Estensioni normali:

es. 1)

Costruire un CRC K del polinomio $f(x) = x^3 + 2x + 1$ su $F = \mathbb{Z}/3\mathbb{Z}$. L'estensione $F \subseteq K$ è normale?

$\Rightarrow$ consideriamo $K_0 = F(\alpha) = F[x]/(f)$ con α radice di f

(f è irriducibile: $f(0) = f(1) = f(2) = 1 \neq 0$)

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

$\Rightarrow$ $x^2 + \alpha x + \alpha^2 + 2 = x^2 - 2\alpha x + \alpha^2 + 2 = (x-\alpha)^2 + 2$

$= (x-\alpha)^2 - 1 = (x - \alpha + 1)(x - \alpha - 1)$

$\Rightarrow$ f si fattorizza completamente

$\Rightarrow$ $K_0 = K$ è CRC di f

$\Rightarrow$ $F \subseteq K$ è NORMALE se e solo se ogni polinomio in $F[x]$ avente una radice in K fattorizza completamente in $K[x]$ ($\Leftrightarrow$ è CRC di un polinomio non costante $f(x) \in F[x]$)

$\Rightarrow$ K è normale

---

es. 2)

Quali delle seguenti estensioni sono normali?

a) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-5})$:

$\Rightarrow$ $\sqrt{-5}$ è radice di $x^2 + 5$ $\Rightarrow$ $[\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2$

$\Rightarrow$ ogni estensione di grado 2 è normale

b) $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ con $\alpha = \sqrt[7]{5}$

$\Rightarrow$ α è radice di $x^7 - 5$, irriducibile per Eisenstein

in $\mathbb{Q}$, tuttavia possiede radici complesse non reali
$\Rightarrow \mathbb{Q}(\alpha)$ non è normale

c) $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \sqrt{5})$ con $\alpha = \sqrt[7]{5}$
$\Rightarrow x^2 - 5$ ha radice $\sqrt{5}$
$\Rightarrow [\mathbb{Q}(\alpha, \sqrt{5}) : \mathbb{Q}(\alpha)] \leq 2 \Rightarrow$ è normale

d) $\mathbb{R} \subseteq \mathbb{R}(\sqrt{-7})$:
$\Rightarrow [\mathbb{R}(\sqrt{-7}) : \mathbb{R}] = 2$ dato che $x^2 + 7$ è polinomio minimo di $\sqrt{-7}$
$\Rightarrow$ è normale

e) $\mathbb{C} \subseteq \mathbb{C}(\sqrt{-7})$:
$\Rightarrow \mathbb{C}(\sqrt{-7}) = \mathbb{C} \Rightarrow$ l'estensione ha grado 1
$\Rightarrow$ è normale

Estensioni Separabili:

Ricordiamo che:

1) Un polinomio irriducibile $f \in F[x]$ è separabile se non ha zeri di molteplicità > 1 in alcuna estensione $F \subseteq K \iff f'(x) \neq 0$
2) Un polinomio $f(x)$ è separabile se lo sono tutti i suoi fattori irriducibili
3) Un elemento algebrico $\alpha \in K$ ($F \subseteq K$ estensione di campi) è separabile se il suo polinomio minimo è separabile in $F[x]$
4) Un'estensione algebrica $F \subseteq K$ è separabile se ogni

$\alpha \in K$ algebrico è separabile su F

$\Rightarrow$ Ogni estensione $F \subseteq K$ con $\operatorname{car} F = 0$ è separabile

$\Rightarrow$ Ogni estensione $F \subseteq K$ con $|F| < +\infty$ è separabile

<u>esempio</u> (estensione NON separabile):

$F_0 = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ con p primo.

$\Rightarrow$ consideriamo l'estensione trascendente $F_0(u) = F$

(con u trascendente $\Leftrightarrow$ u non risolve nessuna equazione polinomiale)

$\Rightarrow F = \left\{ \frac{f}{g} \mid f \in F_0[x],\ g \in F_0[u] \setminus \{0\} \right\}$

$\Rightarrow \operatorname{car} F = p \neq 0 \wedge |F| = \infty$

$\Rightarrow$ consideriamo $f(x) = x^p - u \in F[x]$

1) f è irriducibile

2) f ha radici multiple nel CRC K di f su F

<u>Dim.</u>:

2) In K f ha una radice τ $(\tau^p = u)$

$\Rightarrow (x - \tau)^p \overset{\uparrow}{=} x^p - \tau^p = x^p - u = f$

Sogno della matricola

$\Rightarrow$ tutte le radici di f in K sono uguali a τ

1) Supponiamo $f = gh$ con $0 < \deg g < p$, $g, h \in F[x]$

$\Rightarrow$ per l'unicità della fattorizzazione, $g = (x - \tau)^s$

con $0 < s = \deg g < p$

$\Rightarrow \tau^s \in F \Rightarrow s$ è coprimo con p, quindi per Bezout $\exists\, \alpha, \beta$ t.c. $\alpha s + \beta p = 1$

