che $B \subset A$. Provare che $\mathcal{P}(A)$ è equipotente a $\mathcal{P}(B) \times \mathcal{P}(A \setminus B)$.

Esercizio 13. Sia $\phi : \{0,1,2,3,4\}^{\mathbb{N}} \longrightarrow \{0,1,2\}^{\mathbb{N}}$ tale che

$$(\phi(f))(n) := \begin{cases} 0 & \text{se } f(n) \in \{0,2,4\}; \\ 1 & \text{se } f(n) \in \{1,3\} \end{cases}$$

.

(a) Dire se ϕ è iniettiva e/o suriettiva;

(b) determinare $\mathrm{Im}(\phi)$;

(c) determinare $(\phi)^{-1}(g)$ dove $g : \mathbb{N} \longrightarrow \{0,1,2\}$ è tale che $g(i) := 1$ per ogni i.

Relazioni di equivalenza e Cardinalità

Esercizio 14. Siano $A := \{(1,2),(2,1),(3,1),(4,4)\}$ e $B := \{(1,1),(3,3),(1,3),(2,2),(4,4)\}$. Per ciascuno degli insiemi $A, B, A \cup B, A \cap B, B \setminus A$ dire se si tratta di

(a) una relazione riflessiva su $\{1,2,3,4\}$;

(b) una relazione simmetrica;

(c) una funzione da $\{1,2,3,4\}$ in $\{1,2,3,4\}$.

Esercizio 15. Si dica se le seguenti implicazioni valgano per relazioni R, S in generale

(a) R, S simmetriche $\implies R \cup S$ simmetrica;

(b) R, S simmetriche $\implies R \cap S$ simmetrica;

(c) R, S transitive $\implies R \cup S$ transitiva;

(d) R, S transitive $\implies R \cap S$ transitiva.

Esercizio 16. Consideriamo l'insieme $X := \{1,2,3\}$. Definire una relazione su X tale che

(a) non sia nè riflessiva, nè simmetrica, nè transitiva;

(b) sia riflessiva, simmetrica, ma non transitiva;

(c) sia d'equivalenza.

Svolgere lo stesso esercizio ponendo $X := \mathbb{N}$.

Esercizio 17. Consideriamo su $X := \mathbb{R} \times \mathbb{R}$ la relazione $\approx$ così definita:

$$\forall x, y, z, w \in \mathbb{R} \quad (x,y) \approx (z,w) \iff \exists a \in \mathbb{R} \ \ y = x^3 + a \text{ e } w = z^3 + a.$$

(a) Provare che $\approx$ è una relazione di equivalenza su X.

(b) Determinare un sistema di rappresentanti per $X/\approx$.

Esercizio 18. Consideriamo su $X := \mathbb{Z} \times \mathbb{Z}$ la relazione $\approx$ così definita:

$$\forall x_1, x_2, y_1, y_2 \in \mathbb{Z} \quad (x_1, y_1) \approx (x_2, y_2) \iff 2(x_1 - x_2) = 3(y_2 - y_1).$$

Dimostrare che

(a) $\approx$ è un'equivalenza su X;

(b) $X/\approx$ è equipotente a $\mathbb{Z}$.

Esercizio 19. Consideriamo su $P := \{(a,b,c)|\ a,b,c \in \mathbb{Z}\ \ a,c>0\ \ a^2+b^2 = c^2\}$ la relazione $\approx$ così definita:

$$\forall (a,b,c),(a_1,b_1,c_1) \in P \quad (a,b,c) \approx (a_1,b_1,c_1) \iff a_1(b+c) = a(b_1+c_1).$$

Dimostrare che

(a) $\approx$ è un'equivalenza su P;

(b) $P/\approx$ è equipotente a $\mathbb{Q}^+ := \{x|\ x \in \mathbb{Q}\ \ x>0\}$.

