ESERCIZI - Algebra 1, a.a. 2024/25 (Ilaria Damiani/Flaminio Flamini)

1) Siano A e B due anelli, $f : A \to B$ un omomorfismo di anelli, $X \subseteq A$ un sottoinsieme; dimostrare che

$$f^{-1}(f(X)) = X + ker(f) = \{x + y | x \in X,\ f(y) = 0\}.$$

2) Siano A e B due anelli, $f : A \to B$ un omomorfismo di anelli, $I \subseteq B$ un ideale e $\pi : B \to B/I$ la proiezione sul quoziente; dimostrare che $\pi \circ f$ è suriettiva se e solo se $f(A) + I = B$.

3) Sia A un anello: un elemento $z \in A$ si dice centrale se $za = az\ \forall a \in A$; l'insieme $Z(A) = \{z \in A | za = az\ \forall a \in A\}$ si chiama centro di A.

i) $Z(A)$ è un sottoanello di A? è commutativo?

ii) $Z(A)$ è un ideale di A?

4) Determinare tutti gli ideali dell'anello $\mathbf{Z}/30\mathbf{Z}$ e dire quali tra questi sono primi e quali sono massimali.

5) Siano $I = (10), J = (15) \subseteq \mathbf{Z}$; dire se $\mathbf{Z}/(I \cap J) \cong \mathbf{Z}/I \times \mathbf{Z}/J$.

6) Sia A un anello e siano $I, J \subseteq A$ ideali; provare che $I \cup J$ è un ideale di A se e solo se $I \subseteq J$ oppure $J \subseteq I$.

7) Fare un esempio di un anello A e di due ideali I e J di A tali che $I \cup J$ sia un ideale.

8) Fare un esempio di un anello A tale che $\forall I, J \subseteq A$ ideali si abbia $I \cup J$ ideale.

9) Fare un esempio di un anello A e di due ideali I e J di A tali che $I \cup J$ non sia un ideale.

10) Sia K un campo finito e sia $f : K \to K$ un omomorfismo di campi. Provare che f è un isomorfismo.

11) Siano A un anello e $I \subseteq A$ un ideale. Dimostrare che A/I è commutativo $\Leftrightarrow xy - yx \in I\ \forall x, y \in A$.

12) In $\mathbf{Z}[x]$ si consideri l'ideale $I = (5, x)$. Decidere se si tratta di un ideale principale.

13) Sia A un anello commutativo e siano $x \in A$ nilpotente, $u \in A^*$; dimostrare che:

i) ux è nilpotente;
ii) $1 + x \in A^*$;
iii) $u + x \in A^*$;
iv) è vero che se $v \in A^*$ allora $u - v$ è nilpotente?

14) Sia A un anello commutativo e sia

$$\mathcal{n} = \{x \in A | x \text{ nilpotente}\} = \{x \in A | \exists n > 0 \text{ tale che } x^n = 0\}.$$

i) Dimostrare che $\mathcal{n}$ è un ideale di A;
ii) dimostrare che $A/\mathcal{n}$ è privo di nilpotenti diversi da zero;
iii) dimostrare che se $I \subseteq A$ è un ideale primo allora $\mathcal{n} \subseteq I$;
iv) trovare esempi in cui $\mathcal{n} \neq \{0\}$ e $A/\mathcal{n}$ non è un dominio di integrità;
v) trovare esempi in cui $\mathcal{n} \neq \{0\}$ e $A/\mathcal{n}$ è un dominio di integrità ma non un campo;
vi) trovare esempi in cui $\mathcal{n} \neq \{0\}$ e $A/\mathcal{n}$ è un campo.

15) Sia A un anello e sia $D = \{x \in A | \exists y \neq 0 \text{ tale che } xy = 0\}$. Dire se D è un ideale di A.

16) Sia A un anello commutativo e supponiamo che $A^* = \{1\}$.
(a) Dimostrare che $-1 = 1$.
(b) Dimostrare che $x + x = 0$ per ogni $x \in A$.
(c) Dimostrare che la mappa $f : A \to A$ data da $f(x) = x^2$ è un omomorfismo di anelli.
(d) Dimostrare che f è iniettiva. È sempre suriettiva?

17) Sia $A \neq \{0\}$ un anello tale che $a^2 = a \ \forall a \in A$.
i) Provare che $car(A)$=2.
ii) Provare che A è commutativo.
iii) Trovare esempi di anelli che abbiano la proprietà descritta.

