Martina Cusai 0511845

ESERCIZIO 1:

a.

b. $1, \sqrt[3]{5}, \sqrt[3]{7}, \sqrt[3]{7^2}, \sqrt[3]{35}$

c. Falso, un'estensione di campo per avere un elemento primitivo non può avere caratteristica 0, altrimenti l'estensione sarebbe automaticamente semplice.

d. Vero, $\varphi(n) = 2^s \Rightarrow \varphi(4n) = 2^{s+1}$

e. Sia $\{n_1, n_2, \dots\}$ l'insieme di tutti i numeri interi coprimi positivi non quadratici.
$\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \dots)$ è un'estensione algebrica e infinita

Falso, un'estensione finita è algrica se è anche algebricamente finita

ESERCIZIO 2:

Campo di Spezzamento: Sia F un campo e $0 \neq f \in F[x]$. Un'estensione E di F si dice campo di spezzamento per f su F, se esistono elementi $a_1 \dots a_n \in E$ tali che

(i) $f = a(x-a_1)\dots(x-a_n)$ in $E[x]$ (dove a è il coefficiente direttivo di f)

(ii) $E = F[a_1 \dots a_n]$

Dimostriamo che ogni polinomio a coefficienti in qualsiasi campo ammette un campo di spezzamento:

Sia $f \in F[x]$, $\deg f = n$

~~[illegible]~~ Sia f_1 fattore irriducibile di $f \Rightarrow F_1 := (F[\alpha_1], f_1(\alpha_1) = 0)$

$[F_1 : F] = \deg f_1 \leq n$

Sia f_2 fattore irriducibile di $\frac{f(x)}{x-\alpha_1}$ $\quad (f_2 \in F[\alpha_1][x])$

$\Rightarrow F_2 = F[\alpha_1, \alpha_2] = F_1[\alpha_2]$, $[F_2 : F_1] = \deg f_2 \leq n-1$ $\quad (f_2[\alpha_2] = 0)$

Inoltre, $[F_2 : F] = [F_2 : F_1] \cdot [F_1 : F] \leq n(n-1)$

Itero il procedimento

$\vdots$

f_k fattore irriducibile di $\frac{f_{k}(x)}{(x-\alpha_1)\dots(x-\alpha_{k-1})}$, $f_k \in F_{k-1}[x]$

$\Rightarrow F_k = (F[\alpha_1 \dots \alpha_k], f_k(\alpha_k) = 0)$

$\Rightarrow F_n = F_{n-1}[\alpha_n] = F[\alpha_1 \dots \alpha_n]$, dove f_n fattore irriducibile di $\frac{f(x)}{(x-\alpha_1)\dots(x-\alpha_n)}$

$\Rightarrow f_n = (x-\alpha_n) \Rightarrow \deg(f_n) = 1 \Rightarrow [F_n : F_{n-1}] = 1 \Rightarrow [F_n : F_{n-1}] \leq n!$

$\Rightarrow$ in F_n, f si spezza $\Rightarrow f(x) = (x-\alpha_1)\dots(x-\alpha_n)$, con $f(x) \in F[\alpha_1 \dots \alpha_n][x]$

ESERCIZIO 6:

Teorema Fondamentale della corrispondenza di Galois:

Sia E/F Galois, e sia $G = Gal(E/F)$.

Allora $\{H \leq G\} \xleftrightarrow{1-1} \{M \text{ campo} : F \subseteq M \subseteq E\}$

$$H \longmapsto E^H$$

$$Gal(E/M) \longleftarrow M$$

Inoltre: (i) G corrisponde a F e $\{1\}$ corrisponde a E

(ii) $H_1 \leq H_2 \iff E^{H_1} \supseteq E^{H_2}$

(iii) $\forall \sigma \in G$ • $E^{\sigma H \sigma^{-1}} = \sigma E^H$

• $Gal(E/\sigma M) = \sigma\, Gal(E/M) \sigma^{-1}$

(iv) $H \trianglelefteq G \iff E^H/F$ è un'estensione normale. In tal caso:

$Gal(E^H/F) \cong G/H$

Si fanno delle dimostrazioni separate:

