ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 05/09/2025 ore 10.00 - aula 1

1) Siano:
A un anello commutativo unitario;
$* : A \times A \to A$ l'operazione definita da $x * y = x + y - 2xy \ \forall x, y \in A$;
$\Gamma = \{u \in A | u^2 = u\}$.

i) Dimostrare che $*$ è associativa e ha un elemento neutro: quale?

ii) Dimostrare che Γ è chiuso rispetto a $*$ e che $(\Gamma, *)$ è un gruppo.

iii) Dire tutto quello che si riesce a dire di $(\Gamma, *)$ nel caso in cui A è un dominio di integrità e nel caso in cui $A = \mathbb{Z}/6\mathbb{Z}$.

iv) Se $\#\Gamma < \infty$ determinare $d_1, ..., d_r > 0$ tali che

$$(\Gamma, *) \cong \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}.$$

Che cosa si può dire della struttura del gruppo $(\Gamma, *)$ se $\#\Gamma = \infty$?

2) Si consideri l'anello $A = \mathbb{C}[x, y]/(x^2 - y^2 - 1)$.

i) Dimostrare che $A \cong \mathbb{C}[z, z^{-1}]$.

ii) Dire se x^2-y^2-1 sia irriducibile in $\mathbb{C}[x,y]$ e se x e y siano invertibili in A.

iii) Dimostrare che A è un dominio euclideo.

iv) Determinare $q \in A$, $r \in A^*$ (cioè $q, r \in A$ con r invertibile) tali che

$$(\Diamond) \qquad x = qy + r$$

e spiegare perché $(\Diamond)$ è una divisione euclidea (in A) di x per y.

3) Si considerino:
gli insiemi $\mathbb{N}$ e $\{0, 1\}$ con l'ordinamento standard $\leq$;
l'ordinamento lessicografico $\leq'$ su $\mathbb{N} \times \{0, 1\}$;
l'ordinamento lessicografico $\leq''$ su $\{0, 1\} \times \mathbb{N}$.

i) Dimostrare che $(\mathbb{N} \times \{0, 1\}, \leq') \cong (\mathbb{N}, \leq)$ (isomorfismo di insiemi ordinati).

ii) Dire se $(\{0, 1\} \times \mathbb{N}, \leq'')$ sia ben ordinato.

iii) Dimostrare che, rispetto all'ordinamento $\leq''$, $\{0\} \times \mathbb{N} \subseteq \{0, 1\} \times \mathbb{N}$ è limitato superiormente e non ha massimo.

iv) Dire se $(\mathbb{N} \times \{0, 1\}, \leq')$ e $(\{0, 1\} \times \mathbb{N}, \leq'')$ siano insiemi ordinati isomorfi.

MEMO
Dati due insiemi ordinati $(X, \leq_X)$ e $(Y, \leq_Y)$ si chiama ordinamento lessicografico su $X \times Y$ l'ordinamento $\preceq$ definito nel modo seguente:

$$(x, y) \preceq (x', y') \Leftrightarrow \begin{cases} x \leq_X x' \text{ e } x \neq x' \\ \text{oppure} \\ x = x' \text{ e } y \leq_Y y'. \end{cases}$$

ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 08/07/2025 ore 10.00 - aula 29A

SOLUZIONI

1) Osserviamo preliminarmente che $*$ è un'operazione commutativa:

$$x + y - 2xy = y + x - 2yx.$$

i) Se e è elemento neutro di $(A, *)$ si deve avere in particolare

$$0 = e * 0 = e + 0 - 2e \cdot 0 = e,$$

quindi $e = 0$; d'altra parte $x * 0 = x + 0 - 2x \cdot 0 = x \ \forall x \in A$, quindi 0 è elemento neutro di $(A, *)$.
Inoltre

$$(x * y) * z =$$

$$(x + y - 2xy) * z = x + y - 2xy + z - 2(x + y - 2xy)z =$$

$$= x + y + z - 2(xy + xz + yz) + 4xyz$$

che è un'espressioe simmetrica in x, y, z, quindi è uguale anche a $(y * z) * x$, che per la commutatività di $*$ è uguale a $x * (y * z)$.
Dunque $*$ è associativa.

