ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 16/06/2025 ore 10.00 - aula 29A

1) Si consideri il sistema di congruenze

$$\begin{cases} 7x \equiv 11 \pmod{15} \\ 2^x \equiv x \pmod{5} \end{cases}$$

i) Risolvere l'equazione $7x \equiv 11 \pmod{15}$.

ii) Calcolare l'ordine di 2 nel gruppo $(\mathbb{Z}/5\mathbb{Z})^*$.

iii) Per ogni intero a risolvere l'equazione $2^x \equiv a \pmod{5}$.

iv) Risolvere il sistema

$$\begin{cases} 7x \equiv 11 \pmod{15} \\ 2^x \equiv x \pmod{5} \end{cases}$$

2) Si considerino le relazioni $P \subseteq \mathbb{R} \times \mathbb{R}$ e $\sim \subseteq \mathbb{R} \times \mathbb{R}$ definite nel modo seguente:

$$aPb \Leftrightarrow \forall n \in \mathbb{Z} \text{ tale che } n \leq a \text{ si ha } n \leq b,$$

$$a \sim b \Leftrightarrow aPb \text{ e } bPa.$$

i) Dimostrare che P è una relazione riflessiva e transitiva; P è una relazione d'ordine? P è una relazione di equivalenza?

ii) Dimostrare che $\sim$ è una relazione di equivalenza e descrivere $\mathbb{R}/\sim$.

iii) Dimostrare che P induce una relazione d'ordine $\preceq$ su $\mathbb{R}/\sim$ e descrivere l'insieme ordinato $(\mathbb{R}/\sim, \preceq)$.

iv) $\preceq$ è un ordinamento totale? $\preceq$ è un buon ordinamento?

3) Siano

$$K \text{ un campo}, \quad A_K = K[x,y]/(x^2+xy+y^2).$$

i) Fattorizzare $x^3 - y^3$ in $\mathbb{R}[x,y]$, in $\mathbb{C}[x,y]$, in $(\mathbb{Z}/3\mathbb{Z})[x,y]$.

ii) Dimostrare che $A_{\mathbb{C}}$ e $A_{\mathbb{Z}/3\mathbb{Z}}$ non sono domini di integrità e trovare un divisore non banale di zero in $A_{\mathbb{C}}$ e un elemento nilpotente non banale in $A_{\mathbb{Z}/3\mathbb{Z}}$.

iii) Dimostrare che $A_{\mathbb{R}}$ è un dominio di integrità e non è un campo.

iv) Dimostrare che il campo dei quozienti di $A_{\mathbb{R}}$ è isomorfo a $\mathbb{C}(t)$ (il campo delle funzioni razionali in una variabile a coefficienti in $\mathbb{C}$).

ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 16/06/2025 ore 10.00 - aula 29A

SOLUZIONI

1)
i) L'equazione $7x \equiv 11 \pmod{15}$ è risolubile perché $MCD(7,15) = 1$, quindi 7 è invertibile in $\mathbb{Z}/15\mathbb{Z}$; il suo inverso è -2: $7 \cdot (-2) = -14 \equiv 1 \pmod{15}$; quindi la soluzione cercata è $x = -2 \cdot 11 = -22 \equiv 8 \pmod{15}$.

ii) $2 \in (\mathbb{Z}/5\mathbb{Z})^*$ perché $MCD(2,5) = 1$.
$(\mathbb{Z}/5\mathbb{Z})^*$ ha cardinalità 4, quindi tutti i suoi elementi hanno ordine un divisore di 4.
Poiché $2^2 = 4 \not\equiv 1 \pmod{5}$, l'ordine di 2 in $(\mathbb{Z}/5\mathbb{Z})^*$ è 4.

iii) Per quanto visto al punto ii), 2 è un generatore di $(\mathbb{Z}/5\mathbb{Z})^*$: nel dettaglio

$$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 3 \pmod{5}.$$

Quindi:
se $5|a$ l'equazione $2^x \equiv a \pmod{5}$ non è risolubile;
se $5 \not| a$ l'equazione $2^x \equiv a \pmod{5}$ ha esattamente una soluzione modulo 4, e precisamente:
$a \equiv 1 \pmod{5} \Leftrightarrow x \equiv 0 \pmod{4}$;
$a \equiv 2 \pmod{5} \Leftrightarrow x \equiv 1 \pmod{4}$;
$a \equiv 3 \pmod{5} \Leftrightarrow x \equiv 3 \pmod{4}$;
$a \equiv 4 \pmod{5} \Leftrightarrow x \equiv 2 \pmod{4}$.

