ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 23/09/2025 ore 10.00 - aula 1

1) Siano:
$\sim \subseteq (\mathbb{Z}\times\mathbb{Z})\times(\mathbb{Z}\times\mathbb{Z})$ la relazione definita nel modo seguente:

$$(x,y)\sim(x',y') \Leftrightarrow xy = x'y';$$

$+', \cdot : (\mathbb{Z}\times\mathbb{Z})\times(\mathbb{Z}\times\mathbb{Z}) \to (\mathbb{Z}\times\mathbb{Z})$ le operazioni definite nel modo seguente:

$$(x,y) +' (z,w) = (x+z, y+w), \quad (x,y)\cdot(z,w) = (xz, yw).$$

i) Dimostrare che $\sim$ è una relazione di equivalenza e descrivere il quoziente di $\mathbb{Z}\times\mathbb{Z}$ per $\sim$.

ii) Al variare di $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ descrivere la classe di equivalenza di (x,y) e calcolarne la cardinalità.

iii) Dire se $+'$ e $\cdot$ siano compatibili con $\sim$.

iv) Si denoti con X il quoziente $(\mathbb{Z}\times\mathbb{Z})/\sim$ e sia $* : X\times X \to X$ l'operazione indotta su X da $+'$ (se $+'$ induce un'operazione su X) oppure da $\cdot$ (se $\cdot$ induce un'operazione su X). Dire se $(X,*)$ sia un gruppo.

2) Siano $a,b\in\mathbb{Z}$ e si consideri l'ideale $I_{a,b} = (x^2+a, b) \subseteq \mathbb{Z}[x]$.

i) Determinare la cardinalità e la caratteristica dell'anello quoziente $\mathbb{Z}[x]/I_{a,b}$.

ii) Sia $b\neq 0$; dimostrare che $I_{a,b}$ è primo se e solo se è massimale.
Determinare un elemento $a\in\mathbb{Z}$ tale che $I_{a,0}$ sia primo ma non massimale.

iii) Determinare gli interi a tali che $I_{a,7}$ è un ideale primo: per questi valori di a quali sono gli elementi invertibili di $\mathbb{Z}[x]/I_{a,7}$?

iv) Determinare gli ideali primi, gli elementi invertibili e gli elementi nilpotenti dell'anello $\mathbb{Z}[x]/I_{0,5}$.

3) Siano:
G il gruppo $(\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}, +)$;
per ogni p primo, $G_p = \{x\in G | \exists n\geq 0$ tale che $o(x) = p^n\}$;
A l'anello $(\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}, +, \cdot)$.

i) Descrivere G_p e $Aut_{Gr}(G_p)$ per $p=3$, $p=5$, $p=2$.

ii) Dimostrare che $Aut_{Gr}(G) \cong Aut_{Gr}(G_2)\times Aut_{Gr}(G_3)\times Aut_{Gr}(G_5)$.

iii) Dimostrare che $Aut_{An_1}(A) \leq Aut_{Gr}(G)$ e che $\#Aut_{An_1}(A) = 2$.

iv) Determinare esplicitamente l'automorfismo $\varphi : A\to A$ tale che $\varphi \neq id_A$.

ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 23/09/2025 ore 10.00 - aula 29A

SOLUZIONI

1)
i) Sia $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ la funzione definita da $f(x, y) = xy$. Abbiamo che

$$(x, y) \sim (x', y') \Leftrightarrow xy = x'y' \Leftrightarrow f(x, y) = f(x', y'),$$

quindi $\sim$ è la relazione di equivalenza indotta da f e in particolare è una relazione di equivalenza.
Poiché f è suriettiva (per ogni $x \in \mathbb{Z}$ si ha $x = f(x, 1)$), $(\mathbb{Z}, f)$ è il quoziente di $(\mathbb{Z} \times \mathbb{Z})$ per $\sim$.

