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

1) Si consideri il polinomio $f(x) = x^3 + 3x + 3$.

i) Dire se $f(x)$ sia irriducibile in $\mathbb{C}[x]$, in $\mathbb{R}[x]$, in $\mathbb{Q}[x]$, in $\mathbb{Z}[x]$.

ii) Dimostrare che x è invertibile in $\mathbb{Q}[x]/(f(x))$ e determinarne l'inverso. $\mathbb{Q}[x]/(f(x))$ è un campo?

iii) Dire se gli ideali (2) e (3) dell'anello $\mathbb{Z}[x]/(f(x))$ siano massimali e se siano primi.

iv) Descrivere gli anelli $\mathbb{C}[x]/(f(x))$ e $\mathbb{R}[x]/(f(x))$.

2) Siano:
$n \in \mathbb{Z}$;
$f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ la funzione definita da $f(a, b) = a + n(a - b)$;
$\pi : \mathbb{Z} \to \mathbb{Z}/(n^2 + n)\mathbb{Z}$ la proiezione sul quoziente.

i) Dimostrare che f e $\pi \circ f$ sono omomorfismi suriettivi di gruppo.

ii) Discutere al variare di n in $\mathbb{Z}$ se f e $\pi \circ f$ siano omomorfismi di anelli.

iii) Determinare il nucleo di $\pi \circ f$ e descrivere $(\mathbb{Z} \times \mathbb{Z})/ker(\pi \circ f)$.

iv) Determinare il nucleo di f e dire se esiste un sottogruppo H di $\mathbb{Z} \times \mathbb{Z}$ tale che $\mathbb{Z} \times \mathbb{Z} = ker(f) \oplus H$.

3) Per ogni $n \geq k \geq 0$ sia $a_{n,k}$ il numero delle funzioni biunivoche di un insieme di n elementi in sé, che hanno esattamente k punti fissi, cioè

$$a_{n,k} = \#\{f : \{1, ..., n\} \to \{1, ..., n\} | f \text{ biunivoca e } \#\{i | f(i) = i\} = k\}.$$

i) Calcolare $\sum_{k=0}^{n} a_{n,k}$.

ii) Calcolare $a_{n,n}$, $a_{n,n-1}$, $a_{n,n-2}$.

iii) Dimostrare che $a_{n-k,0} | a_{n,k}$; più precisamente determinare $b_{n,k} \in \mathbb{N}$ tale che $a_{n,k} = b_{n,k} a_{n-k,0}$.

iv) Dimostrare che $\sum_{k=0}^{n} k a_{n,k} = n!$

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

SOLUZIONI

1)
i)

Su $\mathbb{C}$ i polinomi irriducibili sono quelli di grado 1, quindi x^3+3x+3 non è irriducibile in $\mathbb{C}[x]$.

Su $\mathbb{R}$ i polinomi di grado maggiore di 2 sono riducibili, quindi x^3+3x+3 non è irriducibile in $\mathbb{R}[x]$.

Per il criterio di Eisenstein il polinomio x^3+3x+3 è irriducibile in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$ perché 3 non divide il coefficiente di grado massimo e divide tutti gli altri coefficienti, e 3^2 non divide il termine noto.
Alternativamente: le radici razionali del polinomio $f(x) = x^3 + 3x + 3$ sono necessariamente interi che dividono 3, cioè vanno cercate nell'insieme $\{\pm 1, \pm 3\}$; una rapida verifica mostra che nessuno di questi quattro numeri è una radice di $f(x)$, quindi $f(x)$ non ha divisori di grado 1, ed essendo di grado 3 è irriducibile in $\mathbb{Q}[x]$ e in $\mathbb{Z}[x]$.

ii) In $\mathbb{Q}[x]/(f(x))$ si ha che $x^3 + 3x + 3 = 0$, quindi $x(x^2 + 3) = -3$, cioè

$$x \cdot \frac{x^2+3}{-3} = 1.$$

Quindi x è invertibile e il suo inverso è $-\frac{1}{3}x^2 - 1$.
[Si osservi che $-\frac{1}{3}x^2-1$ è l'inverso di x anche in $\mathbb{R}[x]/(f(x))$ e in $\mathbb{C}[x]/(f(x))$.]