Esercizio 20. Definiamo la seguente relazione $\sim$ su $\mathbb{Q}$ ponendo

$$\forall x,y \in \mathbb{Q} \quad x \sim y \iff x-y \in \mathbb{Z}.$$

Si dimostri che

(a) $\sim$ è una relazione d'equivalenza su $\mathbb{Q}$;

(b) se $x := \frac{a}{b} \in \mathbb{Q}$, $[x]_\sim = \{y|\ y \in \mathbb{Q} \quad \exists c \in [a]_{\equiv_b} \quad y = \frac{c}{b}\}$.

Esercizio 21. Sia $\emptyset \neq X$ un insieme, $\mathcal{P}(X)$ l'insieme delle parti di X ed $A := \{0,1,2,3,4\}^X$. Definiamo su A la seguente relazione $\sim$ ponendo

$$\forall \phi,\psi \in A \qquad \phi \sim \psi \iff \{a|\ a \in X,\ \phi(a)=1\} = \{a|\ a \in X,\ \psi(a)=1\}.$$

Provare che

(a) $\sim$ è una relazione di equivalenza su A;

(b) $A/_\sim$ è equipotente a $\mathcal{P}(X)$.

Esercizio 22. Sia $k \in \mathbb{N}$. Si consideri su $\mathbb{Z}$ la relazione $\sim$ così definita:

$$\forall\, a,b \in \mathbb{Z} \qquad a \sim b \iff 2k \mid a+3b.$$

Dire per quali valori di k

(a) $\sim$ è riflessiva;

(b) $\sim$ è una relazione di equivalenza.

Esercizio 23. Definiamo su $\mathbb{C}$ la seguente relazione ρ:

$$\forall z, w \in \mathbb{C} \quad z \,\rho\, w \qquad \Longleftrightarrow \qquad z - w = \overline{w - z}.$$

(a) Verificare che ρ è una relazione di equivalenza.

(b) Descrivere l'insieme quoziente $\mathbb{C}/\rho$ e determinarne la cardinalità.

(c) Stabilire se ρ è compatibile colla somma e/o col prodotto di $\mathbb{C}$.

Esercizio 24. Determinare la cardinalità dei seguenti insiemi

1. $\{x \,|\, x \in \mathbb{R},\ x^2 \in \mathbb{Q} \text{ e } x^3 \in \mathbb{Q}\}$;
2. $\{x \,|\, x \in \mathbb{R},\ x^2 \in \mathbb{Q} \text{ e } x^3 + \sqrt{2} \in \mathbb{Q}\}$;
3. $\{(x, y) \,|\, (x, y) \in \mathbb{Z} \times \mathbb{R},\ (x - y)^2 \in \mathbb{Q}\}$;
4. $\{(x, y) \,|\, (x, y) \in \mathbb{R} \times \mathbb{R},\ x + y\sqrt{2} \in \mathbb{Q}\}$;
5. $\{(x, y) \,|\, (x, y) \in \mathbb{R} \times \mathbb{R},\ x + y\sqrt{2} \in \mathbb{Q} \text{ e } x - y\sqrt{2} \in \mathbb{Q}\}$;
6. $\{U \,|\, U \subseteq \mathbb{R}^3,\ U \text{ è sottospazio di } \mathbb{R}^3\}$.

Introduzione alle strutture algebriche

Esercizio 25. Sia $(S, *)$ un semigruppo e sia $a \in S$. Poniamo $a^1 := a$ e, induttivamente,

$$\forall i \in \mathbb{N}_+ \qquad a^{i+1} := a^i * a. \tag{1}$$

Provare che, per ogni $m, n \in \mathbb{N}_+$, valgono:

(i) $a^m * a^n = a^{m+n}$;

(ii) $(a^m)^n = a^{m \cdot n}$.