ii) Siano $u, v \in \Gamma$, cioè $u^2 = u$, $v^2 = v$. Allora

$$(u * v) \cdot (u * v) =$$

$$= (u + v - 2uv)^2 = u^2 + v^2 + 4u^2v^2 + 2uv - 4u^2v - 4uv^2 =$$

$$= u + v + 4uv + 2uv - 4uv - 4uv = u + v - 2uv =$$

$$= u * v,$$

quindi $u * v \in \Gamma$.
Osserviamo che $0 \in \Gamma$, quindi $(\Gamma, *)$ è un insieme dotato di operazione associativa con elemento neutro.
D'altra parte dati $u, v \in \Gamma$, essi sono inversi uno dell'altro se e solo se $0 = u * v = u + v - 2uv = u^2 + v^2 - 2uv = (u - v)^2$, e questo avviene se $v = u$; effettivamente per ogni $u \in \Gamma$ si ha $u * u = u + u - 2u^2 = 2u - 2u = 0$, quindi in Γ ogni elemento è inverso di se stesso.
Ne segue che $(\Gamma, *)$ è un gruppo.

iii) Sia A un dominio di integrità. Allora $u^2 = u \Leftrightarrow u(u-1) = 0 \Leftrightarrow u = 0$ oppure $u = 1$.
Quindi $\Gamma = \{0, 1\}$, $\#\Gamma = 2$ e $(\Gamma, *) \cong \mathbb{Z}/2\mathbb{Z}$.

Sia $A = \mathbb{Z}/6\mathbb{Z}$. Allora $u \in \Gamma \Leftrightarrow u$ è soluzione della congruenza

$$x(x-1) \equiv 0 \pmod 6,$$

cioè del sistema

$$(\star) \qquad \begin{cases} x(x-1) \equiv 0 \pmod 2 \\ x(x-1) \equiv 0 \pmod 3. \end{cases}$$

Se p è primo la congruenza $x(x-1) \equiv 0 \pmod p$ ha esattamente due soluzioni (0 e 1). Quindi il sistema $(\star)$ ha 4 soluzioni (precisamente si ha $\Gamma = \{0, 1, 3, 4\}$). Dunque $(\Gamma, *)$ è un gruppo con 4 elementi e, come visto nel punto ii), tutti i suoi elementi hanno ordine che divide 2. Ne segue che $(\Gamma, *) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

iv) [Osservazione: dal punto iii) segue che se A è un dominio di integrità si ha $r = 1$, $d_1 = 2$ e se $A = \mathbb{Z}/6\mathbb{Z}$ si ha $r = 2$, $d_1 = d_2 = 2$].

$(\Gamma, *)$ è un gruppo abeliano; se $\#\Gamma < \infty$ allora $(\Gamma, *)$ è un gruppo abeliano finito, quindi esistono $r \in \mathbb{N}$ e $1 < d_r | d_{r-1} | ... | d_1 = mcm\{o(u) | u \in \Gamma\}$ tali che $(\Gamma, *) \cong \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$.
Dal fatto che $u * u = 0$ per ogni $u \in \Gamma$ segue che $mcm\{o(u) | u \in \Gamma\} | 2$.
Quindi o $r = 0$ (e questo avviene se e solo se $A = \{0\}$, perché $0, 1 \in \Gamma$) oppure $r > 0$ e $d_1 = ... = d_r = 2$, cioè

$$\Gamma \cong \prod_{i=1}^{r} \mathbb{Z}/2\mathbb{Z}.$$

In generale (cioè anche se Γ è un insieme infinito) dal fatto che $u * u = 0$ per ogni $u \in \Gamma$ segue che $(\Gamma, *)$ ha una struttura di $(\mathbb{Z}/2\mathbb{Z})$-spazio vettoriale. Se B è una base di Γ su $\mathbb{Z}/2\mathbb{Z}$ abbiamo

$$\Gamma = \oplus_{b \in B} (\mathbb{Z}/2\mathbb{Z})b \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus B}.$$

Osservare che dal risultato generale segue il risultato nel caso finito: se $\#\Gamma < \infty$ si ha $\#B < \infty$, quindi esiste $r (= \#B) \in \mathbb{N}$ tale che

$$\Gamma \cong \oplus_{i=1}^{r} \mathbb{Z}/2\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/2\mathbb{Z},$$

cioè $d_1 = d_2 = ... = d_r = 2$.