$\mathbb{Q}[x]$ è un dominio a ideali principali e $f(x)$ è irriducibile in $\mathbb{Q}[x]$, quindi $f(x)$ genera un ideale massimale; ne segue che $\mathbb{Q}[x]/(f(x))$ è un campo.

iii) Sia $A = \mathbb{Z}[x]/(f(x))$.

$A/(2) \cong \mathbb{Z}[x]/(f(x), 2) \cong (\mathbb{Z}/2\mathbb{Z})[x]/(f(x)) = (\mathbb{Z}/2\mathbb{Z})[x]/(x^3 + x + 1)$. Osserviamo che $0, 1 \in \mathbb{Z}/2\mathbb{Z}$ non sono radici di $f(x)$; dunque $f(x)$ ha grado 3 e non ha radici nel campo $\mathbb{Z}/2\mathbb{Z}$, quindi è irriducibile. Ne segue che $(\mathbb{Z}/2\mathbb{Z})[x]/(f(x))$ è il quoziente di un dominio a ideali principali per l'ideale generato da un polinomio irriducibile, quindi è un campo. Dunque $A/(2)$ è un campo e (2) è massimale, quindi primo, in $A = \mathbb{Z}[x]/(f(x))$.

$A/(3) \cong \mathbb{Z}[x]/(f(x), 3) \cong (\mathbb{Z}/3\mathbb{Z})[x]/(f(x)) = (\mathbb{Z}/3\mathbb{Z})[x]/(x^3)$. Osserviamo che $x \in \mathbb{Z}/3\mathbb{Z}[x]/(x^3)$ è nilpotente diverso da zero, quindi $A/(3)$ non è un dominio di integrità; ne segue che l'ideale (3) non è primo, dunque non è neanche massimale, in $A = \mathbb{Z}[x]/(f(x))$.

iv) Poiché $deg(f(x))$ è dispari, esiste $\alpha \in \mathbb{R}$ tale che $f(\alpha) = 0$, cioè tale che $x - \alpha | f(x)$ in $\mathbb{R}[x]$, quindi anche $x - \alpha | f(x)$ in $\mathbb{C}[x]$.
Sia

$$g(x) = \frac{f(x)}{x - \alpha} = x^2 + \alpha x - \frac{3}{\alpha} = x^2 + \alpha x + \alpha^2 + 3 = ax^2 + bx + c$$

e osserviano che

$$b^2 - 4ac = \alpha^2 - 4(\alpha^2 + 3) = -3(\alpha^2 + 4) < 0,$$

quindi $f(x)$ non ha altre radici reali oltre α.
Alternativamente si può osservare che $\frac{df(x)}{dx} = 3x^2 + 3$ assume su $\mathbb{R}$ solo valori positivi, quindi la funzione $\mathbb{R} \ni x \mapsto f(x) \in \mathbb{R}$ è crescente, dunque $f(x)$ ha una sola radice reale. D'altra parte $f(x) \neq (x - \alpha)^3$.

Quindi le radici complesse di $f(x)$ sono α e due radici β e γ complesse (non reali) coniugate tra loro; in particolare $\alpha, \beta, \gamma \in \mathbb{C}$ sono distinti, cioè $x - \alpha$, $x - \beta$ e $x - \gamma$ sono irriducibili a due a due coprimi in $\mathbb{C}[x]$.
Ne segue che $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$ è la fattorizzazione di $f(x)$ in $\mathbb{C}[x]$ e che

$$\mathbb{C}[x]/(f(x)) \cong \mathbb{C}[x]/(x - \alpha) \times \mathbb{C}[x]/(x - \beta) \times \mathbb{C}[x]/(x - \gamma) \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C}.$$

