ESERCIZI DI ALGEBRA I

Canali A-Di & Dl-Pa – A.A. 2011-12

Settimana 1 – Insiemi e funzioni

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

1. $R \cap S \subseteq T \iff R \subseteq T \cup (R \setminus S)$;
2. $R \cap T = \emptyset \iff R \setminus (S \setminus T) \subseteq (R \setminus S) \setminus T$.

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

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

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

1. $\mathcal{P}(S \cap T) = \mathcal{P}(S) \cap \mathcal{P}(T)$;
2. $\mathcal{P}(S \cup T) = \mathcal{P}(S) \cup \mathcal{P}(T)$.

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

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

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

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

1. 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.
2. 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:

1. $R^{-1} \subseteq R \Longrightarrow R^{-1} = R$;
2. $R \circ R \subseteq R \Longrightarrow R \circ R = R$;
3. $(S \circ R)^{-1} = S^{-1} \circ R^{-1}$;
4. $(R \setminus S)^{-1} = R^{-1} \setminus S^{-1}$.

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

1. $A \subseteq f^{-1}(f(A))$ e $A = f^{-1}(f(A))$ se f è iniettiva;
2. $f^{-1}(f(B)) \subseteq B$ e $B = f^{-1}(f(B))$ se f è suriettiva.

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

1. se $|S| = |T|$ e f è suriettiva, allora f è iniettiva;
2. se $|S| = |T|$ e f è iniettiva, allora f è suriettiva.

Esercizio 8. Sia X un insieme finito, $H := \{0, 1\}^X$. Provare che esiste una biezione da $\mathcal{P}(X)$ in H.

Esercizio 9. Sia X un insieme non vuoto con n elementi e $f : \mathcal{P}(X) \longrightarrow \{1, \ldots, n\}$.

1. Si dimostri che esistono $A, B \in \mathcal{P}(X)$ con $A \neq B$ tali che
$$f(A) = f(B) = f(A \cup B) = f(A \cap B).$$
2. Discutere il caso in cui $X = \emptyset$.

Esercizio 10. Sia A l'insieme dei numeri pari e B quello dei numeri dispari in $\mathbb{Z}$. Sia
$$f : A \times B \longrightarrow B, \qquad (a, b) \longmapsto a - b,$$
$$g : A \times B \longrightarrow A \times B, \qquad (a, b) \longmapsto (ab, a + b).$$

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

Esercizio 11. Sia P l'insieme dei numeri interi pari e D quello dei numeri interi dispari. Si stabilisca una biezione tra:

1. $\mathbb{N}$ e $\mathbb{Z}$;

2. $\mathbb{N}_+$ e P;

3. $\mathbb{N}_+$ e D.

Esercizio 12. Siano X, Y, Z insiemi, $f \in Y^X$ e $g \in Z^Y$. Dimostrare se sono vere le seguenti:

1. $g \circ f$ iniettiva $\implies$ f iniettiva;

2. $g \circ f$ suriettiva $\implies$ f suriettiva;

3. $g \circ f$ iniettiva e f suriettiva $\implies$ g iniettiva;

4. $g \circ f$ suriettiva e g iniettiva $\implies$ f suriettiva.

Settimana 2 – Relazioni di equivalenza e Cardinalità

Esercizio 13. 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

1. una relazione riflessiva su $\{1,2,3,4\}$;
2. una relazione simmetrica;
3. una funzione da $\{1,2,3,4\}$ in $\{1,2,3,4\}$.

Esercizio 14. Si dica se le seguenti implicazioni valgano per relazioni R, S in generale

1. R, S simmetriche $\implies R \cup S$ simmetrica;
2. R, S simmetriche $\implies R \cap S$ simmetrica;
3. R, S transitive $\implies R \cup S$ transitiva;
4. R, S transitive $\implies R \cap S$ transitiva.

Esercizio 15. Consideriamo l'insieme $X := \{1,2,3\}$. Definire una relazione su X tale che

1. non sia nè riflessiva, nè simmetrica, nè transitiva;
2. sia riflessiva, simmetrica, ma non transitiva;
3. sia d'equivalenza.

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

Esercizio 16. Consideriamo su $X := \mathbb{R} \times \mathbb{R}$ la relazione $\approx$ così definita:

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

1. Provare che $\approx$ è una relazione di equivalenza su X.
2. Determinare un sistema di rappresentanti per $X/\approx$.