• che sia 1-1 si ha già dimostrato

• $Aut(E/E^H) = H$ deriva dal corollario/proposizione del teorema di Artin

• $E^{Aut(E/M)} = M$ segue dal fatto che se E/F è Galois $\Rightarrow$ anche E/M è Galois $\Rightarrow E^{Aut(E/M)} = M$

ESERCIZIO 4

$x^3 + 5x + 8$ $\quad \mathbb{F}_3[x]$

$\equiv x^3 + 2x + 2 = f$

$f(0) = 2 \neq 0$

$f(1) = 1 + 2 + 2 = 2 \neq 0$ $\quad \Rightarrow f$ irriducibile $[\mathbb{F}_3[x] : \mathbb{F}_3] = 3$

$f(-1) = -1 - 2 + 2 = -2 \neq 0$

$\Delta = -4 \cdot 2^3 - 27 \cdot 8^2 = -2 \equiv 1 = 1^2$

$\Rightarrow$ il campo di Galois è A_3

ESERCIZIO 5

Sottogruppo transitivo di S_n: $G \subset S_n$ si dice transitivo se $\forall a, b \in \{1, \dots, n\}$ $\exists \sigma \in G : \sigma(a) = b$

I sottogruppi transitivi di S_n sono utili nella Teoria di Galois perchè da una loro proposizione:

"Sia $f \in F[x]$ separabile. $G_f \subset S_n$ è transitivo $\Leftrightarrow$ f irriducibile"

otteniamo che:

$f \in \mathbb{Q}[x]$, $\deg f = 3$ irriducibile $\Rightarrow G_f \begin{cases} S_3 \\ A_3 \end{cases}$

$f \in \mathbb{Q}[x]$ irriducibile, $\deg f = 4 \Rightarrow G_f \begin{cases} S_4 \\ C_4 \\ A_4 \\ D_4 \\ V \end{cases}$

ESERCIZIO 7

Il numero di fattori irriducibili di $f = x^{124} - 1$ è il numero di divisori di 124.

$d(124) = \{1, 2, 4, 31, 62, 124\}$ $\qquad$ $\# d(124) = 6$

$\Rightarrow f = \phi_1 \phi_2 \phi_4 \phi_{31} \phi_{62} \phi_{124}$

Su $\mathbb{F}_5$: $x^{124} - 1 = \frac{1}{x}(x^{125} - x) = \frac{1}{x}(x^{5^3} - x)$ $\qquad$ $d(3) = \{1, 3\}$

$\Rightarrow$ i fattori irriducibili di f in $\mathbb{F}_5[x]$ è 44

ESERCIZIO 8

Per trovare il polinomio minimo di $\cos\left(\frac{\pi}{9}\right)$, troviamo prima il polinomio minimo di $\omega = e^{\frac{i\pi}{9}}$

$$\frac{(x^{18}-1)(x^3-1)}{(x^9-1)(x^6-1)} = \frac{x^9+1}{x^3+1} = x^6 - x^3 + 1$$

$\Rightarrow \omega^6 - \omega^3 + 1 = 0 \Rightarrow \omega^3 + \omega^{-3} - 1 = 0$

Sia $\alpha = 2\cos\left(\frac{\pi}{9}\right) \Rightarrow \alpha = \omega + \omega^{-1}$ e $\alpha^3 = \omega^3 + 3\omega + 3\omega^{-1} + \omega^{-3}$

$\Rightarrow \alpha^3 - 3\alpha - 1 = 0$

Quindi il polinomio minimo di $\cos\left(\frac{\pi}{9}\right)$ è $(2x)^3 - 3(2x) - 1$, o equivalentemente

$$x^3 - \frac{3}{4}x - \frac{1}{8}$$

Dimostriamo ora che è algebrico:

$\forall q \in \mathbb{Q}$, $(\cos q\pi) \in \mathbb{R}$ è algebrico

$q = \frac{m}{n} \in \mathbb{Q} \quad m, n \in \mathbb{Z}, n \neq 0$

$\cos(q\pi) = \cos\left(\frac{m}{n}\pi\right)$

$$\left(\cos\left(\frac{m}{n}\pi\right) + i \operatorname{sen}\left(\frac{m}{n}\pi\right)\right)^n = e^{\pi i m} = (-1)^m$$