D'altra parte $f(x) = (x - \alpha)(x^2 + \alpha x + \alpha^2 + 3)$ è la fattorizzazione di $f(x)$ in $\mathbb{R}[x]$, perché $x - \beta, x - \gamma \notin \mathbb{R}[x]$.
Osserviamo che l'omomorfismo di anelli $\mathbb{R}[x] \to \mathbb{C}$ definito da $x \mapsto \beta$ è suriettivo e ha nucleo $(x^2 + \alpha x + \alpha^2 + 3)$ (ideale massimale in $\mathbb{R}[x]$), quindi $\mathbb{R}[x]/(x^2 + \alpha x + \alpha^2 + 3) \cong \mathbb{C}$.
Dunque

$$\mathbb{R}[x]/(f(x)) \cong \mathbb{R}[x]/(x - \alpha) \times \mathbb{R}[x]/(x^2 + \alpha x + \alpha^2 + 3) \cong \mathbb{R} \times \mathbb{C}.$$

2)
i) Dati (a, b), $(a', b') \in \mathbb{Z} \times \mathbb{Z}$ abbiamo

$$f((a, b) + (a', b')) = f(a + a', b + b') =$$

$$= a + a' + n((a + a') - (b + b')) = a + n(a - b) + a' + n(a' - b') =$$

$$= f(a, b) + f(a', b'),$$

quindi f è un omomorfismo di gruppi.

$f(1,1) = 1$ quindi l'immagine di f è un sottogruppo di $\mathbb{Z}$ che contiene 1; poiché 1 è un generatore di $\mathbb{Z}$ si ha $Im(f) = \mathbb{Z}$, dunque f è suriettiva.

La proiezione sul quoziente è un omomorfismo suriettivo di gruppi, quindi $\pi \circ f$ è composizione di due omomorfismi suriettivi di gruppi quindi è un omomorfismo suriettivo di gruppi.

ii) Osserviamo che se $n^2 + n = 0$ (cioè se $n = 0$ oppure $n = -1$) si ha $\mathbb{Z}/(n^2 + n)\mathbb{Z} = \mathbb{Z}$ e $\pi = id$; in tal caso $\pi \circ f = f$.

Se $n = 0$ $f(a, b) = a$, quindi f è la proiezione da $\mathbb{Z} \times \mathbb{Z}$ sul primo fattore, quindi f e $\pi \circ f = f$ sono omomorfismi di anelli.

Se $n = -1$ $f(a, b) = b$, quindi f è la proiezione da $\mathbb{Z} \times \mathbb{Z}$ sul secondo fattore, quindi f e $\pi \circ f = f$ sono omomorfismi di anelli.

Sia adesso $n^2 + n \neq 0$. Allora

$$f((1,0)(0,1)) = f(0,0) = 0$$

mentre

$$f(1,0)f(0,1) = (n+1)(-n) \neq 0,$$

quindi in questo caso f non è un omomorfismo di anelli.

Osserviamo che $n^2 + n = n(n+1)$ e $(n, n+1) = 1$, quindi la funzione

$$\chi : \mathbb{Z}/(n^2+n)\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/(n+1)\mathbb{Z}$$

definita da

$$[x]_{mod\ n^2+n} \mapsto ([x]_{mod\ n}, [x]_{mod\ n+1})$$

è un isomorfismo di anelli.
Inoltre

$$(\chi \circ \pi \circ f)(a,b) =$$

$$([a + n(a-b)]_{mod\ n}, [(n+1)(a-b) + b]_{mod\ n+1}) =$$

$$= ([a]_{mod\ n}, [b]_{mod\ n+1})$$

dunque $\chi \circ \pi \circ f$ è il prodotto delle due proiezioni sul quoziente

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \quad \text{e} \quad \mathbb{Z} \to \mathbb{Z}/(n+1)\mathbb{Z},$$

quindi è un omomorfismo di anelli, quindi anche $\pi \circ f = \chi^{-1} \circ (\chi \circ \pi \circ f)$ è un omomorfismo di anelli.
Alternativamente, senza usare l'isomorfismo χ, dati (a, b), $(a', b') \in \mathbb{Z} \times \mathbb{Z}$ abbiamo

$$f(a,b)f(a',b') =$$

$$(a+n(a-b))(a'+n(a'-b')) =$$
$$= aa' + n(a(a'-b') + (a-b)a') + n^2(a-b)(a'-b') =$$
$$= aa' + n(aa' - bb') + (n^2+n)(a-b)(a'-b') =$$
$$= f((a,b)(a',b')) + (n^2+n)(a-b)(a'-b') \equiv$$
$$\equiv f((a,b)(a',b')) \pmod{n^2+n}$$

quindi $\pi \circ f$ è un omomorfismo di anelli.