Esercizio 17. 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

1. $\approx$ è un'equivalenza su X;

2. $X/\approx$ è equipotente a $\mathbb{Z}$.

Esercizio 18. 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

1. $\approx$ è un'equivalenza su P;

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

Esercizio 19. 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

1. $\sim$ è una relazione d'equivalenza su $\mathbb{Q}$;

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

Per il *principio del buon ordinamento* ogni sottoinsieme non vuoto di $\mathbb{N}$ ha minimo.

Esercizio 20. Sia $X := \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$. Definiamo una relazione di equivalenza su X ponendo

$$\forall A,B \in X \quad A \sim B \iff \min A = \min(B).$$

Si dimostri che

1. $\sim$ è una relazione d'equivalenza su X;

2. $X/\sim$ è equipotente a $\mathbb{N}$.

Esercizio 21. Sia $\mathcal{R} \subset S \times S$ una relazione sull'insieme S. Consideriamo l'insieme

$$S/\mathcal{R} = \{[a]_\mathcal{R} \,|\, a \in S\} \subset \mathcal{P}(S)\,,$$

dove, per $a \in S$, denotiamo $[a]_\mathcal{R} = \{b \in S \,|\, (a,b) \in \mathcal{R}\} \subset S$. Per ciascuna delle seguenti affermazioni, dimostrarle o trovarne un controesempio:

(i) Se $\mathcal{R}$ è una relazione di equivalenza su S, allora $S/\mathcal{R}$ è una partizione di S.

(ii) Se $S/\mathcal{R}$ è una partizione di S, allora $\mathcal{R}$ è una relazione di equivalenza su S.

(iii) Se $\mathcal{R}$ è una relazione riflessiva, allora $S/\mathcal{R}$ ricopre S.

(iv) Se $\mathcal{R}$ è una relazione riflessiva e $S/\mathcal{R}$ è una collezione di insieme disgiunti, allora $\mathcal{R}$ è una relazione di equivalenza su S e $S/\mathcal{R}$ è una partizione di S.

Esercizio 22. Dato un insieme S ed una collezione di sottoinsiemi $\mathcal{P} \subset \mathcal{P}(S)$, consideriamo la seguente relazione su S:

$$\mathcal{R}_{\mathcal{P}} = \{(a,b) \in S \times S \,|\, (a,b) \in A \text{ per qualche } A \in \mathcal{P}\}\,.$$

Per ciascuna delle seguenti affermazioni, dimostrarle o trovarne un controesempio:

(i) Se $\mathcal{P}$ è una partizione di S, allora $\mathcal{R}_{\mathcal{P}}$ è una relazione di equivalenza su S.

(ii) Se $\mathcal{R}_{\mathcal{P}}$ è una relazione di equivalenza su S, allora $\mathcal{P}$ è una partizione di S.

(iii) Se $\mathcal{P}$ ricopre S, allora $\mathcal{R}_{\mathcal{P}}$ è una relazione riflessiva e simmetrica su S.

(iv) Se $\mathcal{R}_{\mathcal{P}}$ è una relazione transitiva e $\mathcal{P}$ ricopre S, allora $\mathcal{P}$ è una partizione di S e $\mathcal{R}_{\mathcal{P}}$ è una relazione di equivalenza su S.

Esercizio 23. Nel seguente esercizio costruiremo il campo $\mathbb{Q}$ dei numeri razionali a partire dall'insieme dei numeri interi $\mathbb{Z}$.

Assumeremo di sapere cosa sono i numeri interi e cosa vuol dire sommare e moltiplicare due numeri interi (ma NON sappiamo cosa vuol dire due numeri interi!)

1. Consideriamo l'insieme $\mathbb{Z} \times \mathbb{Z}^*$, dove $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$. Definiamo la seguente relazione $\sim$ su questo insieme

$$(a,b) \sim (c,d) \quad \Longleftrightarrow \quad ad = bc\,.$$

Dimostrare che $\sim$ è una relazione di equivalenza.