Osservare anche che il punto iii) segue dal punto iv) e dal calcolo della cardinalità di Γ nei casi A dominio di integrità e $A = \mathbb{Z}/6\mathbb{Z}$.

2) i) Ricordiamo che

$$\mathbb{C}[z, z^{-1}] = \mathbb{C}[z, w]/(zw - 1)$$

e che

$$x^2 - y^2 = (x + y)(x - y).$$

Quindi il cambio di variabili $z = x + y$, $w = x - y$ (che è lineare invertibile) determina un isomorfismo tra $\mathbb{C}[x, y]$ e $\mathbb{C}[z, w]$ tramite il quale $x^2 - y^2 - 1$ corrisponde a $zw - 1$, e induce quindi un isomorfismo tra A e $\mathbb{C}[z, z^{-1}]$.

ii) Poiché $\mathbb{C}[z, z^{-1}]$ (dunque A) è un dominio di integrità, l'ideale $(x^2 - y^2 - 1) \subseteq \mathbb{C}[x, y]$ è primo, dunque $x^2 - y^2 - 1$ è un elemento primo (quindi irriducibile) in $\mathbb{C}[x, y]$.

Alternativamente, osserviamo che $y^2 + 1$ non è un quadrato in $\mathbb{C}(y)$, quindi $x^2 - y^2 - 1 = x^2 - (y^2 + 1)$ è irriducibile in $\mathbb{C}(y)[x]$, dunque è anche irriducibile in $\mathbb{C}[x, y]$.
Sappiamo che l'insieme degli elementi invertibili di $\mathbb{C}[z, z^{-1}]$ è

$$\{az^n | a \in \mathbb{C}^*, n \in \mathbb{Z}\}.$$

Tramite il cambio di variabili descritto al punto i), x e y corrispondono rispettivamente a $\frac{1}{2}(z + z^{-1})$ e $\frac{1}{2}(z - z^{-1})$, quindi non sono invertibili in A.

Anche senza aver dimostrato l'isomorfismo tra A e $\mathbb{C}[z, z^{-1}]$, con un po' più di lavoro si può studiare l'invertibilità o meno di x e y, osservando innanzitutto che la restrizione della proiezione naturale $\mathbb{C}[x, y] \to A$ al sottospazio vettoriale $\mathbb{C}[x] \oplus y\mathbb{C}[x]$ è biunivoca, perché $(x^2 - y^2 - 1) \cap (\mathbb{C}[x] \oplus y\mathbb{C}[x]) = \{0\}$ e $y^2 = x^2 - 1$; analogamente $\mathbb{C}[y] \oplus x\mathbb{C}[y]$ è un insieme di rappresentanti di A in $\mathbb{C}[x, y]$.
Cercare un inverso di x in A equivale quindi a cercare $p, q \in \mathbb{C}[x]$ tali che $x(p + yq) - 1 \in (x^2 - y^2 - 1)$, cioè $xq = 0$, $xp = 1$; ma x non è invertibile in $\mathbb{C}[x]$, quindi tale p non esiste e x non è invertibile neanche in A.
Analogamente y non è invertibile in A.

iii) A è un dominio euclideo perché $\mathbb{C}[z, z^{-1}]$ è un dominio euclideo.

iv) In A abbiamo $1 = x^2 - y^2 = (x + y)(x - y)$ quindi $x + y$ è invertibile (e anche $x - y$ lo è), da cui segue che $q = -1$, $r = x + y$ è una soluzione di $(\Diamond)$: $x = (-1)y + (x + y)$.