Esercizio 26. Si consideri su $\mathbb{Q}^2$ l'operazione

$$\bullet : \mathbb{Q}^2 \times \mathbb{Q}^2 \longrightarrow \mathbb{Q}^2, \qquad ((a_1, b_1), (a_2, b_2)) \longmapsto (a_1 a_2, a_1 b_2 + b_1).$$

Provare che valgono le seguenti affermazioni:

(i) $(\mathbb{Q}^2, \bullet)$ è un monoide;

(ii) per ogni $a, b \in \mathbb{Q}$ e per ogni $n \in \mathbb{N}_+$

$$(a, 0)^n = (a^n, 0) \qquad (1, b)^n = (1, nb).$$

La struttura $(\mathbb{Q}^2, \bullet)$ è commutativa?

Esercizio 27. Sia $(X, \circ)$ una struttura algebrica. Definiamo sull'insieme delle parti di X, che denotiamo col simbolo $\mathfrak{P}(X)$, l'operazione

$$\begin{aligned} \bullet :& \mathfrak{P}(X) \times \mathfrak{P}(X) \longrightarrow \mathfrak{P}(X), \\ & (A, B) \longmapsto \{x |\ x \in X \quad \exists a \in A \quad \exists b \in B \quad x = a \circ b\}. \end{aligned}$$

Provare che valgono le seguenti affermazioni:

1. se $(X, \circ)$ è commutativa, allora $(\mathfrak{P}(X), \bullet)$ è commutativa;
2. se $(X, \circ)$ è associativa, allora $(\mathfrak{P}(X), \bullet)$ è associativa;
3. se $(X, \circ)$ ha elemento neutro, allora $(\mathfrak{P}(X), \bullet)$ ha elemento neutro.

Esercizio 28. Poniamo $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, $G := \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \in \mathbb{Q},\ a, d \in \mathbb{Q}^*\}$ e $H := \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Q}\}$. Dire se:

1. G è un gruppo rispetto all'usuale moltiplicazione tra matrici;

2. H è un sottogruppo di G.

Esercizio 29. Sia $A := \mathbb{Z} \times \mathbb{Q}$ e definiamo su A le seguenti operazioni

$$(a, x) + (b, y) := (a + b, x + y) \quad (a, x) \cdot (b, y) := (ab, xy)$$

Dire se:

1. $B := \{(3a, x) \mid a, x \in \mathbb{Z}\}$ è un sottoanello di A;
2. vale che per ogni $(a, x) \in A$ e $(b, y) \in B$ $(a, x) \cdot (b, y) \in B$.

Gli interi. Divisibilità e fattorizzazione in $\mathbb{Z}$

Esercizio 30. Sia $n \in \mathbb{N}_+$. Dimostrare che

$$\forall z \in \mathbb{Z} \quad n \mid z(z+1)(z+2)(z+3)\dots(z+n-1),$$

cioè il prodotto di n numeri interi consecutivi è divisibile per n.

Esercizio 31. Dimostrare che

$$\forall z \in \mathbb{Z} \quad 6 \mid z^3 - z.$$

Esercizio 32. Dimostrare che, per ogni numero intero dispari z, vale che $8 \mid z^2 - 1$.

Esercizio 33. Dimostrare che, per ogni $a \in \mathbb{Z}$ e per ogni $n \in \mathbb{N}_+$,

$$a - 1 \mid a^n - 1.$$

Esercizio 34. Dimostrare che, per ogni $a \in \mathbb{Z}$ e per ogni numero naturale dispari n,

$$a + 1 \mid a^n + 1.$$

Esercizio 35. Dimostrare che, per ogni $a \in \mathbb{Z}$ e per ogni $m, n \in \mathbb{N}_+$,

$$m \mid n \implies a^m - 1 \mid a^n - 1.$$

Esercizio 36. Dimostrare che

$$\forall n \in \mathbb{N} \quad 3 \mid 4^n + 2.$$

Esercizio 37. Dimostrare che valgono le seguenti identità:

1. $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$;
2. $\sum_{i=0}^{n} 3^i = \frac{1-3^{n+1}}{1-3}$;
3. $\prod_{i=2}^{n}(1 - \frac{1}{i}) = \frac{1}{n}$.