ii) Le classi di equivalenza sono gli insiemi $f^{-1}(xy)$ al variare di (x, y) in $\mathbb{Z} \times \mathbb{Z}$ o equivalentemente sono gli insiemi $f^{-1}(n)$ al variare di n in $\mathbb{Z}$.
$f^{-1}(0)$ consiste di tutte le coppie (x, y) tali che $xy = 0$, cioè tali che $x = 0$ oppure $y = 0$; dunque

$$f^{-1}(0) = (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z})$$

ed è numerabile perché $\mathbb{N} \times \{0\} \subseteq (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z}) \subseteq \mathbb{Z} \times \mathbb{Z}$.
Se $n \neq 0$ la coppia (x, y) appartiene a $f^{-1}(n)$ se e solo se $x|n$ e in tal caso y è univocamente determinato ($y = \frac{n}{x}$). Quindi

$$f^{-1}(n) = \left\{ \left(d, \frac{n}{d} \right) \middle| d|n \right\} \quad \text{e} \quad \#f^{-1}(n) = \#\{d \in \mathbb{Z} | d|n\}.$$

Più precisamente, sia $n \in \mathbb{Z} \setminus \{0\}$; allora esistono unici $p_1, ..., p_h$ primi positivi, $r_1, ..., r_h > 0$ ed $\varepsilon \in \{\pm 1\}$ tali che

$$n = \varepsilon p_1^{r_1} ... p_h^{r_h};$$

poiché $d|n$ se e solo se $d = \pm p_1^{s_1} ... p_h^{s_h}$ con $0 \leq s_i \leq r_i$ per ogni $i = 1, ..., h$, si ha che

$$\#f^{-1}(n) = 2(r_1 + 1)...(r_h + 1).$$

iii) $+'$ non è compatibile con $\sim$ perché

$$(0, 0) \sim (0, 1) \sim (1, 0),$$

$$(0, 0) +' (0, 0) = (0, 0), \quad (0, 1) +' (1, 0) = (1, 1),$$

$$(0, 0) \not\sim (1, 1).$$

$\cdot$ è compatibile con $\sim$. Infatti

$$(x,y) \sim (x',y'),\ (z,w) \sim (z',w') \Rightarrow$$
$$\Rightarrow xy = x'y', zw = z'w' \Rightarrow$$
$$\Rightarrow xyzw = x'y'z'w' \Rightarrow (xz, yw) \sim (x'z', y'w') \Rightarrow$$
$$\Rightarrow (x,y) \cdot (z,w) \sim (x',y') \cdot (z',w').$$

iv) $+'$ non induce un'operazione sul quoziente perché non è compatibile con $\sim$, mentre $\cdot$ è compatibile con $\sim$ dunque induce un'operazione sul quoziente (l'operazione denotata $*$).
L'operazione $* : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ è l'usuale prodotto definito in $\mathbb{Z}$: infatti $n*m = k$ significa $k = f((n,1)\cdot(m,1)) = f(nm,1) = nm$, cioè $n * m = nm$.
In particolare $(X,*)$ non è un gruppo, perché in $\mathbb{Z}$ non esiste l'inverso moltiplicativo per esempio di 0.

2) Si osservi preliminarmente che $\mathbb{Z}[x]/I_{a,b} \cong (\mathbb{Z}/(b))[x]/(x^2+a)$ e che un sistema di rappresentanti è $\{c_1x + c_0 | c_0, c_1 \in \mathbb{Z}/(b)\}$.

i) Dall'osservazione preliminare segue subito che l'omomorfismo di anelli $\mathbb{Z} \to \mathbb{Z}[x]/I_{a,b}$ ha come nucleo l'ideale generato da b e che quindi la caratteristica di $\mathbb{Z}[x]/I_{a,b}$ è $|b|$; segue anche che $\mathbb{Z}[x]/I_{a,b}$ è numerabile se $b = 0$ (perché in corrispondenza biunivoca con $\mathbb{Z}\times\mathbb{Z}$) e che se $b \neq 0$ si ha $\#(\mathbb{Z}[x]/I_{a,b}) = b^2$.

ii) Se $b \neq 0$ l'anello commutativo $\mathbb{Z}[x]/I_{a,b}$ è finito, quindi è un dominio se e solo se è un campo; ne segue che $I_{a,b} \subseteq \mathbb{Z}[x]$ è un ideale primo se e solo se è massimale.
Se $b = 0$ si ha $\mathbb{Z}[x]/I_{a,b} = \mathbb{Z}[x]/(x^2+a)$; osserviamo che per $a = 1$ abbiamo quindi $\mathbb{Z}[x]/I_{a,0} = \mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$ che è un dominio ma non un campo; quindi $I_{1,0}$ è primo ma non massimale.