iv) In i) abbiamo visto che $7x \equiv 11 \pmod{15}$ equivale a $x \equiv 8 \pmod{15}$; poiché $5|15$, questo implica che $x \equiv 8 \equiv 3 \pmod{5}$.
In iii) abbiamo visto che se $a \equiv 3 \pmod{5}$ l'equazione $2^x \equiv a \pmod{5}$ equivale a $x \equiv 3 \pmod{4}$.
Quindi il sistema

$$\begin{cases} 7x \equiv 11 \pmod{15} \\ 2^x \equiv x \pmod{5} \end{cases}$$

equivale al sistema

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 3 \pmod{4}. \end{cases}$$

Poiché $8 \equiv 0 \pmod{4}$, $15 \equiv 3 \pmod{4}$ e $15 \equiv 0 \pmod{15}$, la soluzione del sistema è $x \equiv 8 + 15 \equiv 23 \pmod{15 \cdot 4 = 60}$.

2) Osserviamo preliminarmente che $aPb \Leftrightarrow (n \in \mathbb{Z}, n \leq a \Rightarrow n \leq b)$.
Sia $[a] \in \mathbb{Z}$ la *parte intera* di a, cioè $[a] = max\{n \in \mathbb{Z} | n \leq a\}$.
Allora si ha $aPb \Leftrightarrow [a] \leq [b]$:
infatti se aPb allora $[a] \leq a \leq b$ da cui $[a] \leq b$ cioè $[a] \leq [b]$;
viceversa se $[a] \leq [b]$ allora da $n \leq a$ segue che $n \leq [a] \leq [b] \leq b$ cioè $n \leq b$, quindi aPb.

i) $n \leq a \Rightarrow n \leq a$, quindi aPa, cioè P è riflessiva;
se $n \leq a \Rightarrow n \leq b$ e $n \leq b \Rightarrow n \leq c$ allora $n \leq a \Rightarrow n \leq b \Rightarrow n \leq c$, da cui $n \leq a \Rightarrow n \leq c$, quindi P è transitiva.
$0P\frac{1}{2}$ e $\frac{1}{2}P0$ ma $0 \neq \frac{1}{2}$, quindi P non è antisimmetrica, cioè non è un ordinamento.
$0P1$ ma non è vero che $1P0$, quindi P non è simmetrica, cioè non è una relazione di equivalenza.

ii) $a \sim b \Leftrightarrow [a] \leq [b]$ e $[b] \leq [a] \Leftrightarrow [a] = [b]$, quindi $\sim$ è la relazione indotta dalla funzione $[\cdot] : \mathbb{R} \to \mathbb{Z}$; quindi $\sim$ è di equivalenza.
Poiché $[\cdot]$ è suriettiva, $(\mathbb{R}/\sim, \pi) = (\mathbb{Z}, [\cdot])$.

iii) Siano $a \sim a'$, $b \sim b'$, cioè aPa', $a'Pa$, bPb', $b'Pb$. Allora aPb (e $a'Pa$, bPb') $\Rightarrow a'Pb'$. Ne segue che P induce una relazione $\preceq$ su $\mathbb{R}/\sim$.
$\preceq$ è riflessiva e transitiva perché P è riflessiva e transitiva; inoltre $\preceq$ è antisimmetrica (dunque è un ordinamento), perché $[a] \preceq [b]$ e $[b] \preceq [a] \Rightarrow aPb$ e $bPa \Rightarrow a \sim b \Rightarrow [a] = [b]$.
Poiché $[a] \preceq [b] \Leftrightarrow aPb \Leftrightarrow [a] \leq [b]$, abbiamo che $(\mathbb{R}/\sim, \preceq) \cong (\mathbb{Z}, \leq)$. Questa descrizione di $(\mathbb{R}/\sim, \preceq)$ fornisce anche una dimostrazione alternativa del fatto che $\preceq$ è una relazione d'ordine.

iv) $(\mathbb{Z}, \leq)$, quindi $(\mathbb{R}/\sim, \preceq)$, è totalmente ordinato e, poiché non ha minimo, non è ben ordinato.

