ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 03/03/2026 ore 14.00 - aula 1200

1) Risolvere il sistema di equazioni

$$\begin{cases} 5x \equiv 4 \pmod 9 \\ 7x \equiv 8 \pmod{11}. \end{cases}$$

2) Quanti sono gli omomorfismi di gruppi da $(\mathbb{Z}/14\mathbb{Z}, +)$ a $(\mathbb{Z}/21\mathbb{Z}, +)$? Determinarli tutti.
Quanti sono gli omomorfismi di anelli unitari da $(\mathbb{Z}/14\mathbb{Z}, +, \cdot)$ a $(\mathbb{Z}/21\mathbb{Z}, +, \cdot)$?

3) Fattorizzare in irriducibili il polinomio $p(x) = x^4 - 2x^3 + 2x^2 - 2x + 1 \in \mathbb{R}[x]$ e dimostrare che esiste un anello A tale che

$$\mathbb{R}[x]/(p(x)) \cong \mathbb{C} \times A.$$

In A ci sono elementi nilpotenti non banali? A è un campo?

4) Siano:
$\mathbb{Z}_+$ l'insieme dei numeri interi positivi;
P l'insieme dei numeri primi positivi;
$\mathscr{P}(P)$ l'insieme delle parti di P;
$\sim$ la relazione definita in $\mathbb{Z}_+$ nel modo seguente:

$$n \sim m \Leftrightarrow \exists r \in \mathbb{N} \text{ tale che } n|m^r \text{ e } m|n^r.$$

Dimostrare che $\sim$ è una relazione di equivalenza e descrivere l'insieme quoziente $\mathbb{Z}_+/\sim$ come sottoinsieme di $\mathscr{P}(P)$.

ESAME SCRITTO di ALGEBRA 1 - a.a. 2024/25
Roma, 23/02/2026 ore 10.00 - aula 1

SOLUZIONI

1) Poiché $(9,5)=1$, l'equazione $5x \equiv 4 \pmod 9$ è risolubile e ha una sola soluzione modulo 9; osserviamo che $4 = -5$, quindi la soluzione di tale equazione è $x \equiv -1 \pmod 9$.

Alternativamente si può osservare che l'inverso di 5 in $\mathbb{Z}/9\mathbb{Z}$ è 2, quindi la soluzione di questa equazione è $x = 2 \cdot 4 = 8 \pmod 9$.
Analogamente poiché $(11,7)=1$, l'equazione $7x \equiv 8 \pmod{11}$ è risolubile e ha una sola soluzione modulo 11; osservando che $7 \equiv -4 \pmod{11}$ troviamo che la soluzione di tale equazione è $x \equiv -2 \pmod{11}$.

Anche in questo caso possiamo risolvere l'equazione calcolando l'inverso di 7 in $\mathbb{Z}/11\mathbb{Z}$ (che è -3), quindi la soluzione di $7x \equiv 8 \pmod{11}$ è $x = -3 \cdot 8 \equiv -2 \pmod{11}$.
Poiché $(9,11)=1$, il sistema

$$\begin{cases} x \equiv -1 \pmod 9 \\ x \equiv -2 \pmod{11} \end{cases}$$

(equivalente al sistema dato) è risolubile e ha una (sola) soluzione modulo 99.
$9 \cdot 5 - 11 \cdot 4 = 1$ (identità di Bézout per 9 e 11) implica che $-11 \cdot 4(-1) + 9 \cdot 5(-2)$ è congruo a -1 modulo 9 ed è congruo a -2 modulo 11.
Quindi la soluzione del sistema dato è

$$x \equiv 44 - 90 \equiv 53 \pmod{99}.$$

2) $\mathbb{Z}/14\mathbb{Z}$ è un gruppo ciclico generato da 1, quindi un omomorfismo di gruppi $f : \mathbb{Z}/14\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ è determinato dall'immagine di 1: $f(n) = nf(1)$.
1 ha ordine 14 in $\mathbb{Z}/14\mathbb{Z}$; gli ordini degli elementi di $\mathbb{Z}/21\mathbb{Z}$ sono i divisori di 21.
Quindi un elemento di $\mathbb{Z}/21\mathbb{Z}$ può essere immagine di $1 \in \mathbb{Z}/14\mathbb{Z}$ se e solo se il suo ordine divide 14 e 21, cioè se e solo se il suo ordine divide 7. Gli elementi di $\mathbb{Z}/21\mathbb{Z}$ con questa proprietà sono i multipli di 3, cioè gli elementi di $3\mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z}$.
Ne segue che $\#Hom_{gr}(\mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}) = \#(3\mathbb{Z}/21\mathbb{Z}) = 7$ e che gli omomorfismi cercati sono le funzioni $f_a : \mathbb{Z}/14\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ definiti da $f_a(n) = 3na$ al variare di a in $\mathbb{Z}/7\mathbb{Z}$, dove il prodotto per 3 è l'isomorfismo tra $\mathbb{Z}/7\mathbb{Z}$ e $3\mathbb{Z}/21\mathbb{Z} \subseteq \mathbb{Z}/21\mathbb{Z}$.