18) Sia $\mathbb{R}$ il campo dei numeri reali.
(a) Dimostrare che l'unico omomorfismo di anelli $\mathbb{Q} \to \mathbb{Q}$ è l'identità.
(b) Determinare tutti gli omomorfismi di anelli $\mathbb{Q} \to \mathbb{Z}$ e $\mathbb{Q} \to \mathbb{R}$.
(c) Dimostrare che l'unico omomorfismo di anelli $\mathbb{R} \to \mathbb{R}$ è l'identità.(Sugg: usare la parte (d))
(d) Dimostrare: per $x, y \in \mathbb{R}$ si ha che $x > y$ se e solo se esiste $z \in \mathbb{R}^*$ con $x - y = z^2$.

19) In $\mathbb{R}^2$ si ponga $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \cdot (c, d) = (ac, bd)$. Dimostrare che $(\mathbb{R}^2, +, \cdot)$ è un anello commutativo non isomorfo a $\mathbb{C}$.

20) Sia $A = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a, b \in \mathbb{R}\}$; provare che $A \subseteq \mathcal{M}_{2\times 2}(\mathbb{R})$ è un sottoanello e che $A \cong \mathbb{C}$.

21) Sia $A = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a, b \in \mathbb{Z}_3 \right\}$.

(a) Provare che A è un campo con 9 elementi.

(b) È vero che $(A, +)$ è un gruppo ciclico?

(c) Provare che l'applicazione $\varphi : A \to A$ definita da $\varphi(x) = x^3 \ \ \forall x \in A$ è un isomorfismo diverso dall'identità.

22) Sia $A = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a, b \in \mathbb{Z}_5 \right\}$.

Dire se A sia un anello, se sia commutativo, se sia un dominio di integrità, se sia un campo.

23) Siano A e B due domini di integrità tali che $Q(A) \cong Q(B)$; si può dedurre che $A \cong B$? se si ha l'ulteriore condizione che $A \subseteq B$ si può concludere che $A = B$?

24) Sia K un campo e sia $A = K[x, y]/(x^2y)$: in ognuno dei casi seguenti studiare l'ideale I, dire se si tratta di un ideale primo, massimale, principale e studiare il quoziente A/I:

$I = (\overline{x})$; $(\overline{x^2})$; $(\overline{y})$; $(\overline{y^2})$; $(\overline{xy})$; $(\overline{x^2y})$; $(\overline{xy^2})$; $(\overline{x^2y, xy^2})$; $(\overline{x}, \overline{y})$; $(\overline{x+1}, \overline{y+1})$.

A ha altri ideali oltre quelli studiati sopra?

25) Siano K un campo e $A = K[x, y]/(x^2, y^2)$.

i) Provare che A non è un dominio di integrità e calcolare $dim_K A$;

ii) determinare i divisori dello zero, gli elementi nilpotenti e gli elementi invertibili di A;

iii) dimostrare che A possiede un unico ideale primo e un unico ideale massimale;

iv) provare che se $I \neq (0)$ è un ideale di A allora $\overline{xy} \in I$;

v) determinare tutti gli ideali di A;

vi) per ogni ideale I di A descrivere A/I.

26) Sia K un campo; per ciascuno dei casi seguenti dire se X sia un sottoanello o un ideale di $K[x]$; nel caso sia un ideale studiare $K[x]/X$:

i) $X = \{\sum_{i\geq 0} a_i x^i \in K[x] | a_0 = 0\}$;

ii) $X = \{\sum_{i\geq 0} a_i x^i \in K[x] | a_1 = 0\}$;

iii) $X = \{\sum_{i\geq 0} a_i x^i \in K[x] | a_2 = 0\}$;

iv) $X = \{\sum_{i\geq 0} a_i x^i \in K[x] | a_i = 0 \ \forall i \text{ pari}\}$;

v) $X = \{\sum_{i\geq 0} a_i x^i \in K[x] | a_0 = i = 0 \ \forall i \text{ dispari}\}$;

27) Sia K un campo e si considerino l'anello $A = K[x]$ e il campo $F = K(x)$ (campo dei quozienti di A).

i) Dimostrare che esiste una (unica) estensione $\overline{deg} : F \setminus \{0\} \to \mathbb{Z}$ del grado $deg : A \setminus \{0\} \to \mathbb{N}$ tale che $\overline{deg}(fg) = \overline{deg}(f)\overline{deg}(g) \ \forall f, g \in F \setminus \{0\}$.

ii) $(F, \overline{deg})$ è un dominio euclideo?