2. Consideriamo la partizione associata, ovvero l'insieme delle classi di equivalenza, che denotiamo

$$\mathbb{Q} \;=\; \mathbb{Z}\times\mathbb{Z}^*/\sim \;=\; \left\{ [(a,b)]_\sim \;\middle|\; a\in\mathbb{Z},\; b\in\mathbb{Z}^* \right\}.$$

Definiamo le seguenti operazioni di somma ($+_\mathbb{Q}$) e moltiplicazione ($\cdot_\mathbb{Q}$) su $\mathbb{Q}$:

$$\begin{aligned} [(a,b)]_\sim \,+_\mathbb{Q}\, [(c,d)]_\sim \;&=\; [(ad+bc,bd)]_\sim\,, \\ [(a,b)]_\sim \,\cdot_\mathbb{Q}\, [(c,d)]_\sim \;&=\; [(ac,bd)]_\sim\,. \end{aligned}$$

Dimostrare che queste due operazioni sono ben definite su $\mathbb{Q}$.

3. Dimostrare che $\mathbb{Q}$, insieme con le operazioni definite sopra, è un campo, ovvero: $+_\mathbb{Q}$ soddisfa le proprietà commutativa e associativa, esiste un elemento $\bar{0}\in\mathbb{Q}$ tale che $a+_\mathbb{Q}\bar{0}=a$ per ogni $a\in\mathbb{Q}$, e per ogni $a\in\mathbb{Q}$ esiste un unico elemento $b\in\mathbb{Q}$ tale che $a+_\mathbb{Q} b=\bar{0}$; $\cdot_\mathbb{Q}$ soddisfa le proprietà commutativa e associativa, esiste un elemento $\bar{1}\in\mathbb{Q}$ tale che $a\cdot_\mathbb{Q}\bar{1}=a$ per ogni $a\in\mathbb{Q}$, e per ogni $a\in\mathbb{Q}\backslash\{\bar{0}\}$ esiste un unico elemento $b\in\mathbb{Q}$ tale che $a\cdot_\mathbb{Q} b=\bar{1}$; le operazioni $+_\mathbb{Q}$ e $\cdot_\mathbb{Q}$ sono legate dalla proprietà distributiva.

(**Suggerimento:** pensare alla coppia (a,b) come al "numero" $\frac{a}{b}$).

Esercizio 24. Sia X un insieme infinito. Provare che $|X^X| = |\{0,1\}^X| = |\mathbb{N}^X|$.

Esercizio 25. 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. $\{U \,|\, U\subseteq\mathbb{R}^3,\; U \text{ è sottospazio di } \mathbb{R}^3\}$.

Settimana 3 – Introduzione alle strutture algebriche

Esercizio 26. 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 27. 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 28. 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 29. Sia G un gruppo e $H \subseteq G$. Dimostrare che sono equivalenti:

(i) H è un sottogruppo di G;

(ii) $H \neq \emptyset$ e per ogni $x, y \in H$ $xy^{-1} \in H$.

Esercizio 30. Sia A un anello e $H \subseteq A$. Dimostrare che sono equivalenti:

(i) H è un sottoanello di A;

(ii) $(H, +)$ è sottogruppo di $(A, +)$ e per ogni $x, y \in H$ $xy \in H$.

Sia G un gruppo e H un sottogruppo di G. Per ogni $x \in G$, definiamo $Hx := \{hx \,|\, h \in H\}$ e $xH := \{xH \,|\, h \in H\}$. H si definisce *sottogruppo normale* se

$$\forall x \in G \quad Hx = xH.$$

Definiamo su G la seguente relazione $\sim_H$:

$$\forall x, y \in G \quad x \sim_H y \quad \iff \quad xy^{-1} \in H.$$

Diremo che $\sim_H$ è *compatibile* con l'operazione di G se

$$\forall x, y, z, h \in G: \quad x \sim_H y \quad \text{e} \quad z \sim_H h \qquad \Longrightarrow \qquad xz \sim_H yh.$$

Esercizio 31. Poniamo $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, $G := \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \,|\, b \in \mathbb{Q},\ a, d \in \mathbb{Q}^*\}$ e $H := \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,|\, b \in \mathbb{Q}\}$. Dire se:

1. G è un gruppo rispetto all'usuale moltiplicazione tra matrici;
2. H è un sottogruppo di G eventualmente normale.

Esercizio 32. 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. $B := \{(3a, x) \,|\, a, x \in \mathbb{Z}\}$ è un sottoanello di A;
2. vale che per ogni $(a, x) \in A$ e $(b, y) \in B$ $(a, x) \cdot (b, y) \in B$.

Settimana 4 – Gli interi. Divisibilità e fattorizzazione in $\mathbb{Z}$

Esercizio 33. 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 34. Dimostrare che

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

Esercizio 35. Dimostrare che, per ogni numero intero dispari z, vale che $8 \mid z^2 - 1$.

