es. 1)

a) Sia $K \subseteq F$ un'estensione finita t.c. $[F : K] = 2^n$, $n \in \mathbb{N}$. Dim. che $\forall f \in K[x]$ t.c. $\deg f = 3 \wedge$ f ha uno zero in F, possiede già uno zero in K

$\Rightarrow$ sia $\alpha \in F$ t.c. $f(\alpha) = 0_F$

$\Rightarrow$ il polinomio minimo h di α divide f

$\Rightarrow \deg h \leqslant 3$

$\Rightarrow$ consideriamo $K \subseteq K(\alpha) \subseteq F$ campo intermedio:

$[K(\alpha) : K]\ 2^m$, $m \leqslant n$

$\Rightarrow 2^m \leqslant 3 \Rightarrow m = 0 \vee m = 1$

$\Rightarrow$ se $m = 0$, $2^m = 1$ e $\alpha \in K$ ✓

$\Rightarrow$ se $m = 1$, $2^m = 2$ e f è divisibile per h

$\Rightarrow f = h \cdot g$ con $\deg g = 1 \Rightarrow g$ ha uno zero in $K \Rightarrow f$ ha uno zero in K

b) Sia $K \subseteq K(\alpha)$ estensione di deg dispari. Dim. che $K(\alpha) = K(\alpha^2)$

$\Rightarrow K(\alpha^2) \subseteq K(\alpha)$ $(\alpha^2 = \alpha \cdot \alpha)$

$\Rightarrow \underbrace{K \subseteq K(\alpha^2) \subseteq K}_{\deg\, =\, 2n+1}(\alpha)$

$\Rightarrow [K(\alpha) : K(\alpha^2)] = 2n + 1$

$\Rightarrow \alpha$ è radice di $X^2 - \alpha^2 \in K(\alpha^2)[X]$

$\Rightarrow [K(\alpha) : K(\alpha^2)] \leqslant 2 \Rightarrow 2n+1 \leqslant 2 \Leftrightarrow n = 0$

$\Rightarrow [K(\alpha) : K(\alpha^2)] = 1$

c) Sia $u = \sqrt{3} + i\sqrt{2}$. È vero che $\mathbb{Q}(u) = \mathbb{Q}(u^2)$

$\Rightarrow u^2 = 3 - 2 + 2i\sqrt{6} \iff u^2 - 1 = 2i\sqrt{6}$

$\iff u^4 - 2u^2 + 25 = 0 \Rightarrow u$ è radice di $x^4 - 2x^2 + 25$

$\Rightarrow f(x) = x^4 - 2x^2 + 25$ è irriducibile (riduzione mod 7)

quindi è il polinomio minimo

$\Rightarrow [\mathbb{Q}(u) : \mathbb{Q}] = 4$

$\Rightarrow$ Calcoliamo $[\mathbb{Q}(u) : \mathbb{Q}(u^2)]$:

$\mathbb{Q} \subseteq \mathbb{Q}(u^2) \subseteq \mathbb{Q}(u) \Rightarrow [\mathbb{Q} : \mathbb{Q}(u^2)] = ?$

$\Rightarrow u^2$ è radice di $x^2 - 2x + 25$

$\Rightarrow \frac{\Delta}{4} = -24 < 0 \Rightarrow$ è irriducibile in $\mathbb{Q}$

$\Rightarrow f(x) = x^2 - 2x + 25$ è il polinomio minimo di u^2 su $\mathbb{Q}$

$\Rightarrow [\mathbb{Q} : \mathbb{Q}(u^2)] = 2 \Rightarrow [\mathbb{Q}(u) : \mathbb{Q}(u^2)] = 2 \neq 1$

$\Rightarrow \mathbb{Q}(u) \neq \mathbb{Q}(u^2)$

---

es. 2)

