ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 27/01/2026 ore 10.00 - aula 1

1-i) Descrivere le proprietà dell'anello $\mathbb{Z}/7\mathbb{Z}$.

1-ii) Descrivere la struttura del gruppo $(\mathbb{Z}/7\mathbb{Z})^*$.

1-iii) Risolvere il sistema di congruenze

$$(*) \qquad \begin{cases} 3x \equiv 2 \pmod 7 \\ 3^x \equiv 2 \pmod 7. \end{cases}$$

1-iv) Determinare il numero di interi positivi x minori di 100 che risolvono il sistema $(*)$.

2) Siano:
G un gruppo abeliano;
$\sigma : G \to G$ un omomorfismo di gruppi tale che $\sigma^2 = id_G$;
$K = \{g \in G | \sigma(g) = g\}$ l'insieme dei punti fissi di σ.
Dimostrare che:

i) σ è un automorfismo di G e K è un sottogruppo di G; descrivere $\sigma\big|_K$.

ii) σ induce un omomorfismo di gruppi $\bar{\sigma} : G/K \ni gK \mapsto \sigma(g)K \in G/K$; $\bar{\sigma}$ è un automorfismo?

iii) se G è finito di cardinalità dispari allora l'unico punto fisso di $\bar{\sigma}$ è l'elemento neutro di G/K.

iv) Esibire un esempio di G gruppo abeliano e $\sigma \in Aut(G)$ con $\sigma^2 = id_G$ tali che K sia un sottogruppo non banale di G; descrivere G/K e $\bar{\sigma}$.

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

$$v(n) = m \Leftrightarrow 2^m \leq |n| < 2^{m+1}$$

e siano $a, b, q, r \in \mathbb{Z}$ elementi tali che

$$(*) \qquad a = bq + r.$$

i) Dimostrare che v è una valutazione euclidea su $\mathbb{Z}$.

ii) Se $a = 2$ e $b = 3$ determinare q, r tali che $(*)$ sia una divisione euclidea in $(\mathbb{Z}, v)$.

iii) Mostrare un esempio di divisione euclidea $(*)$ in $(Z, |\cdot|)$ che non è una divisione euclidea in $(\mathbb{Z}, v)$.

iv) Dimostrare che se $(*)$ è una divisione euclidea in $(\mathbb{Z}, v)$ allora $(*)$ è una divisione euclidea anche in $(Z, |\cdot|)$.

ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 27/01/2026 ore 10.00 - aula 29A

SOLUZIONI

1-i) $\mathbb{Z}/7\mathbb{Z}$ è un quoziente di $\mathbb{Z}$, quindi è un anello commutativo unitario; $\mathbb{Z}/7\mathbb{Z}$ ha 7 elementi; poiché 7 è un numero primo $\mathbb{Z}/7\mathbb{Z}$ è un campo.

1-ii) $(\mathbb{Z}/7\mathbb{Z})^*$ ha 6 elementi; è il gruppo moltiplicativo di un campo finito, quindi è un gruppo ciclico; dunque $(\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$.
Oltre all'unità (l'elemento 1) che ha ordine 1, in $(\mathbb{Z}/7\mathbb{Z})^*$ ci sono due elementi di ordine 6 (ciascuno dei quali genera tutto il gruppo), due elementi di ordine 3 e un elemento di ordine 2 (l'elemento $-1 = 6$). Osserviamo che $3^3 = 27 = -1 \neq 1$, quindi 3 ha ordine 6 ed è un generatore di $(\mathbb{Z}/7\mathbb{Z})^*$.