Esercizio 38. Dimostrare che, per ogni $a, b \in \mathbb{Z}$, vale

$$mcd(ab, a+b) \mid mcd(a^2, b^2).$$

Esercizio 39. Dimostrare che

$$\forall z \in \mathbb{Z} \quad mcd(3z+4, 4z+5) = 1.$$

Esercizio 40. Siano $p, q \in \mathbb{N}_+$ e consideriamo su $X := \mathbb{Z} \times \mathbb{Z}$ la relazione $\approx$ così definita:

$$\forall x_1, x_2, y_1, y_2 \in \mathbb{Z} \quad (x_1, y_1) \approx (x_2, y_2) \iff p(x_1 - x_2) = q(y_2 - y_1).$$

Dimostrare che

1. $\approx$ è un'equivalenza su X;
2. determinare un sottinsieme di $\mathbb{Z}$ equipotente a $X/\approx$.

Esercizio 41. Dimostrare che, per ogni $z \in \mathbb{Z}$, vale

$$mcd(z, z+2) = \begin{cases} 1 & \text{se } z \text{ è dispari;} \\ 2 & \text{se } z \text{ è pari.} \end{cases}$$

Esercizio 42. Siano $a, b, c \in \mathbb{Z}$ e $d := \mathrm{mcd}(a, b)$. Si dimostri che

1. $|c|d = \mathrm{mcd}(ca, cb)$;
2. $\mathrm{mcd}(a - b, a + b) \in \{d, 2d\}$.

Esercizio 43. Siano $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ tali che $ad = bc$. Si dimostri che $a^2 + b^2 + c^2 + d^2$ non è un numero primo.

Esercizio 44. Dimostrare che esistono infiniti numeri primi nell'insieme $\{3k + 2 \mid k \in \mathbb{N}\}$.

Esercizio 45. Dimostrare che

$$\forall n \in \mathbb{N} \quad 2^n - 1 \in \mathbb{P} \implies n \in \mathbb{P}.$$

Esercizio 46. Dimostrare che

$$\forall a, n \in \mathbb{N} \quad a^n - 1 \in \mathbb{P} \quad \text{e} \quad n > 1 \implies a = 2 \quad \text{e} \quad n \in \mathbb{P}.$$

I primi della forma $2^n - 1$ per qualche primo n si dicono *primi di Mersenne*.

Esercizio 47. Sia $p \in \mathbb{P}$. Dimostrare che

$$\forall m, n \in \mathbb{N} \quad m \mid p^n \implies m \mid p^m.$$

Esercizio 48. Sia $a \in \mathbb{N}$. Dimostrare che

$$\forall m, n \in \mathbb{N} \quad m \mid a^n \implies m \mid a^m.$$

Interi modulo n. Equazioni alle congruenze.

Esercizio 49. Dimostrare che un numero dispari che è somma di due quadrati è sempre congruo a 1 modulo 4.

Esercizio 50. Al variare di $a \in \mathbb{Z}$ determinare se il seguente sistema di equazioni congruenziali è compatibile, ed in tal caso trovarne le soluzioni:

$$\begin{cases} 2x \equiv 5(7) \\ x \equiv 4(9) \\ 4x \equiv a(15) \end{cases}$$

Esercizio 51. Determinare per quali interi $a, b \in \mathbb{Z}$ il seguente sistema di equazioni ammette soluzioni

$$\begin{cases} ax \equiv 3(5) \\ 3x \equiv b(8) \end{cases}$$

Esercizio 52. Dire, motivando la risposta, quali delle seguenti equazioni ammettono soluzioni intere:

$$324x + 81y = 26$$
$$324x + 81y = 27$$
$$36x + 90y = 54$$

Gruppi

Esercizio 53. Siano $m, n \in \mathbb{Z}$. Poniamo $d := mcd(m, n)$ e $c := mcm(m, n)$. Provare che valgono le seguenti affermazioni:

(i) $\mathbb{Z}m + \mathbb{Z}n \leq \mathbb{Z}$ e $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}d$;

(ii) $\mathbb{Z}m \cap \mathbb{Z}n \leq \mathbb{Z}$ e $\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}c$;

(iii) $\langle \mathbb{Z}m \cup \mathbb{Z}n \rangle = \mathbb{Z}m + \mathbb{Z}n$.