iii) Sappiamo che $\pi \circ f$ è suriettiva, quindi

$$(\mathbb{Z}\times\mathbb{Z})/ker(\pi\circ f) \cong Im(\pi\circ f) = \mathbb{Z}/(n^2+n)\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/(n+1)\mathbb{Z}.$$

Ovviamente per quanto visto al punto ii) abbiamo

$$ker(\pi\circ f) = ker(\chi\circ\pi\circ f) = n\mathbb{Z}\times(n+1)\mathbb{Z}.$$

Alternativamente, senza usare χ, abbiamo che

$$(a,b) \in ker(\pi\circ f) \Leftrightarrow f(a,b) = (n+1)a - nb \equiv 0 \pmod{n(n+1)}.$$

Ora $n(n+1)|(n+1)a-nb \Leftrightarrow n|a$ e $(n+1)|b$, quindi $ker(\pi\circ f) = n\mathbb{Z}\times(n+1)\mathbb{Z}$.

iv)

Nel caso $n=0$ oppure $n=-1$ abbiamo visto nel punto ii) che $\pi\circ f = f$ e nel punto iii) che

$$ker(f)(= ker(\pi\circ f)) = \begin{cases} \{0\}\times\mathbb{Z} & \text{se } n=0 \\ \mathbb{Z}\times\{0\} & \text{se } n=-1. \end{cases}$$

Sia $n \neq 0,-1$; $(a,b) \in ker(f) \Leftrightarrow f(a,b) = 0 \Leftrightarrow (n+1)a - nb = 0$; ovviamente $(n,n+1) \in ker(f)$; d'altra parte $(n+1)a = nb \Rightarrow n+1|nb$, quindi $(n+1)|b = (n+1)k$ per qualche $k\in\mathbb{Z}$; ne segue che $0 = (n+1)a-nb = (n+1)(a-nk)$, dunque (poiché $n+1\neq 0$) $a = nk$.
Quindi per ogni $n\in\mathbb{Z}$ (anche per $n=0,-1$) $ker(f)$ è il sottogruppo di $\mathbb{Z}\times\mathbb{Z}$ generato da $(n,n+1)$, cioè

$$ker(f) =< (n,n+1) >= \mathbb{Z}(n,n+1).$$

Sia $\gamma : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ l'(unico) omomorfismo di anelli di $\mathbb{Z}$ in $\mathbb{Z}\times\mathbb{Z}$, cioè la funzione $a\mapsto(a,a)$. $f\circ\gamma = id_{\mathbb{Z}}$, quindi

$$Im(\gamma)\cap ker(f) = \{0\}$$

e

$$Im(\gamma) + ker(f) = f^{-1}(f(\gamma(\mathbb{Z}))) = f^{-1}(\mathbb{Z}) = \mathbb{Z} \times \mathbb{Z},$$

quindi

$$\mathbb{Z} \times \mathbb{Z} = Im(\gamma) + ker(f) = Im(\gamma) \oplus ker(f).$$

Alternativamente, senza usare γ, si può osservare che

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

quindi

$$\mathbb{Z} \times \mathbb{Z} =< (0,1), (1,1) >=< (n, n+1), (1,1) >= ker(f) + < (1,1) >$$

e

$$ker(f) \cap < (1,1) >= \{(nk, (n+1)k) | k \in \mathbb{Z}\} \cap \{(r,r) | r \in \mathbb{Z}\} = \{0\}.$$