iii) Poiché $\mathbb{Z}/7\mathbb{Z}$ è un campo, dall'osservazione preliminare segue che $\mathbb{Z}[x]/I_{a,7}$ è un dominio se e solo se il polinomio $x^2 + a$ è irriducibile in $(\mathbb{Z}/7\mathbb{Z})[x]$, cioè se e solo se $-a$ non è un quadrato in $\mathbb{Z}/7\mathbb{Z}$. Ora i quadrati in $\mathbb{Z}/7\mathbb{Z}$ sono $0^2 = 0$, $(\pm1)^2 = 1$, $(\pm2)^2 = 4$,$(\pm3)^2 = 2$, quindi $I_{a,7}$ è un ideale primo di $\mathbb{Z}[x]$ se e solo se $a \neq 0, -1, -4, -2$, cioè se e solo se $a = 1, 2, 4$.
Per tali valori di a l'anello $\mathbb{Z}[x]/I_{a,7}$ è un campo, quindi i suoi elementi invertibili sono tutti e soli gli elementi diversi da zero.

iv) Nell'anello $\mathbb{Z}[x]/I_{0,5}$ si ha $x^2 = 0$ quindi x è nilpotente e appartiene a tutti gli ideali primi. D'altra parte l'ideale (x) è massimale perché

$$(\mathbb{Z}[x]/I_{0,5})/(x) \cong (\mathbb{Z}/5\mathbb{Z})[x]/(x) \cong \mathbb{Z}/5\mathbb{Z}$$

che è un campo, quindi (x) è l'unico ideale primo (e anche l'unico ideale massimale).
Tutti gli elementi della forma c_1x sono nilpotenti, perché multipli di un elemento nilpotente in un anello commutativo; viceversa tutti gli elementi della forma $c_1x + c_0$ con $c_0 \neq 0$ sono invertibili, altrimenti apparterrebbero ad un ideale non banale (quindi ad un ideale massimale), mentre non appartengono all'unico ideale massimale (x).
Poiché un elemento non può essere contemporaneamente invertibile e nilpotente, $\mathbb{Z}[x]/I_{0,5}$ è l'unione (disgiunta) dei suoi elementi nilpotenti (i multipli di x) e dei suoi elementi invertibili (quelli che non sono multipli di x).

3) Osserviamo preliminarmente che per il teorema cinese del resto la funzione

$$\Psi : \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

definita da $\Psi(a, b) = (a \bmod 3, a \bmod 2, b \bmod 2, b \bmod 5)$ (che per brevità scriviamo $\Psi(a, b) = (a, a, b, b)$) definisce un isomorfismo di anelli, quindi anche di gruppi.

i) Dall'osservazione preliminare segue subito che $G_3 \cong \mathbb{Z}/3\mathbb{Z}$, $G_5 \cong \mathbb{Z}/5\mathbb{Z}$, $G_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Gli elementi di G_3 sono quelli della forma $(2a, 0)$, gli elementi di G_5 sono quelli della forma $(0, 2b)$, gli elementi di G_2 sono quelli della forma $(3a, 5b)$.
Dalla descrizione di G_p segue quella di $Aut_{Gr}(G_p)$:

$$Aut_{Gr}(G_3) \cong Aut_{Gr}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^* = \{\pm 1\} \cong (\mathbb{Z}/2\mathbb{Z}, +),$$

$$Aut_{Gr}(G_5) \cong Aut_{Gr}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z}, +),$$

$$Aut_{Gr}(G_2) \cong Aut_{Gr}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z});$$

ora ogni automorfismo di G_2 fissa l'elemento neutro e induce quindi per restrizione una permutazione di $G_2 \setminus \{(0, 0)\}$, cioè un elemento di $\mathcal{S}_3$; questo significa che $Aut_{Gr}(G_2)$ è isomorfo a un sottogruppo di $\mathcal{S}_3$.
D'altra parte per ogni $g \neq h$ in $G_2 \setminus \{(0, 0)\}$ la funzione