28) Siano $A = \mathbf{Q}[x, y]$, $B = \mathbf{Q}[x, y]/(x^2 + 2x + 2)$, $f = x^2y^2 - 2x - 2$.

i) Dimostrare che A e B sono domini a fattorizzazione unica.

ii) Dimostrare che f è irriducibile in A.

iii) Dimostrare che f non è irriducibile in B e determinarne i fattori irriducibili.

29) Sia $\mathcal{C}^0(\mathbb{R})$ l'anello delle funzioni continue di $\mathbb{R}$ in $\mathbb{R}$ con le usuali operazioni di somma e prodotto e per $x_0 \in \mathbb{R}$ sia $I_{x_0} = \{f \in \mathcal{C}^0(\mathbb{R}) | f(x_0) = 0\}$.

i) Dimostrare che $\mathcal{C}^0(\mathbb{R})$ non è un dominio di integrità.

ii) dimostrare che I_{x_0} è un ideale di $\mathcal{C}^0(\mathbb{R})$;

iii) I_{x_0} è un ideale primo? è un ideale massimale?

iv) provare che I_{x_0} non è un ideale principale (suggerimento: data $f \in I_{x_0}$ provare che $|f|$ e $\sqrt{|f|} \in I_{x_0}$, ma che $\sqrt{|f|} \notin (f)$).

30) Sia $\mathcal{C}^\infty(\mathbb{R}) \subseteq \mathcal{C}^0(\mathbb{R})$ il sottoanello delle funzioni derivabili infinite volte con derivate continue e per $x_0 \in \mathbb{R}$ sia $J_{x_0} = \{f \in \mathcal{C}^\infty(\mathbb{R}) | f(x_0) = 0\}$.

i) Dimostrare che $\mathcal{C}^\infty(\mathbb{R})$ non è un dominio di integrità.

ii) dimostrare che J_{x_0} è un ideale di $\mathcal{C}^\infty(\mathbb{R})$;

iii) J_{x_0} è un ideale primo? è un ideale massimale?

iv) provare che J_{x_0} è un ideale principale (suggerimento: provare che la funzione $x \mapsto x - x_0$ genera J_{x_0}).

31) Sia $\mathcal{C}^0(\mathbb{R})$ l'anello delle funzioni continue di $\mathbb{R}$ in $\mathbb{R}$ con le usuali operazioni di somma e prodotto e per $x_0 \in \mathbb{R}$ sia $I_{x_0} = \{f \in \mathcal{C}^0(\mathbb{R}) | f(x_0) = 0\}$.

i) Dimostrare che I_{x_0} è un ideale di $\mathcal{C}^0(\mathbb{R})$;

ii) determinare $\mathcal{C}^0(\mathbb{R})/I_{x_0}$;

iii) se $x_1 \in \mathbb{R}$ determinare $\mathcal{C}^0(\mathbb{R})/(I_{x_0} \cap I_{x_1})$.

32) Sia K un campo; dire se $K[[x]]$ è un dominio euclideo.

33) Siano $A \subseteq B$ due domini.

i) Dire se A a fattorizzazione unica $\Rightarrow$ B a fattorizzazione unica;

ii) Dire se B a fattorizzazione unica $\Rightarrow$ A a fattorizzazione unica.

34) Siano $A \subseteq B$ due domini di integrità. Dimostrare che B euclideo $\not\Rightarrow A$ euclideo e che A euclideo $\not\Rightarrow B$ euclideo.

35) Sia $A = \mathbb{Z}[x]/(2x-1)$.
i) Provare che A è un dominio di integrità;
ii) provare che A ha caratteristica zero;
iii) determinare il campo dei quozienti di A;
iv) provare che $\forall a \in A\ \exists m \in \mathbb{Z}, n \in \mathbb{N}$ tali che $a = \overline{mx^n}$;
v) dimostrare che $2 \in A^*$ e che $A = \{m2^n | m, n \in \mathbb{Z}\}$;
vi) determinare A^* e $A^* \cap \mathbb{Z}$;
vii) determinare $\{a \in A | a \text{ irriducibile}\} \cap \mathbb{N}$;
viii) dimostrare che A è un dominio a fattorizzazione unica e che

$$(\{a \in A | a \text{ irriducibile}\}/\sim) \simeq \{\overline{p} \in A | p \in \mathbb{Z} \text{ primo tale che } p \geq 3\},$$

dove $\sim$ è la relazione di equivalenza definita da $a \sim b \Leftrightarrow \exists u \in A^*$ tale che $b = ua$;
ix) dimostrare che A è un dominio euclideo.