Esercizio 36. Dimostrare che, per ogni $a \in \mathbb{Z}$ e per ogni $n \in \mathbb{N}_+$,

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

Esercizio 37. Dimostrare che, per ogni $a \in \mathbb{Z}$ e per ogni numero naturale dispari n,

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

Esercizio 38. 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 39. Dimostrare che

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

Esercizio 40. 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 41. Dimostrare che, per ogni $a, b \in \mathbb{Z}$, vale

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

Esercizio 42. Dimostrare che

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

Esercizio 43. 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 44. 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 45. 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 46. 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 47. Dimostrare che esistono infiniti numeri primi nell'insieme $\{3k+2 \mid k \in \mathbb{N}\}$.

Esercizio 48. Dimostrare che

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

Esercizio 49. 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 50. Sia $p \in \mathbb{P}$. Dimostrare che

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

Esercizio 51. Sia $a \in \mathbb{N}$. Dimostrare che

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

Settimana 5 – Numeri primi. Interi modulo n. Equazioni alle congruene. (E ancora su strutture algebriche).

Esercizio 52. Sia G un gruppo, e sia $H \subset G$ un sottogruppo. Consideriamo la seguente relazione su G:

$$x \overset{H}{\sim} u \iff y^{-1}x \in H$$

(i) Verificare che $\overset{H}{\sim}$ è una relazione di equivalenza.

(ii) Denotiamo con $G/H \subset \mathcal{P}(G)$ la partizione corrispondente. Dato $x \in G$, descrivere la sua classe di equivalenza $\bar{x} \in G/H$.

(iii) "Definiamo" una struttura di gruppo nell'insieme quoziente G/H prendendo come unità $\bar{1} \in G/H$, come prodotto di $\bar{x}$ e $\bar{y}$ l'elemento $\overline{xy} \in G/H$, e come inverso di $\bar{x}$ l'elemento $\overline{x^{-1}} \in G/H$. Determinare quali condizioni in H garantiscono che in questo modo si ottiene un gruppo.

(iv) Mostrare con un controesempio che l'insieme quoziente G/H non è sempre un gruppo.

Esercizio 53. Dimostrare che un numero dispari che è somma di due quadrati è sempre congruo a 1 modulo 4.

Esercizio 54. Al variare di $a = 0, 1, 2, ¨15$ 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 55. 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 56. Abbiamo un barattolo di lenticchie e sappiamo con certezza che il loro numero è compreso tra 500 e 1000. Se togliamo le lenticchie a due a due, a tre a tre, a quattro a quattro, a cinque a cinque, oppure a sei a sei, nel barattolo resta sempre una lenticchia. Se invece togliamo le lenticchie a gruppi di sette, non ne rimane nessuna. Quante lenticchie contiene il barattolo?

Esercizio 57. 1. Verificare che $(\mathbb{Z}/n)^* = \{\bar{a} \in \mathbb{Z}/n \,|\, MCD(a,n) = 1\}$ è l'insieme degli elementi invertibili di $\mathbb{Z}/n$.

2. La funzione di Eulero $\phi : \mathbb{N}\backslash\{0\} \to \mathbb{N}$ è definita da $\phi(n) = \#(\mathbb{Z}/n)^*$, ovvero $\phi(n)$ è il numero di elementi invertibili in $\mathbb{Z}/n$. Calcolare $\phi(n)$ nel caso in cui n sia primo, e nel caso in cui $n = pq$ è prodotto di due primi.

Esercizio 58. Dire, motivando la risposta, quali delle seguenti equazioni ammettono soluzioni intere:

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

Settimana 6 – Anelli, sottoanelli, ideali.

Esercizio 59. 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 60. 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 61. 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 62. 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 63. 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 64. 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 65. 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 66. Sia J un ideale di $\mathbb{Z}$. Fornire una descrizione esplicita dell'ideale $\sqrt{J}$ definito come nell'esercizio precedente.

Esercizio 67. 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 68. Provare che l'anello $\mathbb{Z}/\mathbb{Z}15$ ha due soli ideali non banali e che tali ideali sono massimali.

Esercizio 69. 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 $\ker f$.

Settimana 8 – Anello dei polinomi. Domini Euclidei.

