SOLUZIONI

AL310 AA16/17 (Teoria delle Equazioni) ESAME DI FINE SEMESTRE Roma, 21 Dicembre 2016.

COGNOME .... *NOME* .... *MATRICOLA* ....

Risolvere il massimo numero di esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. *Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Scrivere il proprio nome anche nell'ultima pagina.* 1 Esercizio = 5 punti. Tempo previsto: 2 ore. Nessuna domanda durante la prima ora e durante gli ultimi 20 minuti.

FIRMA	1	2	3	4	5	6	7	8	TOT.
....									

1. Rispondere alle seguenti domande fornendo una giustificazione di una riga:

a. E' vero che il campo di spezzamento su $\mathbf{F}_p$ di $f(X) \in \mathbf{F}_p[X]$ ha sempre $p^{\deg f}$ elementi?

NO. Ad esempio se $f = X^2 \in \mathbb{F}_p[X]$, $(\mathbb{F}_p)_{X^2} = \mathbb{F}_p$ ha p elementi

b. E' vero che per ogni $a \in \mathbf{Q}^*$, il grado $[\mathbf{Q}[a^{1/4}] : \mathbf{Q}] = 4$?

NO. Ad esempio se $a = 4$, $[\mathbb{Q}[4^{1/4}] : \mathbb{Q}] = 2$

c. Quali sono i valori di $b \in \mathbf{Q}^*$, per cui $\mathbf{Q}[b^{1/6}]/\mathbf{Q}$ è Galois.

$b = c^3, c \in \mathbb{Q}$. Infatti $\mathbb{Q}[b^{1/6}] = \mathbb{Q}[\sqrt{c}]$ è Galois su $\mathbb{Q}$ e se $(b^{1/6})^2 \notin \mathbb{Q}$, allora $f_{b^{1/6}}(x)$ ha radici non reali . . .

d. È vero che tutti i gruppi di Galois dei polinomi di grado 5 sono tutti sottogruppi di S_5?

Si. $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \subseteq \mathrm{Sym}(\{\alpha_1, \alpha_2, \ldots, \alpha_5\}) \cong S_5$ dove $f(x) = \prod_{j=1}^{5}(X - \alpha_j)$

2. Fornire un esempio di un polinomio irriducibile di grado sei il cui gruppo di Galois è isomorfo a S_3.

Sia $K = \mathbb{Q}_{x^3-2} = \mathbb{Q}(\sqrt{-3}, 2^{\frac{1}{3}}) = \mathbb{Q}(\sqrt{-3}+2^{\frac{1}{3}})$

Allora $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$

Inoltre $f_{\sqrt{-3}+2^{\frac{1}{3}}}(x) = ((x-\sqrt{-3})^3-2)((x+\sqrt{-3})^3-2)$

$= (x^2+3)^3 - 6(x^3-9x) + 4$

è
- irriducibile
- ha grado 6
- ha gruppo di Galois isomorfo a S_3

3. Sia p un numero primo. Sia $H \subset \mathrm{Gal}(\mathbf{Q}[\zeta_p]/\mathbf{Q})$ l'unico sottogruppo con $(p-1)/2$ elementi. Si determini il periodo di Gauss η_H.

Sia g una radice primitiva mod p.

Allora $H = \langle g^2 \rangle \subseteq \langle g \rangle = U(\mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$

Sappiamo che

$$\eta_{\langle g^2 \rangle} = \sum_{x=1}^{(p-1)/2} e^{\frac{2\pi i x^2}{p}} = -\frac{1}{2} \pm \frac{\sqrt{(-1)^{\frac{p-1}{2}}p}}{2}$$

dove il segno non è stato mai calcolato in classe.

4. Dopo aver dimostrato che $X^2 + 3 \in \mathbf{F}_5[X]$ è irriducibile, si consideri $\mathbf{F}_{5^2} = \mathbf{F}_5[\alpha], \alpha^2 = 2$ e si determinino i generatori.

X^2+3 è irriducibile perchè non ha radici in $\mathbb{F}_5$ $(\pm 1^2+3=4,\ \pm 2^2+3=2,\ 0^2+3=3)$

$\mathbb{F}_5[\alpha]^* = \langle 2+\alpha \rangle$ infatti $(2+\alpha)^{12} = -1$ e $(2+\alpha)^8 = 2(1-\alpha)$

Dunque i generatori sono $(2+\alpha)^k$, $k \in (\mathbb{Z}/24\mathbb{Z})^*$

e cioè

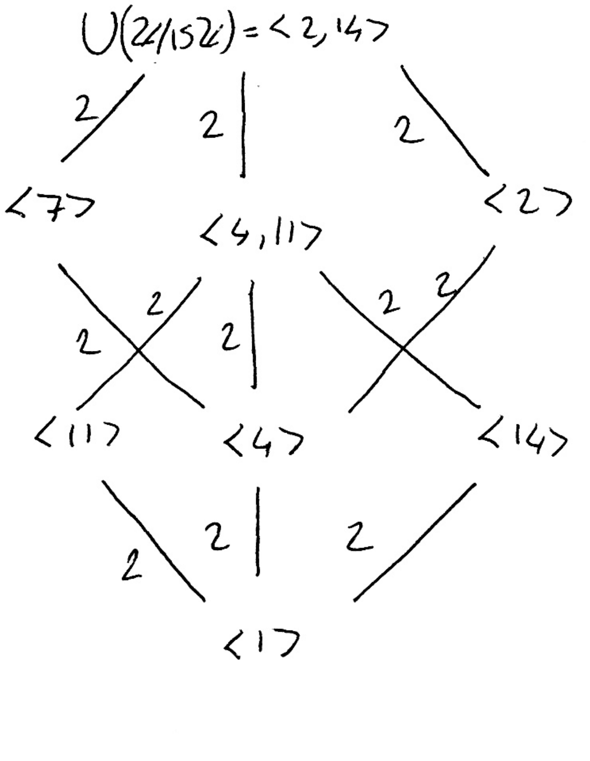
$2+\alpha,\ (2+\alpha)^5,\ (2+\alpha)^7,\ (2+\alpha)^{11}$