Sia λ una fissata radice cubica di 3, e sia $\alpha = \lambda + \lambda^2$

a) Verificare che α è algebrico su $\mathbb{Q}$ e trovare il suo polinomio minimo $f(x) \in \mathbb{Q}$

$$\begin{aligned}\Rightarrow \alpha^3 &= \lambda^3 + 3\lambda^4 + 3\lambda^5 + \lambda^6 \\ &= \lambda^3(1 + 3\lambda + 3\lambda^2 + \lambda^3) \\ &= 3(1 + 3(\lambda + \lambda^2) + 3) \\ &= 3(4 + 3\alpha)\end{aligned}$$

$\Rightarrow \alpha$ è radice di $f(x) = x^3 - 9x - 12$

$\Rightarrow f$ è irriducibile per Eisenstein ($p = 3$)

b) Verificare che $\mathbb{Q}(\alpha) = \mathbb{Q}(\lambda)$

$\subseteq : \Rightarrow \quad \alpha = \lambda + \lambda^2, \quad \mathcal{B}_{\mathbb{Q}(\lambda)} = \{1, \lambda, \lambda^2\} \Rightarrow \alpha \in \mathbb{Q}(\lambda)$

$\supseteq : \Rightarrow \quad \mathcal{B}_{\mathbb{Q}(\alpha)} = \{1, \alpha, \alpha^2\}, \quad \alpha^2 = \lambda^2 + 2\lambda^3 + \lambda^4$

$= \lambda^2 + 3\lambda + 6$

$\Rightarrow \alpha^2 - \alpha = 3\lambda + 6 - \lambda = 2\lambda + 6$

$\Rightarrow \lambda = \frac{1}{2}(\alpha^2 - \alpha - 6)$ ✓

---

es. 3)

Sia $F = \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{I}$, $I = (x^2 + 2x - 1)$

a) Verificare che F è un campo

$\Rightarrow$ deve essere:

I massimale $\Leftrightarrow$ f irriducibile

$\Rightarrow f(x) = x^2 + 2x - 1$

$\Rightarrow f(0) = -1, \ f(1) = 2, \ f(2) = 2, \ f(3) = -1$

$f(4) = 3$

$\Rightarrow f$ irriducibile $\Rightarrow F$ campo

b) Calcolare $|F|$

$\Rightarrow [F : \mathbb{Z}/5\mathbb{Z}] = 2 \Rightarrow |F| = 5^2 = 25$

c) Verificare che $\overline{x} = x + I$ è radice cubica di $\overline{3} = 3 + I$ in F

$\Rightarrow \overline{x}^3 = \overline{3} \quad \Rightarrow x^3 = x(1 - 2x) = x - 2x^2$

$= x - 2(1 - 2x) = x - 2 + 4x = -2 = 3$

---

es. 4) Vero o falso?

a) Se f è polinomio minimo di un elemento $a \in K$ (K campo) e g è polinomio minimo di un elemento $b \in K$, allora fg è polinomio minimo di $ab \in K$

$\Rightarrow$ FALSO, f, g sono irriducibili MA fg NON lo è

b) Se p è primo, allora $\operatorname{car}(\mathbb{Q}[x]/(x^2-p)) = p$

$\Rightarrow$ FALSO, $\operatorname{car} \mathbb{Q} = 0 \Rightarrow \mathbb{Q}[x]/(x^2-p) \approx \mathbb{Q}(\sqrt{p})$ e $\operatorname{car} \mathbb{Q}(\sqrt{p}) = 0$

---

es. 5)

Sia $f(x) = x^3 + x + 1$, $g(x) = x^2 + x + 1$

a) Scomporre g in polinomi irriducibili in $\mathbb{Z}/3\mathbb{Z}[x]$

$\Rightarrow g(1) = 3 = 0 \Rightarrow g(x) = (x-1)q(x)$

$\Rightarrow g(x) = x^2 - 2x + 1 = (x-1)^2$

b) Scomporre f in polinomi irriducibili in $\mathbb{Z}/3\mathbb{Z}[x]$

$\Rightarrow f(1) = 0 \Rightarrow f(x) = (x-1)q(x)$

$$
\begin{array}{rrrr|l}
x^3 & & +x & +1 & x-1 \\
\cline{5-5}
-x^3 & +x^2 & & & x^2+x-1 \\
\cline{1-4}
// & x^2 & +x & +1 & \\
 & -x^2 & +x & & \\
\cline{2-4}
 & // & 2x & +1 & \\
 & & -2x & -1 & \\
\cline{3-4}
 & & // & // &
\end{array}
$$