3) Ricordiamo preliminarmente che $K[x, y]$ è un dominio a fattorizzazione unica e che in $K[x, y]$ tutti i polinomi di grado 1 sono irriducibili.

i) In generale $x - y | x^3 - y^3 = (x - y)(x^2 + xy + y^2)$.

Se $K = \mathbb{Z}/3\mathbb{Z}$ allora $x^2 + xy + y^2 = x^2 - 2xy + y^2 = (x - y)^2$, quindi $x^3 - y^3 = (x - y)^3$ è la fattorizzazione di $x^3 - y^3$ in irriducibili in $(\mathbb{Z}/3\mathbb{Z})[x, y]$. Notiamo anche che $(\mathbb{Z}/3\mathbb{Z})[x, y]$ è un anello di caratteristica 3, quindi la funzione $a \mapsto a^3$ è un omomorfismo di anelli: questa osservazione fornisce un'altra dimostrazione del fatto che $(x - y)^3 = x^3 - y^3$.

Se $K = \mathbb{C}$ sia ω una radice primitiva cubica di 1 (quindi $\omega \neq 1$, $\omega^3 = 1$, da cui segue $\omega^2 + \omega + 1 = 0$).

Allora in $\mathbb{C}[x,y]$ $x^3-y^3=(x-y)(x-\omega y)(x-\omega^2 y)$ è la fattorizzazione di x^3-y^3 in irriducibili (e $x^2+xy+y^2=(x-\omega y)(x-\omega^2 y)$).

Osservare che $x-\omega y$ e $x-\omega^2 y$ non appartengono a $\mathbb{R}[x,y]$, quindi in $\mathbb{R}[x,y]$ si ha che x^2+xy+y^2 è irriducibile e $x^3-y^3=(x-y)(x^2+xy+y^2)$ è la fattorizzazione in irriducibili.

ii) Osserviamo preliminarmente che i polinomi di grado 1 sono non nulli in A_K perché tutti i multipli non nulli di x^2+xy+y^2 hanno grado ≥ 2.

In i) abbiamo visto che se $K=\mathbb{C}$ oppure $K=\mathbb{Z}/3\mathbb{Z}$ allora x^2+xy+y^2 non è irriducibile in $K[x,y]$, quindi $A_K=K[x,y]/(x^2+xy+y^2)$ non è un dominio di integrità.
I conti già fatti implicano che $(x-\omega y)(x-\omega^2 y)=0$ in $A_{\mathbb{C}}$ (quindi $x-\omega y$ è un divisore non banale dello zero) e $(x-y)^2=0$ in $A_{\mathbb{Z}/3\mathbb{Z}}$ (quindi $x-y$ è un elemento nilpotente non banale).

iii) Abbiamo anche visto che x^2+xy+y^2 è irriducibile in $A_{\mathbb{R}}$ (che è un dominio fattorizzazione unica), quindi è primo, quindi genera un ideale primo; dunque il quoziente $A_{\mathbb{R}}$ è un dominio di integrità.
Osserviamo che

$$A_{\mathbb{R}}/(y)\cong\mathbb{R}[x,y]/(x^2+xy+y^2,y)\cong\mathbb{R}[x]/(x^2)$$

che è diverso sia da $\{0\}$ sia da $A_{\mathbb{R}}$ ($\mathbb{R}[x]/(x^2)$ non è un dominio di integrità).
Quindi $A_{\mathbb{R}}$ ha un ideale non banale, dunque non è un campo.
Alternativamente si può osservare che tutti i polinomi appartenenti all'ideale (x^2+xy+y^2,y) di $\mathbb{R}[x,y]$ hanno termine costante nullo, quindi 1 non appartiene a tale ideale; da ciò segue che y è un elemento non nullo e non invertibile in $A_{\mathbb{R}}$ (segue anche che (x^2+xy+y^2,y) è un ideale non banale di $\mathbb{R}[x,y]$). Dunque $A_{\mathbb{R}}$ non è un campo.