Quindi

$$\mathbb{Z} \times \mathbb{Z} = ker(f) \oplus < (1,1) > .$$

3)
i) $\sum_{k=0}^{n} a_{n,k}$ è la cardinalità dell'insieme delle funzioni biunivoche di $\{1, ..., n\}$ in sé con un numero qualsiasi di punti fissi, cioè è la cardinalità dell'insieme delle funzioni biunivoche di $\{1, ..., n\}$ in sé. Dunque

$$\sum_{k=0}^{n} a_{n,k} = n!$$

ii)

Esiste un'unica funzione di $\{1, ..., n\}$ in sé con n punti fissi: l'identità (che è biunivoca). Quindi $a_{n,n} = 1$.

Non esistono funzioni biunivoche di $\{1, ..., n\}$ in sé con $n-1$ punti fissi: se f ha $n-1$ punti fissi, l'iniettività e/o la suriettività di f implicano che anche l'ennesimo punto è fisso. Quindi $a_{n,n-1} = 0$.
Equivalentemente se esistono $i \neq j$ tali che $f(i) = j$ l'iniettività di f implica che $f(j) \neq j$, quindi esistono almeno due punti non fissi per f; dunque se $f \neq id$ allora f ha non più di $n-2$ punti fissi. Quindi $a_{n,n-1} = 0$.

Le funzioni biunivoche f di $\{1, ..., n\}$ in sé con $n-2$ punti fissi sono in corrispondenza biunivoca con i sottoinsiemi di $\{1, ..., n\}$ con 2 elementi: infatti se i e j non sono punti fissi di f si deve avere necessariamente

$$(\star) \qquad f(r) = r \ \text{ per ogni } r \neq i, j, \quad f(i) = j, \quad f(j) = i;$$

viceversa per ogni $i \neq j$ $(\star)$ definisce una funzione biunivoca di $\{1, ..., n\}$ in sé con $n-2$ punti fissi.
Ne segue che $a_{n,n-2} = \binom{n}{2}$.

iii) Sia $X \subseteq \{1, ..., n\}$ un insieme di cardinalità k; le funzioni biunivoche f di $\{1, ..., n\}$ in sé tali che $f(i) = i \Leftrightarrow i \in X$ sono in corrispondenza biunivoca con le funzioni biunivoche $\tilde{f} : \{1, ..., n\} \setminus X \to \{1, ..., n\} \setminus X$ che non hanno punti fissi: la corrispondenza biunivoca è data da $f \mapsto f\big|_{\{1,...,n\}\setminus X}$.
Ci sono quindi esattamente $a_{n-k,0}$ funzioni biunivoche f di $\{1, ..., n\}$ in sé tali che X sia l'insieme dei punti fissi di f.
Ne segue che $a_{n,k} = \#\{X \subseteq \{1, ..., n\} | \#X = k\} \cdot a_{n-k,0} = \binom{n}{k} \cdot a_{n-k,0}$.

Notare che questo risultato implica anche il punto ii) osservando che $a_{0,0} = 1$, $a_{1,0} = 0$, $a_{2,0} = 1$.

iv) Dai punti iii) e i) segue che

$$\sum_{k=0}^{n} k a_{n,k} = \sum_{k=1}^{n} k \binom{n}{k} \cdot a_{n-k,0}.$$

Ora

$$k\binom{n}{k} = k\frac{n!}{k!(n-k)!} =$$

$$= \frac{n!}{(k-1)!(n-k)!} = n\frac{(n-1)!}{(k-1)!(n-k)!} = n\binom{n-1}{k-1}$$

quindi

$$\sum_{k=0}^{n} k a_{n,k} =$$

$$= n\sum_{k=1}^{n} \binom{n-1}{k-1} \cdot a_{n-k,0} = n\sum_{k=0}^{n-1} \binom{n-1}{k} \cdot a_{n-(k+1),0} =$$

$$= n\sum_{k=0}^{n-1} \binom{n-1}{k} \cdot a_{(n-1)-k,0} = n\sum_{k=0}^{n-1} a_{n-1,k} = n(n-1)! =$$

$$= n!$$