36) Sia A un sottoanello di $\mathbb{Q}$.
i) Dimostrare che esiste un sottoinsieme P_A di $\{p \in \mathbb{Z}_+ | p \text{ primo}\}$ tale che $A = \left\{ \frac{a}{\prod_{i=1}^{h} p_i^{r_i}} \middle| a \in \mathbb{Z},\ p_i \in P_A,\ h, r_i \in \mathbb{N} \right\}$.
ii) Determinare A^*.
iii) Dimostrare che A è un dominio euclideo e trovarne gli irriducibili.
iv) Dimostrare che $A \mapsto P_A$ definisce una corrispondenza biunivoca tra $\{A \subseteq \mathbb{Q} \text{ sottoanello}\}$ e $\mathcal{P}(\{p \in \mathbb{Z}_+ | p \text{ primo}\})$.

37) Sotto quali condizioni $a+ib, c+id \in \mathbb{Z}[i]$ sono uguali a meno di invertibili? Sotto quali condizioni $a+ib, a-ib$ sono uguali a meno di invertibili?

38) Trovare il massimo comun divisore tra $2+i$ e $2-i$ in $\mathbb{Z}[i]$.

39) Calcolare $MCD(4+3i, 13+i)$ in $\mathbb{Z}[i]$.

40) Calcolare l'inverso di tutti gli elementi non nulli di $\mathbb{Z}[i]/(3)$.

41) Determinare gli elementi non invertibili di $\mathbb{Z}[i]/(5)$.

42) Siano $a, b \in \mathbb{Z}$ primi tra loro. Dimostare che $\mathbb{Z}[i]/(a+ib) \cong \mathbb{Z}/(a^2+b^2)$.

43) Calcolare la cardinalità e la caratteristica dell'anello $\mathbb{Z}[i]/(6+3i)$.

44) Sia A un anello e siano $a, b \in A$. a e b si dicono *associati*, o *uguali a meno di invertibili* (e si scrive $a \sim b$) se esiste $u \in A^*$ tale che $b = ua$.

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

ii) Esibire un insieme di rappresentanti per $\sim$ nei casi seguenti:

$$A = \mathbb{Z}, \quad \mathbb{Z}[i], \quad \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}[x]/(10x-1);$$

$$A = K, \quad K[x], \quad K[x, x^{-1}], \quad K[[x]]$$

dove K è un campo.

45) Determinare le soluzioni in $\mathbb{Z}$ dell'equazione $X^2+1 = Y^3$. Sia (x, y) una soluzione.

(a) Dimostrare che x è un intero pari;

(b) Dimostrare che gli elementi $x+i$ e $x-i$ di $\mathbb{Z}[i]$ hanno MCD uguale a 1;

(c) Far vedere che $x+i$ è il cubo di un elemento $a+bi \in \mathbb{Z}[i]$;

(d) Concludere che $(x, y) = (0, 1)$.

46) Sia $v : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ la funzione definita nel modo seguente:

$$v(n) = [log_2(n)] = \text{parte intera di } log_2(n),$$

cioè $2^{v(n)} \leq n < 2^{v(n)+1}$.
Dimostrare che $(\mathbb{Z}, v)$ è un dominio euclideo.
In particolare concludere che su un anello possono esistere più di una valutazione euclidea.

47) Siano A un dominio di integrità, $v, V : A \setminus \{0\} \to \mathbb{N}$ funzioni tali che

$$\forall a, b \in A \text{ con } b \neq 0 \ \exists q, r \in A \text{ tali che } a = bq + r \text{ e } \begin{cases} r = 0 \\ \text{oppure} \\ v(r) < v(b), \end{cases}$$

e

$$V(a) = min\{v(ax) | x \in A \setminus \{0\}\}.$$

Dimostrare che (A, V) è un dominio euclideo.

48) Sia A un dominio di integrità e si definiscano sottoinsiemi A_n di A $(n \in \mathbb{N})$ nel modo seguente:

$$A_0 = \{0\}, \quad A_{n+1} = \{0\} \cup \{b \in A | (b) + A_n = A\}.$$

Dimostrare che:

i) $A_1 = \{0\} \cup A^*$.

ii) $A_n \subseteq A_{n+1}\ \forall n \in \mathbb{N}$.

iii) se (A, v) è un dominio euclideo allora $\cup_{n\in\mathbb{N}} A_n = A$.

iv) viceversa se $\cup_{n\in\mathbb{N}} A_n = A$ allora la funzione

$$A \setminus \{0\} \ni a \mapsto min\{n \in \mathbb{N} | a \in A_n\} \in \mathbb{N}$$

è una valutazione euclidea.

v) se esiste $n \in \mathbb{N}$ tale che $A_{n+1} = A_n \neq A$ allora non esiste valutazione euclidea su A.