Esercizio 70. 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 71. 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 72. 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 73. (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 74. Sia A l'anello che si ottiene a partire da $\mathbb{Z}[i]$ imponendo la relazione $1 + 3i = 0$ (ovvero $A = \mathbb{Z}[i]/(1 + 3i)$. Si dimostri che $A \simeq \mathbb{Z}/10$.

Esercizio 75. Ricordiamo che, dato un anello A ed un elemento $a \in A$, l'anello che si ottiene a partire da A ed "aggiungendo" $\sqrt{a}$ è, per definizione, $A[\sqrt{a}] = A[x]/(x^2 - a)$. Si dimosti che $\mathbb{Z}/5[\sqrt{3}]$ è un campo, mentre $\mathbb{Z}/11[\sqrt{3}]$ non è un campo.

Esercizio 76. 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 77. 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 78. Stabilire se i seguenti polinomi sono irriducibili in $\mathbb{Q}[x]$:

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

Esercizio 79. 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 80. 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 81. 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 82. 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.

Settimana 9 – Domini Euclidei, domini a ideali principali, e domini a fattorizzazione unica. Fattorizzazione di polinomi.

Esercizio 83. 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 84. 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 85. 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 86. Provare che $x^4 + 3x^3 + 2x + 4$ non è irriducibile in $(\mathbb{Z}/\mathbb{Z}5)[x]$.

Esercizio 87. 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 88. 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 89. 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 90. 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 91. 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 92. 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 93. 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 94. Sia p un numero primo. Dimostrare che, per ogni $n \geq 1$, il polinomio $x^n - p$ è irriducibile in $\mathbb{Z}[x]$.

Esercizio 95. 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:

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

(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 (2)) che $x^4 + 1$ è riducibile in $\mathbb{F}_p[x]$.

Settimana 10 – Fattorizzazione di polinomi e nell'anello $\mathbb{Z}[i]$. Moduli su un anello.

Esercizio 96. 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 97. 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 98. 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 99. 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 100. Descrivere l'anello quoziente $\mathbb{Z}[i]/(p)$ nei seguenti casi:

(a) $p = 2$,

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

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

Esercizio 101. In questo esercizio definiamo il modulo quoziente M/U di un A-modulo M per un sottomodulo $U \subset M$.

Definiamo su M la relazione di equivalenza $\sim$ data da: $u \sim v$ se e solo se $v - u \in U$.

1. Verificare che $\sim$ è una relazione di equivalenza.
2. Descrivere l'insieme quoziente $M/U = M/\sim$.
3. Definire sull'insieme quoziente M/U una struttura di modulo su A.
4. Dimostrare che la mappa quoziente $\pi : M \to M/U$ è un omomorfismo di anelli.

Esercizio 102. In questo esercizio dimostriamo il *Primo Teorema di Isomorfismo* per A-moduli:
Sia $\varphi : M \to N$ un omomorfismo di moduli su A. Dimostrare che esiste un unico isomorfismo di A-moduli $\bar{\varphi} : M/\ker(\varphi) \to \mathrm{Im}(\varphi)$ tale che $\bar{\varphi} \circ \pi = \varphi$ (dove $\pi : M \to M/\ker(\varphi)$ è la mappa quoziente).

Esercizio 103. In questo esercizio dimostriamo il *Secondo Teorema di Isomorfismo* per A-moduli:
Siano M un A-modulo e $U \subset M$ un sottomodulo.

1. Descrivere una corrispondenza biunivoca $\pi : \mathcal{U} \to \bar{\mathcal{U}}$ tra l'insieme $\mathcal{U}$ di tutti i sottomoduli V di M che contengono U, e l'insieme $\bar{\mathcal{U}}$ di tutti i sottomoduli di M/U.

2. Dato $V \in \mathcal{U}$, dimostrare che esste un isomorfismo "canonico" $M/V \simeq (M/U)/\pi(V)$.

Esercizio 104. In questo esercizio dimostriamo il *Terzo Teorema di Isomorfismo* per A-moduli:
Siano M un A-modulo e $U, v \subset M$ sottomoduli. Consideriamo i sottomoduli $U \cap V \subset M$ e $U + V = \{u + v \,|\, u \in U, v \in V\} \subset M$. Esiste un isomorfismo ''canonico" di A-moduli: $(U + V)/V \simeq U/(U \cap V)$.