$\Rightarrow \tau^{\alpha s + \beta p} = \underset{\in F}{(\tau^s)^\alpha} \cdot \underset{u \in F}{(\tau^p)^\beta} \in F \Rightarrow \tau \in F$

$\Rightarrow \tau = \frac{v(u)}{w(u)}$ con $v, w \in F[x] \Rightarrow v(u) = \tau \cdot w(u)$

$\Rightarrow (v(u))^p = \tau^p (w(u))^p = u\,(w(u))^p$

$\Rightarrow v(u)^p - u\,w(u)^p = 0$

$\Rightarrow$ i termini di grado massimo NON si elidono ↯

$\Rightarrow f$ è irriducibile

$\Rightarrow f$ NON è separabile

Calcolo di gruppi di automorfismi:

es. 3)

Calcolare i seguenti gruppi di automorfismi

a) $Aut_{\mathbb{R}}(\mathbb{C})$:

$\Rightarrow z \in \mathbb{C} \Rightarrow z = a + ib$, $a, b \in \mathbb{R}$

$\Rightarrow \varphi \in Aut_{\mathbb{R}}(\mathbb{C}) \Rightarrow \varphi(z) = \varphi(\underset{\| \; a}{a}) + \varphi(\underset{\| \; b}{b})\varphi(i)$

$\Rightarrow \varphi(i)^2 = \varphi(i^2) = -1 \Rightarrow \varphi(i) = \pm i$

$\Rightarrow$ se $\varphi(i) = i$, $\varphi = Id$, se $\varphi(i) = -i$, φ è il coniugio di $\mathbb{C}$ $(\varphi(z) = \varphi(\overline{z}))$

b) $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$:

$\Rightarrow \mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mid a, b, c \in \mathbb{Q} \}$

$\Rightarrow \varphi \in Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) \Rightarrow \varphi(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + b\,\varphi(\sqrt[3]{2}) + c\,\varphi(\sqrt[3]{2})^2$

$\Rightarrow \varphi(\sqrt[3]{2})^3 = \varphi(2) = 2 \Rightarrow \varphi(\sqrt[3]{2})$ è radice di $x^3 - 2$

$\Rightarrow \varphi(\sqrt[3]{2}) = \sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}$ con $w = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

$\Rightarrow$ deve essere $\varphi(\sqrt[3]{2}) = \sqrt[3]{2} \Rightarrow \varphi = Id$

c) $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{7}))$:

$\Rightarrow \varphi(a+b\sqrt{7}) = a + b\,\varphi(\sqrt{7}) \Rightarrow \varphi(\sqrt{7})^2 = 7$

$\Rightarrow \varphi(\sqrt{7}) = \pm\sqrt{7} \Rightarrow$ se $\varphi(\sqrt{7}) = \sqrt{7}$, $\varphi = Id$

$\Rightarrow$ se $\varphi(\sqrt{7}) = -\sqrt{7}$, $\varphi(a+b\sqrt{7}) = a - b\sqrt{7}$ che è isomorfismo $(\mathbb{Q}(\sqrt{7}) \cong \mathbb{Q}(-\sqrt{7}))$

$\Rightarrow |Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{7}))| \leq [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$

$\Rightarrow Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{7})) = \{Id, \varphi\}$

d) $Aut_F(F(\tau))$ dove:

$F = \mathbb{F}_p(u) = \left\{ \frac{f}{g} \mid f \in \mathbb{F}_p[x],\ g \in \mathbb{F}_p \setminus \{0\} \right\}$ (p primo),

τ radice di $x^p - u$

$\Rightarrow$ sia $p = 5$, $Aut_F(F(\tau))$

$\Rightarrow$ in $F(\tau)$, $x^p - u = (x - \tau)^p$

$\Rightarrow \varphi(a+b\tau) = a + b\,\varphi(\tau)$ con:

$\varphi(\tau)^p = u \Rightarrow \varphi(\tau)$ è radice di $x^p - u$

$\Rightarrow \varphi(\tau) = \tau \Rightarrow \varphi = Id$

$\Rightarrow Aut_F(F(\tau)) = \{Id\}$

N.B.

Notare che $|Aut_F(F(\tau))| < [F(\tau) : F]$

$\Rightarrow F \subseteq F(\tau)$ NON è separabile (come visto sopra)

MA è normale (è CRC di $x^p - u$)