Ora in un dominio euclideo gli elementi invertibili sono gli elementi di valutazione minima; poiché (in A) r è invertibile e y non lo è, si ha che la valutazione di r è sicuramente strettamente minore della valutazione di y, quindi $(\Diamond)$ è una divisione euclidea.

3) Osserviamo preliminarmente che in generale $X \times Y$ è l'unione di una copia $\{x\} \times Y$ di $(Y, \leq_Y)$ per ogni elemento $x \in X$ e che se $x \neq x'$ gli elementi di $\{x\} \times Y$ sono lessicograficamente minori degli elementi di $\{x'\} \times Y$ (cosa che con abuso di notazione possiamo scrivere $\{x\} \times Y \preceq \{x'\} \times Y$) se e solo se $x \leq_X x'$.
Dunque $(\mathbb{N} \times \{0,1\}, \leq')$ può essere descritto come l'unione di un'infinità numerabile di copie di $\{0,1\}$ una dietro l'altra

$$\{0\} \times \{0,1\} \leq' \{1\} \times \{0,1\} \leq' ... \leq' \{n\} \times \{0,1\} \leq' ...$$

mentre $(\{0,1\} \times \mathbb{N}, \leq'')$ è l'uniome di due copie di $\mathbb{N}$ una dietro l'altra.

i) Si considerino le funzioni $\varphi : \mathbb{N} \times \{0,1\} \to \mathbb{N}$ e $\psi : \mathbb{N} \to \mathbb{N} \times \{0,1\}$ definite nel modo seguente:

$$\varphi(n, \varepsilon) = 2n + \varepsilon, \quad \psi(n) = \left(\left[\frac{n}{2} \right], n - 2 \left[\frac{n}{2} \right] \right) = \begin{cases} \left(\frac{n}{2}, 0 \right) & \text{se } 2|n \\ \left(\frac{n-1}{2}, 1 \right) & \text{altrimenti.} \end{cases}$$

È immediato verificare che φ e ψ sono ben definite e sono l'una l'inversa dell'altra.
Inoltre $n \leq m \Rightarrow \left[\frac{n}{2} \right] \leq \left[\frac{m}{2} \right]$; se $\left[\frac{n}{2} \right] < \left[\frac{m}{2} \right]$ si ha $\psi(n) \leq' \psi(m)$; se invece $\left[\frac{n}{2} \right] = \left[\frac{m}{2} \right] = r$ si ha $n = 2r + \varepsilon$, $m = 2r + \delta$ con $\varepsilon, \delta \in \{0,1\}$ e $\psi(n) = (r, \varepsilon)$, $\psi(m) = (r, \delta)$; da $n \leq m$ segue $\varepsilon \leq \delta$, quindi anche in questo caso $\psi(n) \leq' \psi(m)$. Dunque ψ è un morfismo biunivoco di insiemi ordinati. Poiché $(\mathbb{N}, \leq)$ è totalmente ordinato, ψ è un isomorfismo di insiemi ordinati.

ii) $(\{0,1\} \times \mathbb{N}), \leq'')$ è ben ordinato perché $(\{0,1\}, \leq)$ e $(\mathbb{N}, \leq)$ sono ben ordinati. (È un fatto generale che se $(X, \leq_X)$, $(Y, \leq_Y)$ sono ben ordinati anche l'ordinamento lessicografico su $X \times Y$ è un buon ordinamento).

iii) Per ogni $n \in \mathbb{N}$ si ha $(0, n) <'' (0, n+1) \in \{0\} \times \mathbb{N}$, quindi $\{0\} \times \mathbb{N}$ non ha massimo.
Per ogni $n \in \mathbb{N}$ si ha $(0, n) \leq'' (1, 0)$, quindi $\{0\} \times \mathbb{N}$ è limitato superiormente da $(1, 0)$.

iv) In $(\mathbb{N} \times \{0\}, \leq') \cong (\mathbb{N}, \leq)$ tutti i sottoinsiemi non vuoti limitati superiormente hanno massimo; dunque per quanto visto al punto iii)

$$(\mathbb{N} \times \{0\}, \leq') \ncong (\{0\} \times \mathbb{N}, \leq'').$$