1-iii) Il punto 1-ii) implica che la congruenza $3^x \equiv a \pmod 7$ è risolubile per ogni a primo con 7 e la soluzione è definita modulo 6.
Poiché $3^2 = 9 \equiv 2 \pmod 7$, la congruenza $3^x \equiv 2 \pmod 7$ equivale alla congruenza $x \equiv 2 \pmod 6$.
Inoltre l'inverso di 3 in $\mathbb{Z}/7\mathbb{Z}$ è 5, quindi la congruenza $3x \equiv 2 \pmod 7$ equivale alla congruenza $x \equiv 5 \cdot 3x \equiv 5 \cdot 2 = 10 \equiv 3 \pmod 7$.
Dunque il sistema $(*)$ equivale al sistema di congruenze lineari

$$\begin{cases} x \equiv 3 \equiv -4 \pmod 7 \\ x \equiv 2 \equiv -4 \pmod 6. \end{cases}$$

-4 è chiaramente una soluzione di questo sistema, e dal fatto che 6 e 7 sono primi tra loro segue che la soluzione del sistema $(*)$ è definita modulo 42, ed è quindi $x \equiv -4 \pmod{42}$.

1-iv) Abbiamo visto che le soluzioni del sistema $(*)$ sono tutti i numeri della forma $-4+42k$ al variare di k in $\mathbb{Z}$. La condizione $0 < -4+42k < 100$ equivale alle condizioni $42k > 4$ e $42k < 104$, cioè $k > 0$ e $k \leq 2$, dunque ci sono esattamente due soluzioni di $(*)$ nell'intervallo dei numeri interi da 1 a 99.

2)

i) Per ogni $g \in G$ si ha $g = \sigma^2(g) = \sigma(\sigma(g))$, quindi $g \in Im(\sigma)$, cioè σ è suriettiva; d'altra parte se $g \in Ker(\sigma)$ si ha $g = \sigma(\sigma(g)) = \sigma(e) = e$, quindi il nucleo di σ è banale, cioè σ è iniettiva.
Ne segue che σ è un omomorfismo di gruppi iniettivo e suriettivo, quindi è invertibile, cioè è un automorfismo.

Alternativamente: $\sigma^2 = id$ implica che σ è inverso sinistro e destro di σ, cioè che σ è invertibile (con inverso σ).
Se $g \in K$, cioè se $\sigma(g) = g$, si ha $\sigma(g^{-1}) = \sigma(g)^{-1} = g^{-1}$, quindi $g^{-1} \in K$; se inoltre anche $\sigma(g') = g'$ si ha $\sigma(gg') = \sigma(g)\sigma(g') = gg'$, quindi $gg' \in K$. Dunque K è chiuso rispetto all'inverso e al prodotto, cioè è un sottogruppo di G.
Se $g \in K$ si ha che $\sigma(g) = g$, quindi $\sigma\big|_K = id_K$.

ii) Poiché G è un gruppo abeliano e K è un sottogruppo, G/K è un gruppo. Poiché $\sigma(K) \subseteq K$ (più precisamente $\sigma(K) = K$), K è contenuto nel nucleo della composizione $G \ni g \mapsto \sigma(g) \mapsto \sigma(g)K \in G/K$, che dunque induce un omomorfismo di gruppi $\bar{\sigma} : G/K \to G/K$.
Ovviamente $\bar{\sigma}^2 = id_{G/K}$, quindi per il punto i) $\bar{\sigma}$ è un automorfismo.

iii) Osserviamo innanzitutto che l'ipotesi implica che anche G/K è un gruppo finito di cardinalità dispari; ne segue che tutti i suoi elementi hanno ordine dispari.
Sia $x \in G/K$ tale che $\bar{\sigma}(x) = x$ e sia $g \in G$ tale che $x = gK$; allora $gK = x = \bar{\sigma}(x) = \sigma(g)K$, cioè $g^{-1}\sigma(g) \in K$.
Dunque $\sigma(g^{-1}\sigma(g)) = g^{-1}\sigma(g)$, cioè $\sigma(g)^{-1}g = g^{-1}\sigma(g)$, cioè $g^2 = \sigma(g^2)$.
Questo significa che $g^2 \in K$, cioè $x^2 = g^2K = K$, quindi $o(x)|2$; ma x ha ordine dispari, quindi $o(x) = 1$, cioè x è l'elemento neutro di G/K.