49) Sia $A = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ il minimo sottoanello di $\mathbb{C}$ che contiene $\frac{1+\sqrt{-19}}{2}$.

i) Dimostrare che $A \cong \mathbb{Z}[x]/(x^2 - x + 5)$.

ii) Dimostrare che non esistono omomorfismi di anelli $f : A \to \mathbb{Z}/2\mathbb{Z}$ o $f : A \to \mathbb{Z}/3\mathbb{Z}$; equivalentemente non esiste $I \subseteq A$ ideale tale che $A/I \cong \mathbb{Z}/2\mathbb{Z}$ oppure $A/I \cong \mathbb{Z}/3\mathbb{Z}$.

iii) Dimostrare che la funzione $A \ni z \mapsto z\bar{z} = |z|^2 \in \mathbb{R}$ ha valori in $\mathbb{N}$.

iv) Dimostrare che $A^* = \{\pm 1\}$.

v) Dimostrare che $\{z \in A | (z) + (\{0\} \cup A^*) = A\} = A^*$.

vi) Concludere che A non è un dominio euclideo.

*vii) Dimostrare che A è un dominio a ideali prinicipali.

* v. Appunti di Algebra di Schoof oppure Appunti di Algebra di Stumbo.

50) Si chiama anello delle funzioni aritmetiche l'insieme

$$\mathcal{A} = \{f : \mathbb{Z}_+ \to \mathbb{C}\}$$

con somma $+$ e prodotto $*$ definiti da:

$$(f + g)(n) = f(n) + g(n), \quad (f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

i) Dimostrare che effettivamente $\mathcal{A}$ è un anello ($*$ si chiama prodotto di convoluzione): qual è l'elemento neutro del prodotto?

ii) Dimostrare che $\mathcal{A}$ è commutativo ed è un dominio di integrità.

iii) Determinare gli elementi invertibili di $\mathcal{A}$.

iv) Una funzione $f : \mathbb{Z}_+ \to \mathbb{C}$ si dice *moltiplicativa* se $f \neq 0$ e

$$f(mn) = f(m)f(n) \text{ per ogni } m, n > 0 \text{ tali che } (m, n) = 1.$$

Dimostrare che $\{f : \mathbb{Z}_+ \to \mathbb{C} | f \text{ è moltiplicativa}\}$ è un sottogruppo di $\mathcal{A}^*$.

v) Siano $e, \mathbb{1}, I, d, \varphi \in \mathcal{A}$ definite da:

$$e(n) = \delta_{n,0},\ \mathbb{1}(n) = 1,\ I(n) = n,\ d(n) = \#\{d \in \mathbb{Z}_+ | d|n\},\ \varphi(n) = \#(\mathbb{Z}_n)^*.$$

Determinare $\mathbb{1} * \mathbb{1}$; provare che $\varphi * \mathbb{1} = I$; determinare $\mathbb{1}^{-1}$.

[Notazione: $\mathbb{1}^{-1}$ si denota μ e si chiama funzione di Möbius.]

51) Siano K un campo, $n \in \mathbb{N}$, e $A_n = K[x,y]/(x^2 - y^n)$.

i) Dire per quali n A_n è un dominio;

ii) dire per quali n A_n è un dominio a fattorizzazione unica;

iii) sia n tale che A_n è un dominio: determinare $Q(A_n)$;

iv) sia n tale che A_n non è un dominio: trovare i divisori di zero e gli elementi nilpotenti di A_n.

52) Sia K un campo e $\forall n \in \mathbb{N}$ si definisca l'anello A_n nel modo seguente: $A_0 = K$, $n > 0 \Rightarrow A_n = A_{n-1}[x_n]$;

i) osservare che si ha $A_0 \subseteq A_1 \subseteq ... \subseteq A_n \subseteq ...$;

ii) sia $A = \cup_{n\in\mathbb{N}} A_n$; dimostrare che esiste un'unica struttura di anello su A tale che l'inclusione $A_n \hookrightarrow A$ sia un'omomorfismo di anelli $\forall n \in \mathbb{N}$; l'anello A si indica con $A = K[x_1, ..., x_n, ...]$;

iii) provare che $K[x_1, ..., x_n, ...]$ è un anello;

iv) $K[x_1, ..., x_n, ...]$ è un dominio? è un dominio a fattorizzazione unica? è un campo?

v) esibire ideali primi, ideali massimali, ideali principali e ideali non principali in $K[x_1, ..., x_n, ...]$.