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ni (a, b) \mapsto g^a h^b \in G_2$$

determina un ben definito isomorfismo di gruppi, quindi $Aut_{Gr}(G_2)$ ha 6 elementi; ne segue che

$$Aut_{Gr}(G_2) \cong \mathcal{S}_3.$$

ii) Poiché gli elementi di G_p sono quelli che hanno ordine una potenza di p e l'ordine di un elemento è conservato dagli isomorfismi di gruppo, ogni

automorfismo di G mappa isomorficamente ogni G_p in se stesso; quindi abbiamo un ben definito omomorfismo iniettivo di gruppi

$$Aut_{Gr}(G) \ni \varphi \mapsto (\varphi\big|_{G_2}, \varphi\big|_{G_3}, \varphi\big|_{G_5}) \in Aut_{Gr}(G_2) \times Aut_{Gr}(G_3) \times Aut_{Gr}(G_5).$$

Viceversa per la proprietà universale del prodotto di gruppi ogni terna $(\varphi_2, \varphi_3, \varphi_5)$ con $\varphi_p \in Aut_{Gr}(G_p)$ determina un automorfismo di gruppi φ di $G_2 \times G_3 \times G_5 \cong G$ in sé tale che $\varphi\big|_{G_p} = \varphi_p$ per ogni p.
Dunque $Aut_{Gr}(G) \cong Aut_{Gr}(G_2) \times Aut_{Gr}(G_3) \times Aut_{Gr}(G_5)$.

iii) Un automorfismo dell'anello A è una funzione biunivoca di $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ in sé che conserva somma e prodotto, quindi in particolare è una funzione biunivoca di $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ in sé che conserva la somma, cioè è un automorfismo del gruppo G. Dunque $Aut_{An_1}(A) \subseteq Aut_{Gr}(G)$ e la tesi segue poiché l'operazione rispetto alla quale questi due insiemi sono gruppi è per entrambi la stessa (la composizione).
$\varphi \in Aut_{An_1}(A)$ se e solo se $\tilde{\varphi} = \Psi\varphi\Psi^{-1} \in Aut_{An_1}(\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z})$, e questo avviene se e solo se

$$\tilde{\varphi}\big|_{\mathbb{Z}/3\mathbb{Z}}, \quad \tilde{\varphi}\big|_{\mathbb{Z}/5\mathbb{Z}}, \quad \tilde{\varphi}\big|_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}}$$

sono automorfismi di anelli.
Ora per ogni $n \in \mathbb{Z}$ esiste un unico omomorfismo (automorfismo) di anelli $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$: $Aut_{An_1}(\mathbb{Z}/n\mathbb{Z}) = \{id\}$.
D'altra parte un automorfismo di anelli di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ conserva

$$(1,1) = (1,0) + (0,1),$$

quindi induce (ed è determinato da) una permutazione di $\{(1,0),(0,1)\}$, quindi $Aut_{An_1}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ ha al più 2 elementi. Poiché la funzione

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ni (a,b) \mapsto (b,a) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

non è l'identità ed è un automorfismo di anelli, si ha

$$\#Aut_{An_1}(A) = \#Aut_{An_1}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = 2.$$

iv) Sia $\varphi \in Aut_{An_1}(A) \setminus \{id\}$; per il punto iii) si ha che

$$\Psi\varphi\Psi^{-1}(a,a',b,b') = (a,b,a',b'),$$

cioè che

$$\Psi\varphi(a,b) = (a,b,a,b),$$

o ancora equivalentemente che

$$\varphi(a,b) = (x,y) \quad \text{con} \quad (a,b,a,b) = (x,x,y,y),$$

che significa

$$\begin{cases} x \equiv a \pmod 3 \\ x \equiv b \pmod 2 \end{cases} \quad \text{e} \quad \begin{cases} y \equiv a \pmod 2 \\ y \equiv b \pmod 5. \end{cases}$$

Ricordiamo che $a, x \in \mathbb{Z}/6\mathbb{Z}$ e $b, y \in \mathbb{Z}/10\mathbb{Z}$.
Considerando le identità di Bézout $3 \cdot 1 + 2 \cdot (-1) = 1$ e $5 \cdot 1 + 2 \cdot (-2) = 1$, troviamo

$$x = -2a + 3b, \quad y = 5a - 4b.$$

Dunque

$$\varphi(a,b) = (-2a + 3b, 5a - 4b).$$