Esercizio 105. Sia V lo spazio vettoriale sul cambo $\mathbb{K}$ di dimensione infinita, con base $\{v_1, v_2, \dots\}$. Consideriamo l'anello unitario non commutativo $A = \mathrm{End}(V)$. Dato $n \in \mathbb{N}$, definiamo $T_0, T_1, \dots, T_{n-1} \in A$ nel seguente modo:

$$T_i(v_k) = 0 \text{ se } k \not\equiv i \mod (n),$$
$$T_i(v_k) = v_{\frac{k-i}{n}} \text{ se } k \equiv i \mod (n).$$

(a) Dimostrare che $T_0, T_1, \dots, T_{n-1}$ formano una base di A (visto come A-modulo sinistro).

(b) Dedurre che valgono gli isomorfismi di A-moduli $A \simeq A^1 \simeq A^2 \simeq A^3 \simeq \dots$.

Settimana 11 – Moduli su un anello.

Esercizio 106. Determinare la struttura dei moduli su $\mathbb{Z}$ aventi come matrice di presentazione:

(a) $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$,

(b) $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$,

(c) $\begin{pmatrix} 2 & 0 & 0 \end{pmatrix}$,

(d) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$,

(e) $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$,

(f) $\begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix}$,

(g) $\begin{pmatrix} 2 & 4 \\ 1 & 4 \end{pmatrix}$.

Esercizio 107. Sia $M \subset \mathbb{Z}^3$ il sottogruppo abeliano generato da

$$\begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}, \quad \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}.$$

1. Trovare una base v_1, v_2, v_3 ed interi $1 < d_1 \mid \ldots \mid d_r$ tali che $d_1 v_1, \ldots, d_r v_r$ sia una base di M.
2. Determinare la struttura del gruppo quoziente $\mathbb{Z}^3/M$.

Esercizio 108. Sia M il sottomodulo di $\mathbb{Z}^2$ generato da

$$\begin{pmatrix} 3 \\ 2 \end{pmatrix}, \quad \begin{pmatrix} 4 \\ -5 \end{pmatrix}.$$

Determinare la struttura di $\mathbb{Z}^2/M$.

Esercizio 109. Sia $M \subset \mathbb{Z}^2$ il sottogruppo generato da

$$\begin{pmatrix} 5 \\ 12 \end{pmatrix}, \quad \begin{pmatrix} 3 \\ 10 \end{pmatrix}, \quad \begin{pmatrix} 2 \\ 14 \end{pmatrix}.$$

Determinare una base di M.

Esercizio 110. Sia $M \subset \mathbb{Z}^3$ il sottomodulo generato da

$$\begin{pmatrix} 4 \\ 2 \\ 2 \end{pmatrix}, \quad \begin{pmatrix} 6 \\ 6 \\ 3 \end{pmatrix}, \quad \begin{pmatrix} 5 \\ 5 \\ 5 \end{pmatrix}.$$

(a) Quanti elementi ha M?

(b) Quanti elementi ha $\mathbb{Z}^3/M$?

Esercizio 111. Sia $a+bi \in \mathbb{Z}[i]$, e siano $d = MCD(a,b)$ e $D = (a^2+b^2)/d$. Dimostrare che esiste un isomorfismo di gruppi abeliani $\mathbb{Z}[i]/(a+bi) = \mathbb{Z}/d \times \mathbb{Z}/D$.
(*Suggerimento:* considerare l'isomorpfismo di $\mathbb{Z}$-moduli $\phi : \mathbb{Z}[i] \to \mathbb{Z}^2$ dato da $\phi(x+iy) = (x,y)$. Trovare un sistema di generatori per $\phi((a+ib)) \subset \mathbb{Z}^2$.)

Esercizio 112. Sia A la matrice di un omomorfismo $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ tra due moduli liberi, relativamente a due basi fissate.

(a) Mostrare che φ è iniettivo se e solo se $\det(A) \neq 0$.

(b) Mostrare che φ è suriettivo se e solo se $\det(A) = \pm 1$.

(c) Dedurre che se $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ è suriettivo, allora è anche iniettivo, mentre non è vero il viceversa.

Esercizio 113. Elencare tutti i gruppi abeliani di cardinalità 2310 a meno di isomorfismo.

Esercizio 114. Sia A una matrice quadrata $n \times n$ a coefficienti interi con determinante $\det(A) > 0$. Mostrare che il gruppo quoziente $\mathbb{Z}^n/A\mathbb{Z}^n$ ha cardinalità pari a $\det(A)$.