vi) dimostrare che $K[x_1, ..., x_n, ...]/(x_{n+1}, x_{n+2}, ...) \cong K[x_1, ..., x_n]$;

vii) $\forall n \in \mathbb{N}$ sia $B_n \subseteq K[x_1, ..., x_n, ...]$ il sottoanello generato da $\{x_{n+1}, x_{n+2}, ...\}$; provare che $B_n = K[x_{n+1}, x_{n+2}, ...] \cong K[x_1, ..., x_n, ...]$ $\forall n \in \mathbb{N}$, che $A = B_0 \supseteq B_1 \supseteq ...$ e che $\cap_{n\in\mathbb{N}} B_n = K$.

53) Siano K un campo, $I \subseteq K[x_1, ..., x_n, ...]$ l'ideale generato da $\{x_n^2 - x_{n+1} | n \in \mathbb{Z}_+\}$; dimostrare che $K[x_1, ..., x_n, ...]/I \cong K[x_1]$.

54) Siano K un campo, $I \subseteq K[x_1, ..., x_n, ...]$ l'ideale generato da $\{x_n - x_{n+1}^2 | n \in \mathbb{Z}_+\}$, $A = K[x_1, ..., x_n, ...]/I$ e $\pi : K[x_1, ..., x_n, ...] \to A$ la proiezione sul quoziente.

i) dimostrare che $\forall n \in \mathbb{Z}_+$ $\pi(K[x_1, ..., x_n]) \cong K[t]$;

ii) dimostrare che A è un dominio di integrità;

iii) siano $a_1, ..., a_N \in A$; dimostrare che l'ideale $(a_1, ..., a_N)$ è principale;

iv) dimostrare che l'ideale generato da $\{\pi(x_1), ..., \pi(x_n), ...\}$ non è principale e dedurne che A non è un dominio a ideali principali;

v) confrontare i risultati dei punti iii) e iv);

vi) Dimostrare che $\pi(x_1)$ non è prodotto di irriducibili in A.

55) Dimostrare che $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

56) Dimostrare che $(\mathbb{Z}/9\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$ ed esibire un generatore.

57) Sia $p > 0$ primo, e siano $G = \mathbb{Z}/p^2\mathbb{Z}$ e $H =< p >$.
Dimostrare che $H \cong \mathbb{Z}/p\mathbb{Z}$ e che $G/H \cong \mathbb{Z}/p\mathbb{Z}$.

58) Sia $p > 0$ primo, e siano $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $\{0\} < H < G$ un sottogruppo non banale.
Dimostrare che $H \cong \mathbb{Z}/p\mathbb{Z}$ e che $G/H \cong \mathbb{Z}/p\mathbb{Z}$.

59) Siano G, $\tilde{G}$ due gruppi abeliani, $H \leq G$, $\tilde{H} \leq \tilde{G}$ sottogruppi tali che $H \cong \tilde{H}$ e $G/H \cong \tilde{G}/\tilde{H}$.
Dimostrare con un esempio che non necessariamente si ha $G \cong \tilde{G}$.

60) Sia $p > 0$ primo, e siano $G = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $H =< (0,1) >$, $K =< (p,0) >$. Dimostrare che $H \cong K \cong \mathbb{Z}/p\mathbb{Z}$ e che $G/H \ncong G/K$.

61) Sia G un gruppo tale che $x^2 = e$ per ogni $x \in G$. Dimostrare che G è abeliano e determinarne la struttura.

62) Dato un gruppo abeliano Γ e un numero primo $p > 0$ sia

$$\Gamma_p = \{x \in \Gamma | \exists r \geq 0 \text{ tale che } o(x) = p^r\}.$$

i) Dimostrare che Γ_p è un sottogruppo di Γ.

ii) Siano G e H due gruppi abeliani e $f : G \to H$ un omomorfismo di gruppi. Dimostrare che per ogni $p > 0$ primo si ha $f(G_p) \subseteq H_p$.

iii) Siano G e H due gruppi abeliani finiti; dimostrare che le restrizioni inducono una corrispondenza biunivoca

$$Hom_{Gr}(G,H) \to \prod_{p \text{ primo}} Hom_{Gr}(G_p, H_p).$$

63) Sia $n > 1$. Dimostrare che $Aut_{Gr}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ e determinare $Aut_{An_1}(\mathbb{Z}/n\mathbb{Z})$.

64) Descrivere il gruppo $Aut_{An_1}((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}))$.

65) Descrivere il gruppo $Aut_{Gr}((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}))$.