Trovare, se esistono, due interi h, k tali che $\mathbb{Z}h \cup \mathbb{Z}k$ non è un sottogruppo di $\mathbb{Z}$ e due interi $r, s \neq 1$ tali che $\mathbb{Z}r \cup \mathbb{Z}s = \mathbb{Z}$.

Esercizio 54. Sia $(G, \cdot)$ un gruppo. Dimostrare che, per ogni $H, K \leq G$, $H \cap K \leq G$. Estendere tale risultato ad un arbitrario numero di sottogruppi di $(G, \cdot)$.

Esercizio 55. Sia $(G, \cdot)$ un gruppo. Dimostrare che, per ogni $H, K \leq G$, valgono le seguenti affermazioni:

(i) $H \cup K \leq G \iff H \subseteq K \quad \text{o} \quad K \subseteq H$;

(ii) $H \cdot K \leq G \iff H \cdot K = K \cdot H$.

Esercizio 56. Sia $(G, \cdot)$ un gruppo e $H \leq G$. Dimostrare che sono equivalenti le seguenti affermazioni:

(i) $\forall x \in G \quad Hx = xH$;

(ii) $\forall x \in G \quad x^{-1}Hx = H$.

Esercizio 57. Provare che un gruppo G è abeliano se, e solo se, per ogni $x, y \in G$ risulta $(xy)^{-1} = x^{-1}y^{-1}$.

Esercizio 58. Sia $p \in \mathbb{P}$ e siano

$$S := \{q |\ q \in \mathbb{Q} \quad \exists j \in \mathbb{N}_0 \quad p^j q \in \mathbb{Z}\}$$

$$T := \{q |\ q \in \mathbb{Q} \quad \exists r \in \mathbb{N} \quad mcd(r, p) = 1 \quad rq \in \mathbb{Z}\}$$

Provare che valgono le seguenti affermazioni:

(i) S, T sono sottogruppi di $(\mathbb{Q}, +)$;

(ii) $S \cap T = \mathbb{Z}$.

Esercizio 59. Sia G un gruppo, e il suo elemento neutro, $a \in G$ e $m, n \in \mathbb{Z}$ primi tra loro. Provare che, se $a^m = e$, allora esiste $b \in G$ tale che $a = b^n$.

Esercizio 60. Sia G un gruppo finito. Dimostrare che, per ogni $x, y \in G$, valgono le seguenti affermazioni:

(i) $o(x) = o(y^{-1}xy)$;

(ii) $o(xy) = o(yx)$;

(iii) se $xy = yx$, allora $o(xy)$ divide $o(x)o(y)$.

Esercizio 61. Sia G un gruppo abeliano finito e siano $x, y \in G$ tali che $mcd(o(x), o(y)) = 1$. Dimostrare che valgono le seguenti affermazioni:

(i) $o(xy) = o(x)o(y)$;

(ii) $\langle x \rangle \langle y \rangle$ è un sottogruppo ciclico di G.

Esercizio 62. Si consideri nel gruppo simmetrico S_8 la permutazione

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 3 & 7 & 5 & 1 & 8 & 4 \end{pmatrix}.$$

Determinare la decomposizione di α in cicli disgiunti e l'ordine di α. Provare inoltre che esiste una permutazione di $S_8 \setminus \langle \alpha \rangle$ che commuta con α.

Esercizio 63. Completare la scrittura

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & 7 & & & 5 & & 6 & \end{pmatrix}$$

in modo da ottenere:

(i) una permutazione $\alpha \in \mathcal{S}_8$ prodotto di un numero pari di cicli disgiunti;

(ii) una permutazione $\beta \in \mathcal{S}_8$ prodotto di un numero dispari di cicli disgiunti.