iv) Sia H un gruppo abeliano non banale e siano $G = H \times H$, $\sigma : G \to G$ la funzione definita da $\sigma(h_1, h_2) = (h_2, h_1)$. Ovviamente G è un gruppo abeliano e σ è un omomorfismo di gruppi con $\sigma^2 = id$.
Abbiamo che $K = \{(h_1, h_2) \in G | h_1 = h_2\} = \{(h, h) | h \in H\}$.
Osserviamo che se $h \in H \setminus \{e_H\}$ allora $(e, h) \in G$, $(e, h) \notin K$ (dunque $K \neq G$) ed $e_G \neq (h, h) \in K$ (dunque $K \neq \{e_G\}$), quindi K è un sottogruppo non banale di G.
Sia $f : G \to H$ la funzione definita da $f((h_1, h_2)) = h_1 h_2^{-1}$.
Ovviamente f è suriettiva ($h = f((h, e))$ per ogni $h \in H$); poiché H è abeliano f è un omomorfismo di gruppi; il suo nucleo è K. Dunque f induce un isomorfismo $\bar{f} : G/K \to H$, cioè $G/K \cong H$.
Infine osserviamo che se $g = (h_1, h_2)$ abbiamo

$$g\sigma(g) = (h_1, h_2)(h_2, h_1) = (h_1 h_2, h_2 h_1) \in K$$

quindi $\bar{\sigma}(gK) = (gK)^{-1}$ per ogni $g \in G$, cioè $\bar{\sigma}(x) = x^{-1}$ per ogni $x \in G/K$.

3)

i) Siano $a, b \in \mathbb{Z} \setminus \{0\}$. Vogliamo provare che $v(ab) \geq v(a)$.

Questo è vero perché

$$v(a) = n \Rightarrow |a| \geq 2^n \Rightarrow |ab| \geq |a| \geq 2^n \Rightarrow v(ab) \geq n = v(a).$$

Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Vogliamo provare che esistono $q, r \in \mathbb{Z}$ tali che $a = bq + r$ e $v(r) < v(b)$.
Sappiamo che esistono $q, r \in \mathbb{Z}$ tali che $a = bq + r$ e $|r| \leq \frac{|b|}{2}$ (cioè un rappresentante r di a in $\mathbb{Z}/b\mathbb{Z}$ può essere scelto in modo tale che $|r| \leq \frac{|b|}{2}$). Con tale scelta abbiamo

$$v(b) = n \Rightarrow |b| < 2^{n+1} \Rightarrow |r| \leq \frac{|b|}{2} < \frac{2^{n+1}}{2} = 2^n \Rightarrow v(r) < n = v(b).$$

Ne segue che $(\mathbb{Z}, v)$ è un dominio euclideo.

ii) $2 = 3 \cdot 1 - 1$; se poniamo $q = 1$, $r = -1$ abbiamo quindi $2 = 3q + r$; d'altra parte $2^0 \leq 1 < 2^1 \leq 3 < 2^2$ quindi $v(-1) = 0 < 1 = v(3)$.

iii) $2 = 3 \cdot 0 + 2$ è una divisione euclidea in $(\mathbb{Z}, |\cdot|)$ perché $|2| < |3|$ ma non in $(\mathbb{Z}, v)$ perché $v(2) = 1 = v(3)$, quindi $v(2) \not< v(3)$.

iv) Siano $b \neq 0$ e $a = bq + r$ una divisione euclidea in $(\mathbb{Z}, v)$, cioè $r = 0$ oppure $v(r) < v(b)$; se $r = 0$ allora $a = bq + r$ è una divisione euclidea in $(\mathbb{Z}, |\cdot|)$; se $v(r) < v(b)$ allora

$$|r| < 2^{v(r)+1} \leq 2^{v(b)} \leq |b|,$$

quindi anche in questo caso $a = bq + r$ è una divisione euclidea in $(\mathbb{Z}, |\cdot|)$.