Corso di laurea Matematica
Algebra 2
a.a. 2025–26
Scritto 20 gennaio 2026

Svolgere i seguenti esercizi. Le risposte vanno giustificate con brevità e chiarezza.

1. Sia $G = \{x \in \mathbb{Q} \mid x > 0\}$. Provare che G è un sottogruppo di $(\mathbb{Q} \setminus \{0\}, \cdot)$. Descrivere le classi laterali di G in $\mathbb{Q} \setminus \{0\}$ e dire chi è il gruppo quoziente $(\mathbb{Q} \setminus \{0\})/G$.

2. Provare che $x^p + p - 1 \in \mathbb{Z}[x]$ è irriducibile per ogni numero primo p.

3. Usando il metodo di Berlekamp, (ma non solo!) scomporre in fattori irriducibili il polinomio $x^{20} + 2 \in \mathbb{Z}_5[x]$.

4. Provare che l'elemento $\sqrt[3]{2+\sqrt{2}} \in \mathbb{C}$ è algebrico su $\mathbb{Q}$ e trovare il suo polinomio minimo.

5. Siano K, L campi, con L estensione di K. Si supponga che $[L : K] = p$ con p numero primo. Provare che non esiste nessun campo K' che sia intermedio tra K ed L (cioè che sia estensione di K e sottocampo di L), oltre ovviamente a K ed L.

1) Sia $g, h \in G$ $g>0$ e $h>0$ quindi $gh>0$ quindi $gh \in G$.
Se $1>0$ quindi $1 \in G$.
Sia $g \in G$ allora $g>0$ quindi $\tilde{g}>0 \Rightarrow \tilde{g} \in G$
I laterali di G in $\mathbb{Q}\setminus\{0\}$ sono G e $-G = \{x \in \mathbb{Q} \mid x<0\}$
infatti se Gh è un laterale, è della forma $\{gh \mid g \in G\}$
e $\{gh \mid g \in G\} = G$ se $h>0$ ed è $-G$ se $h<0$.
Sia $C_2 = \{-1, 1\}$ il gruppo ciclico di ordine 2 (rispetto al prodotto)
Sia $\varphi : \mathbb{Q}\setminus\{0\} \to C_2$ data da $\varphi(x) = \text{segno di } x = \frac{x}{|x|}$.
φ è omom. di gruppi $\left(\varphi(gh) = \frac{gh}{|gh|} = \frac{g}{|g|}\cdot\frac{h}{|h|} = \varphi(g)\cdot\varphi(h)\right)$
è suriettiva e $\ker\varphi = G$. Quindi $\mathbb{Q}\setminus\{0\}/G$ è isomorfo al gruppo ciclico C_2.

2). Sia $f : \mathbb{Z}[x] \to \mathbb{Z}[x]$ data da $f(a)=a$ $\forall a \in \mathbb{Z}$, $f(x) = x+1$
Per teo. che estende f è (si estende a) un omom. di anelli.
Inoltre, definendo $g : \mathbb{Z}[x] \to \mathbb{Z}[x]$ con $g(a) = a$ $\forall a \in \mathbb{Z}$ e
$g(x) = x-1$ si vede che g è omomorfismo di anelli e g è
inverso di f. Quindi f è isomorfismo di anelli.

$$f(x^p + p - 1) = (x+1)^p + p - 1 = x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \dots + \binom{p}{p-1}x + 1 + p - 1$$

$$= x^p + px(q(x)) + p. \quad (q(x) \in \mathbb{Z}[x])$$

Nell'ultimo passaggio si usa il fatto che se p è primo, p divide
$\binom{p}{i}$ per ogni $i = 1, \dots, p-1$
Il polinomio $x^p + px \cdot q(x) + p$ è irriducibile per Eisenstein,
quindi, essendo f un isomorfismo, anche $x^p + p - 1$ è irriducibile in $\mathbb{Z}[x]$

3) $x^{20} + 2 \in \mathbb{Z}_5[x]$. Per piccolo teorema di Fermat $2^5 = 2$ in $\mathbb{Z}_5$
quindi $x^{20} + 2 = (x^4)^5 + 2^5 = (x^4 + 2)^5$ in $\mathbb{Z}_5[x]$.
Si tratta allora di fattorizzare $x^4 + 2$ con Berlekamp.

$p=5$ $d=4$ Si tratta di trovare i resti di $x^{i\cdot p}$ $(i=0,1,\dots,d-1)$ quando viene diviso per x^4+2.

$x^0 = 0\cdot(x^4+2)+1$ $\qquad$ $x^5 = x^4\cdot x \equiv 3x \mod x^4+2$.

$x^{10} \equiv 4x^2 \mod x^4+2$ $\qquad$ $x^{15} \equiv 2x^3 \mod x^4+2$.

Quindi la matrice Q vale: $Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$. $Q-I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Quindi $\ker(Q-I) = \left\{ \begin{pmatrix} l_0 \\ l_1 \\ l_2 \\ l_3 \end{pmatrix} \;\middle|\; 2l_1=0,\ 3l_2=0,\ l_3=0 \right\}$ e pertanto una base di $\ker(Q-I)$ è il vettore $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. In particolare $\dim \ker(Q-I)=1$ inoltre il polinomio x^4+2 non è libero da quadrati ($\operatorname{mcd}(x^4+2, 3x^3)=1$) quindi x^4+2 è irriducibile. Quindi $(x^4+2)^5$ è la scomposizione in fattori irriducibili del polinomio $x^{20}+2$.

4). Sia $a = \sqrt[3]{2+\sqrt{2}}$ allora $a^3 = 2+\sqrt{2} \Rightarrow a^3-2 = \sqrt{2} \Rightarrow$ $(a^3-2)^2 = 2 \Rightarrow a^6-4a^3+2=0$. Pertanto a è soluzione del polinomio monico $x^6-4x^3+2 \in \mathbb{Q}[x]$. Tale polinomio è irriducibile per Eisenstein, quindi è il polinomio minimo, su $\mathbb{Q}$, di $\sqrt[3]{2+\sqrt{2}}$.

5). Sia K' campo intermedio, quindi $L : K' : K$. Per teorema della torre $[L:K] = [L:K']\cdot[K':K]$. Quindi $[L:K']\cdot[K':K]=p$. essendo p primo $[L:K']=p$, $[K':K]=1$ o $[L:K']=1$, $[K':K]=p$. Nel primo caso $K'=K$, nel secondo caso $K'=L$.