Un omomorfismo di anelli unitari è un omomorfismo di gruppi che conserva il prodotto e mappa 1 in 1. Ma 1 non è multiplo di 3 in $\mathbb{Z}/21\mathbb{Z}$ quindi non esistono omomorfismi di anelli unitari da $\mathbb{Z}/14\mathbb{Z}$ a $\mathbb{Z}/21\mathbb{Z}$.

3) $p(1) = 0$ quindi $p(x)$ è divisibile per $x-1$; si ha $\frac{p(x)}{x-1} = x^3 - x^2 + x - 1$ che a sua volta è divisibile per $x-1$: $x^3 - x^2 + x - 1 = (x-1)(x^2+1)$.
$(x-1)$ e (x^2+1) sono irriducibili (non associati) in $\mathbb{R}[x]$, dunque

$$p(x) = (x-1)^2(x^2+1)$$

è la fattorizzazione in irriducibili di $p(x)$; inoltre il teorema cinese implica che

$$\mathbb{R}[x]/(p(x)) \cong \mathbb{R}[x]/((x-1)^2) \times \mathbb{R}[x]/(x^2+1).$$

Poiché $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ abbiamo che

$$\mathbb{R}[x]/(p(x)) \cong \mathbb{C} \times \mathbb{R}[x]/((x-1)^2),$$

quindi l'anello A è

$$A = \mathbb{R}[x]/((x-1)^2).$$

In A si ha $x-1 \neq 0$ e $(x-1)^2 = 0$, quindi $x-1$ è un elemento nilpotente non banale di A.
In particolare $x-1$ non è invertibile, quindi A non è un campo.

4) Sia $n \in \mathbb{Z}_+$: allora $n|n = n^1$ quindi $n \sim n$; dunque $\sim$ è riflessiva.
La simmetria di $\sim$ è evidente dalla definizione.
Siano $n, m, l \in \mathbb{Z}_+$ tali che $n \sim m$ e $m \sim l$: allora esistono $r, s \in \mathbb{N}$ tali che $n|m^r$, $m|n^r$, $m|l^s$, $l|n^s$. Ne segue che $n|m^r|(l^s)^r = l^{rs}$ e $l|n^s|(m^r)^s = m^{rs}$.
Questo significa che $m \sim l$, dunque $\sim$ è transitiva.
Abbiamo così provato che $\sim$ è una relazione di equivalenza.
Osserviamo che $n|m^r$ se e solo se i divisori primi di n sono anche divisori primi di m. Quindi $n \sim m$ se e solo se n e m hanno gli stessi divisori primi.
Consideriamo la funzione $f : \mathbb{Z}_+ \to \mathscr{P}(P)$ definita da $f(n) = \{p \in P \text{ t.c. } p|n\}$.
Per quanto visto finora $f(n) = f(m)$ se e solo se $n \sim m$, quindi f induce una funzione iniettiva $\bar{f} : \mathbb{Z}_+/\sim \to \mathscr{P}(P)$, la cui immagine coincide con l'immagine di f.
Ora ogni intero è divisibile solo per un numero finito di primi; viceversa dato un insieme finito di numeri primi positivi $\{p_1, ..., p_r\}$ si ha che $f(p_1 \cdot ... \cdot p_r) = \{p_1, ..., p_r\}$.
Dunque $Im(\bar{f}) = Im(f) = \{X \subseteq P | \#X < \infty\}$.
Ne segue che $\mathbb{Z}_+/\sim \cong \{X \in \mathscr{P}(P) | \#X < \infty\}$ è la richiesta descrizione di $\mathbb{Z}_+/\sim$ come sottoinsieme di $\mathscr{P}(P)$.