iv) Osserviamo preliminarmente che $\mathbb{R}[x]\oplus y\mathbb{R}[x]\subseteq\mathbb{R}[x,y]$ è un insieme di rappresentanti per A_R, cioè che la restrizione a $\mathbb{R}[x]\oplus y\mathbb{R}[x]$ della proiezione canonica $\pi:\mathbb{R}[x,y]\to A_{\mathbb{R}}$ è biunivoca (ed è un omomorfismo di gruppi).
Infatti $y^2=-x^2-xy$ in $A_{\mathbb{R}}$ da cui, per induzione sul grado in y, segue che $\pi\big|_{\mathbb{R}[x]\oplus y\mathbb{R}[x]}$ è suriettiva.
D'altra parte ogni multiplo non nullo di x^2+xy+y^2 ha grado ≥ 2 in y, quindi $ker(\pi\big|_{\mathbb{R}[x]\oplus y\mathbb{R}[x]})=\{0\}$, cioè $\pi\big|_{\mathbb{R}[x]\oplus y\mathbb{R}[x]}$ è iniettiva.
Osserviamo anche che $\{1,\omega\}$ è una base di $\mathbb{C}$ su $\mathbb{R}$, quindi $\mathbb{C}[t]=\mathbb{R}[t]\oplus\omega\mathbb{R}[t]$.

Per costruire un isomorfismo tra il campo dei quozienti di $A_{\mathbb{R}}$ (che denotiamo $\mathcal{Q}$) e $\mathbb{C}(t)$ (che è il campo dei quozienti di $\mathbb{C}[t]$) cominciamo con il costruire un omomorfismo iniettivo di anelli $A_{\mathbb{R}}\to\mathbb{C}[t]$, cioè un omomor-

fismo $f : \mathbb{R}[x, y] \to \mathbb{C}[t]$ tale che $ker(f) = (x^2+xy+y^2)$: costruiamo f come l'omomorfismo definito univocamente dalle seguenti condizioni:

$f\big|_{\mathbb{R}}$ è l'immersione di $\mathbb{R}$ in $\mathbb{C} \subseteq \mathbb{C}[t]$;

$f(x) = t \in \mathbb{C}[t]$;

$f(y) = \omega t \in \mathbb{C}[t]$.

Poiché $f(x^2+xy+y^2) = (1+\omega+\omega^2)t^2 = 0$, l'ideale (x^2+xy+y^2) è contenuto in $ker(f)$, quindi f induce un omomorfismo di anelli $\bar{f} : A_{\mathbb{R}} \to \mathbb{C}[t]$.

Per dimostrare che $\bar{f}$ è iniettivo basta verificare che $f\big|_{\mathbb{R}[x]\oplus y\mathbb{R}[x]}$ è iniettiva: dati $p(x),\ q(x) \in \mathbb{R}[x]$ abbiamo $f(p(x) + yq(x)) = p(t) + \omega tq(t)$, quindi $p(x) + yq(x) \in ker(f) \Leftrightarrow p(t) + \omega tq(t) = 0 \Leftrightarrow p(t) = tq(t) = 0 \Leftrightarrow p = q = 0$.

Ne segue che la composizione $A_{\mathbb{R}} \overset{\bar{f}}{\hookrightarrow} \mathbb{C}[t] \hookrightarrow \mathbb{C}(t)$ è un omomorfismo iniettivo di un dominio in un campo, quindi induce un omomorfismo di campi $\tilde{f} : \mathcal{Q} \to \mathbb{C}(t)$.

Poiché tutti gli omomorfismi di campo sono iniettivi, per provare che $\tilde{f}$ è un isomorfismo basta provarne la suriettività:

è ovvio che $\mathbb{R} \subseteq Im(\tilde{f})$, perché $\tilde{f}(\mathbb{R}) = f(\mathbb{R}) = \mathbb{R} \subseteq \mathbb{C}$;

$\omega = \frac{f(y)}{f(x)} = \frac{\bar{f}(y)}{\bar{f}(x)} = \tilde{f}(\frac{y}{x})$;

$t = f(x) = \tilde{f}(x)$.

Quindi $\mathbb{C}[t] \subseteq Im(\tilde{f})$, da cui la tesi perché $Im(\tilde{f})$ è un campo e $\mathbb{C}(t)$ è il minimo campo che contiene $\mathbb{C}[t]$.