$\Rightarrow f(x) = (x-1)(x^2+x-1) = (x-1)(x^2-4x+4)$

$\overset{!}{=} (x-1)(x-2)^2$

c) Calcolare $MCD\{f, g\}$ in $\mathbb{Z}/3\mathbb{Z}[x]$

$$\Rightarrow f(x) = (x+2)\, g(x) + \underbrace{(x-1)}_{=: r(x)}$$

$$\Rightarrow MCD\{f, g\} = x-1$$

d) Calcolare $MCD\{f, g\}$ in $\mathbb{Z}/2\mathbb{Z}[x]$

$$\Rightarrow f(x) = x^3+x+1 \ , \ g(x) = x^2+x+1$$

$$\begin{array}{rrrr|l} x^3 & & +x & +1 & x^2+x+1 \\ \cline{5-5} -x^3 & -x^2 & -x & & x+1 \\ \cline{1-4} // & -x^2 & // & +1 & \\ & -x^2 & +x & & \\ \cline{2-4} & // & +x & +1 & \end{array}$$

$$\Rightarrow x^2+x+1 = x(x+1)+1$$

$$MCD\{f, g\} = 1$$

---

es. 6) Vero o falso?

a) $\mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/2\mathbb{Z}[x]/(x^4+x^2+1)$ è un'estensione di campi di $\deg = 4$

$\Rightarrow$ x^4+x^2+1 NON ha zeri, tuttavia:

$$(x^2+x+1)^2 = x^4+x^2+1$$

$\Rightarrow$ NON è irriducibile $\Rightarrow$ NON è un campo $\Rightarrow$ FALSO

b) $(2x+1)$ è massimale di $\mathbb{Q}[x]$

$\Rightarrow$ VERO ($2x+1$ è irriducibile)

c) $\bar{x}^2$ è invertibile in $\mathbb{Q}[x]/((x^2+1)(x-1))$

$$f(x) = (x^2+1)(x-1) = x^3-x^2+x-1$$

$$\Rightarrow \begin{array}{c|l} x^3-x^2+x-1 & x^2 \\ \cline{2-2} \vdots & x-1 \\ x-1 & \end{array}$$

$\Rightarrow x^3 - x^2 + x - 1 = x^2(x-1) + (x-1)$

$\Rightarrow$ $x^2 \;|\; x-1$, quoziente $x+1$, resto 1 $\Rightarrow x^2 = (x-1)(x+1) + 1$ MCD

$\Rightarrow$ VERO: $\bar{x}^2$ è invertibile

$\Rightarrow 1 = x^2 - (x-1)(x+1) = x^2 - \left(\left(x^3 - x^2 + x - 1\right) - x^2(x-1)\right)(x+1) = x^2 - (x+1)f + (x^2-1)x^2$

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

$\Rightarrow$ in $\mathbb{Q}[x]/\left((x^2+1)(x-1)\right)$: $\bar{1} = \bar{x}^2 \cdot \bar{x}^2$

$\Rightarrow (\bar{x}^2)^{-1} = \bar{x}^2$

d) Un divisore di $0 \in R$ anello NON è MAI invertibile

$a \neq 0$ t.c. $\exists b \neq 0$ con $ab = 0$

$\Rightarrow$ se a è invertibile:

$a^{-1}ab = a^{-1}0 \Rightarrow b = 0$ ↯ a NON è divisore di 0

$\Rightarrow$ FALSO