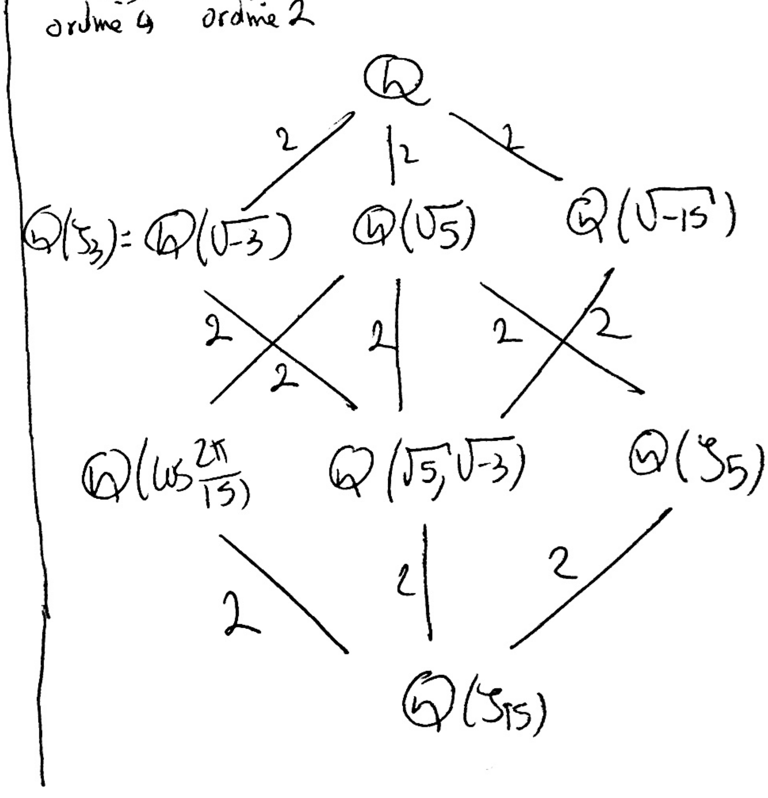
$(2+\alpha)^{13},\ (2+\alpha)^{17},\ (2+\alpha)^{19}$ e $(2+\alpha)^{23}$

5. Descrivere il reticolo dei sottocampi del campo ciclotomico $\mathbf{Q}[\zeta_{15}]$ menzionando i ciascun caso i generatori.

$Gal(\mathbb{Q}[\zeta_{15}]/\mathbb{Q}) \cong U(\mathbb{Z}/15\mathbb{Z}) = \{1,2,4,7,8,11,13,14\} = \langle 14, 2 \rangle \cong C_2 \times C_4$

ordine 4 ordine 2





6. Si enunci nella completa generalità il Teorema di corrispondenza di Galois.

Vedere le note del Milne

7. Dopo aver enunciato il Teorema dell'elemento primitivo, si consideri $E = \mathbf{Q}[\sqrt{3}, \sqrt{-2}, \sqrt{-6}]$. Determinare un elemento primitivo $\gamma \in E$ su $\mathbf{Q}$ e scriverne il polinomio minimo su $\mathbf{Q}$. Descrivere inoltre tutti i sottocampi di E.

$E = \mathbb{Q}[\sqrt{3}, \sqrt{-2}] = \mathbb{Q}[\sqrt{3}+\sqrt{-2}]$ in quanto $\sqrt{-6} = \sqrt{3}\cdot\sqrt{-2}$

e l'orbita $(\sqrt{3}+\sqrt{-2})^{Gal(E/\mathbb{Q})} = \{\pm\sqrt{3}\pm\sqrt{-2}\}$ contiene 4 numeri distinti

~~Pertanto~~ Però $f_{\sqrt{3}+\sqrt{-2}}(x) = ((x-\sqrt{-2})^2 - 3)((x+\sqrt{-2})^2-3)$

$= (x^2+2)^2 - 6(x^2+2) + 9$

$$\begin{tikzcd}
 & E \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{-6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

8. Determinare un numero algebrico il cui polinomio minimo sui razionali ha un gruppo di Galois isomorfo a C_{24}.

Sia $p = 73 = 1 + 24\cdot 3$. Sia g una radice primitiva modulo 73. Allora $Gal(\mathbb{Q}(\zeta_{73})/\mathbb{Q}) \cong U(\mathbb{Z}/73\mathbb{Z}) = \langle g \rangle$

Sia $H = \langle g^{24}\rangle = \{g^{24}, g^{48}, 1\} \leq U(\mathbb{Z}/73\mathbb{Z})$

e sia $\eta_H = \zeta_{73} + \zeta_{73}^{g^{24}} + \zeta_{73}^{g^{48}} \in \mathbb{Q}(\zeta_{73})^H$.

Si ha che $Gal(\mathbb{Q}(\eta_H)/\mathbb{Q}) \cong \dfrac{U(\mathbb{Z}/73\mathbb{Z})}{H}$

$\cong \langle g\rangle / \langle g^{24}\rangle \cong C_{24}$

Pertanto $G_{f_{\eta_H}} \cong C_{24}$