66) Descrivere i gruppi $Aut_{An_1}(\mathbb{Z} \times \mathbb{Z})$ e $Aut_{Gr}(\mathbb{Z} \times \mathbb{Z})$.

67) Siano $p \in \mathbb{Z}$ primo dispari, $r > 0$.
Risolvere la congruenza $x^2 \equiv 2x \ (mod\ p^r)$.
Risolvere la congruenza $x^2 \equiv 2x \ (mod\ 2^r)$.

Più in generale: risolvere la congruenza $x^2 \equiv 2x \ (mod\ n)$ ($n > 1$ intero).

68) Dimostrare che $2^{2^n} + 1$ è primo per $n = 0, 1, 2, 3, 4$.
Questa osservazione è alla base della **congettura** di Fermat: $2^{2^n} + 1$ è primo per ogni $n \in \mathbb{N}$.
Dimostrare che $641 | 2^{2^5} + 1$ e che la congettura di Fermat è **falsa**.

69) Risolvere la congruenza $x^4 \equiv_{17} 1$; descrivere l'anello $(\mathbb{Z}/17\mathbb{Z})[x]/(x^4 - 1)$.

70) Risolvere la congruenza $x^4 \equiv_{19} 1$, descrivere l'anello $(\mathbb{Z}/19\mathbb{Z})[x]/(x^4 - 1)$.

71) Risolvere la congruenza $x^5 \equiv x \ (mod\ 5)$ e fattorizzare il polinomio $x^5 - x \in (\mathbb{Z}/5\mathbb{Z})[x]$.
Dimostrare che tutte le funzioni di $\mathbb{Z}/5\mathbb{Z}$ in $\mathbb{Z}/5\mathbb{Z}$ sono polinomiali, cioè che l'omomorfismo di anelli $Fun : (\mathbb{Z}/5\mathbb{Z})[x] \to (\mathbb{Z}/5\mathbb{Z})^{\mathbb{Z}/5\mathbb{Z}}$ definito da $Fun(p)(\alpha) = p(\alpha)$ è suriettivo.

72) Sia K un campo e sia $Fun : K[x] \to K^K$ la funzione definita nel modo seguente: $Fun(p)(\alpha) = p(\alpha)\ \forall \alpha \in K$.
$Fun(p)$ è detta la funzione definita dal polinomio p e una funzione di K in K si dice polinomiale se appartiene all'immagine di Fun.
i) Dimostrare che se $\#K = \infty$ allora Fun è iniettiva non suriettiva.
ii) Dimostrare che se $\#K < \infty$ allora Fun è suriettiva non iniettiva: determinarne il nucleo.

73) Sia $p \in \mathbb{Z}$ primo. Dimostrare che per ogni $a \in \mathbb{Z}$ si ha $a^p \equiv a \ (mod\ p)$.
Questo risultato si chiama "piccolo teorema di Fermat".

74) Sia A un anello commutativo di caratteristica $p > 0$, con $p \in \mathbb{Z}$ primo. Dimostrare che la funzione $A \ni a \mapsto a^p \in A$ è un omomorfismo di anelli.

75) Siano $n, a \in \mathbb{Z}$ primi tra loro e sia φ la funzione di Eulero ($\varphi(n) = \#\{r \in \mathbb{N} | r < n,\ (r, n) = 1\}$).
i) Dimostrare che $a^{\varphi(n)} \equiv 1 \ (mod\ n)$.
ii) Discutere al variare di n se esista $m < \varphi(n)$ tale che $a^m \equiv 1 \ (mod\ n)$ per ogni $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

76) Siano p un primo dispari, $r > 0$. Dimostrare che $(\mathbb{Z}/p^r\mathbb{Z})^*$ è un gruppo ciclico e che $(\mathbb{Z}/2p^r\mathbb{Z})^* \cong (\mathbb{Z}/p^r\mathbb{Z})^*$. $(\mathbb{Z}/4p^r\mathbb{Z})^*$ è ciclico?

77) Sia $r > 2$. Dimostrare che $(\mathbb{Z}/2^r\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$: è un gruppo ciclico?

78) Classificare il gruppo $(\mathbb{Z}/5880\mathbb{Z})^*$ tramite le potenze di primi e tramite divisori elementari.

79) Il gruppo $(\mathbb{Z}/15\mathbb{Z})^*$ è ciclico? Descrivere tale gruppo per potenze di primi e per divisori elementari.

80) Il gruppo $(\mathbb{Z}/50\mathbb{Z})^*$ è ciclico? Descrivere tale gruppo per potenze di primi e per divisori elementari.