Esercizio 64. Siano

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 8 & 4 & 6 & 3 & 1 & 2 \end{pmatrix},$$

$$\beta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 8 & 4 & 7 & 1 & 3 & 2 \end{pmatrix}.$$

Determinare $\pi \in \mathcal{S}_8$ tale che $\pi^{-}\alpha\pi = \beta$ e, per ogni $n \in \mathbb{N}$, α^n abbia almeno un'orbita di cardinalità 5. Scrivere α^n come prodotto di trasposizioni.

Esercizio 65. Siano

$$\psi_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 7 & 6 & 4 \end{pmatrix},$$

$$\psi_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 6 & 4 & 7 \end{pmatrix},$$

$$\psi_3 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 7 & 4 & 5 & 6 & 3 \end{pmatrix}.$$

Per ogni $\sigma \in \mathcal{S}_3$ poniamo $\phi_\sigma := \psi_{1\sigma}\psi_{2\sigma}\psi_{3\sigma}$.

(i) Per ogni $\sigma \in \mathcal{S}_3$ si dia ϕ_σ nella scrittura standard.

(ii) Per ogni $\sigma \in \mathcal{S}_3$ si dia la decomposizione di ϕ_σ in cicli disgiunti.

(iii) Per ogni $\sigma, \sigma' \in \mathcal{S}_3$ si dica se esiste una permutazione $\pi \in \mathcal{S}_7$ tale che $\pi^- \phi_\sigma \pi = \phi_{\sigma'}$ dando una tale permutazione nel caso che la risposta sia positiva.

(iv) Si diano un numero $k \in \mathbb{N}$ e trasposizioni $\tau_1, \ldots, \tau_k, \tau'_1, \ldots, \tau'_k \in \mathcal{S}_7$ tali che $\{\tau_1, \ldots, \tau_k\} \neq \{\tau'_1, \ldots, \tau'_k\}$ e $\tau_1 \cdots \tau_k = \psi_1\psi_2\psi_3 = \tau'_1 \cdots \tau'_k$.

Esercizio 66. Per ogni $n \in \mathbb{N}$ poniamo $\pi_n := (12)(123)\cdots(12\cdots n) \in S_n$. Si dia la decomposizione di π_n in cicli disgiunti e la struttura ciclica di π_n.

Esercizio 67. Siano $n \in \mathbb{N}, \zeta_1, \zeta_2$ cicli di $\mathcal{S}_n \setminus \{id\}, A_1, A_2$ le loro orbite non banali, $\pi := \zeta_1\zeta_2$.

(i) Sia $|A_1 \cap A_2| = 1$. Si dimostri che π è un ciclo $\neq id$.

(ii) Sia $|A_1 \cap A_2| = 2$. Si dimostri che π è un ciclo se, e solo se, $Fix\pi \cap A_1 \cap A_2 \neq \emptyset$.

Anelli, sottoanelli, ideali.

Esercizio 68. 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 69. 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 70. 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 71. 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 72. 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 73. 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 74. 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 75. Sia J un ideale di $\mathbb{Z}$. Fornire una descrizione esplicita dell'ideale $\sqrt{J}$ definito come nell'esercizio precedente.

Esercizio 76. 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 77. Provare che l'anello $\mathbb{Z}/\mathbb{Z}15$ ha due soli ideali non banali e che tali ideali sono massimali.

Esercizio 78. 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 79. 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 80. 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 81. 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 82. (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 83. 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 84. 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 85. Stabilire se i seguenti polinomi sono irriducibili in $\mathbb{Q}[x]$:

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

Esercizio 86. 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 87. 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 88. 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 $(\mathbb{Z}/\mathbb{Z}2)[x]/J$.

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

Esercizio 89. 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 90. 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 91. 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 92. Provare che $x^4 + 3x^3 + 2x + 4$ non è irriducibile in $(\mathbb{Z}/\mathbb{Z}5)[x]$.

Esercizio 93. 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 94. 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 95. 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 96. 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 97. 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 98. 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 99. 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 100. 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.