81) Determinare i numeri $n > 1$ tali che $(\mathbb{Z}/n\mathbb{Z})^*$ sia ciclico.

82) Siano p primo, G gruppo abeliano tale che $\#G = p^3$, $x, y \in G$ tali che $G =< x, y >$ e $o(x) = o(y) = p^2$.
i) Classificare G.
ii) Determinare $x', y' \in G$ tali che $G =< x' > \oplus < y' >$.
iii) Fare un esempio di G, x, y, x', y' con tali proprietà.

83) Sia G un gruppo tale che $\#G = 4$. Dimostrare che G è abeliano. Determinare tutti i gruppi di cardinalità 4 a meno di isomorfismo.

84) Determinare tutti i gruppi abeliani di cardinalità 8 a meno di isomorfismo.

85) Determinare tutti i gruppi abeliani di cardinalità 6 a meno di isomorfismo.

86) Determinare tutti i gruppi abeliani di cardinalità 600 a meno di isomorfismo.

87) Siano H e K due sottogruppi di $\mathbb{Q}$ diversi da $\{0\}$. Dimostrare che $H \cap K \neq \{0\}$. Dedurre che $\mathbb{Q}$ non è somma diretta di sottogruppi non banali (un gruppo abeliano con questa proprietà si dice indecomponibile). Osservare che $\mathbb{Q}$ non è un gruppo ciclico e concludere che $\mathbb{Q}$ non è somma diretta di gruppi ciclici.

88) Sia $\Gamma \leq \mathbb{Q}/\mathbb{Z}$ un sottogruppo finitamente generato. Dimostrare che Γ è un gruppo ciclico; più precisamente dimostrare che esiste $n > 0$ tale che $\Gamma =< \frac{1}{n} > \cong \mathbb{Z}/n\mathbb{Z}$.

89) Sia $p > 0$ primo e sia $(\mathbb{Q}/\mathbb{Z})_p = \{a \in \mathbb{Q}/\mathbb{Z} | \exists r \in \mathbb{N} \text{ tale che } o(a) = p^r\}$. Domostrare che tutti i sottogruppi non banali di $(\mathbb{Q}/\mathbb{Z})_p$ sono ciclici e che $(\mathbb{Q}/\mathbb{Z})_p$ non è ciclico.

90) Siano $p > 0$ primo, $r > 0$ e $G = \mathbb{Z}/p^r\mathbb{Z}$. Dimostrare che G è indecom-

ponibile, cioè che $G = H \oplus K \Rightarrow H = \{0\}$ oppure $K = \{0\}$.
Dimostrare che se $\mathbb{Z}/n\mathbb{Z}$ è indecomponibile allora n è la potenza di un primo.

91) Siano K un campo e $K(x)$ il campo delle funzioni razionali in una variabile, cioè il campo dei quozienti di $K[x]$. Si considerino i gruppi moltiplicativi K^* e $K(x)^*$ rispettivamente di K e di $K(x)$.

i) Dimostrare che K^* è un sottogruppo di $K(x)^*$ e che $K(x)^*/K^*$ è somma diretta di gruppi ciclici.

ii) Caso $K = \mathbb{C}$: determinare un isomorfismo esplicito tra $\mathbb{C}(x)^*/\mathbb{C}^*$ e $\oplus_{\alpha\in\mathbb{C}}\mathbb{Z}$.

iii) Dimostrare che l'inclusione $\mathbb{R}[x] \hookrightarrow \mathbb{C}[x]$ induce un omomorfismo iniettivo di gruppi $R(x)^*/\mathbb{R}^* \to \mathbb{C}(x)^*/\mathbb{C}^*$; descrivere la composizione

$$R(x)^*/\mathbb{R}^* \to \mathbb{C}(x)^*/\mathbb{C}^* \to \oplus_{\alpha\in\mathbb{C}}\mathbb{Z}.$$

92) Sia A un dominio a fattorizzazione unica e sia Q il campo dei quozienti di A.

i) Dimostrare che il gruppo Q^*/A^* è somma diretta di gruppi ciclici.

ii) Confrontare il punto i) con il risultato dell'esercizio precedente.

iii) Studiare il caso $A = K[[x]]$ e dimostrare che in questo caso Q^*/A^* è ciclico.

***

Si consigliano tutti gli esercizi sulle **Congruenze** proposti nel libro **Chirivì-Del Corso-Dvornicich**, Esercizi scelti di Algebra, vol. 1, pagine 77-83. Ovviamente anche qualsiasi altro esercizio è utile.