ALGEBRA 2. Seconda prova di esonero
prof. Valentina Barucci
9 giugno 2016

1. Sia $f(x) = x^4 - 9x^2 - 36$.

(a) Se K è il campo di spezzamento di $f(x)$ su $\mathbb{Q}$, allora

$$[K : \mathbb{Q}] = \quad ....$$

Una base di K su $\mathbb{Q}$ è

$$\{..\}$$

(b) Se L è il campo di spezzamento di $f(x)$ su $\mathbb{Q}(\sqrt{3})$, allora

$$[L : \mathbb{Q}(\sqrt{3})] = \quad ....$$

Una base di L su $\mathbb{Q}(\sqrt{3})$ è

$$\{..\}$$

Soluzione: La fattorizzazione in fattori irriducibili di $f(x)$ su $\mathbb{Q}$ è

$$(x^2 + 3)(x^2 - 12)$$

e $K = \mathbb{Q}(i\sqrt{3}, 2\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$. Si ha quindi $[K : \mathbb{Q}] = 4$ e una base di K su $\mathbb{Q}$ è per esempio $\{1, i, \sqrt{3}, i\sqrt{3}\}$.
La fattorizzazione in fattori irriducibili di $f(x)$ su $\mathbb{Q}(\sqrt{3})$ è

$$(x^2 + 3)(x - 2\sqrt{3})(x + 2\sqrt{3}))$$

Si ha quindi $[L : \mathbb{Q}(\sqrt{3})] = 2$ e una base di K su $\mathbb{Q}(\sqrt{3})$ è per esempio $\{1, i\}$.

Altra versione:
Sia $f(x) = x^4 - 6x^2 - 16$.
(a) Se K è il campo di spezzamento di $f(x)$ su $\mathbb{Q}$, allora

$$[K : \mathbb{Q}] = \quad ....$$

Una base di K su $\mathbb{Q}$ è

$$\{..\}$$

(b) Se L è il campo di spezzamento di $f(x)$ su $\mathbb{Q}(\sqrt{3})$, allora

$$[L : \mathbb{Q}(\sqrt{3})] = \quad ....$$

Una base di L su $\mathbb{Q}(\sqrt{3})$ è

$\{$..$\}$

Soluzione: La fattorizzazione in fattori irriducibili di $f(x)$ su $\mathbb{Q}$ è

$$(x^2+2)(x^2-8)$$

e $K = \mathbb{Q}(i\sqrt{2}, 2\sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$. Si ha quindi $[K : \mathbb{Q}] = 4$ e una base di K su $\mathbb{Q}$ è per esempio $\{1, i, \sqrt{2}, i\sqrt{2}\}$.

Su $\mathbb{Q}(\sqrt{3})$, la fattorizzazione in fattori irriducibili di $f(x)$ è la stessa di quella su $\mathbb{Q}$, $[L : \mathbb{Q}(\sqrt{3})] = 4$ e una base è per esempio la stessa di prima, $\{1, i, \sqrt{2}, i\sqrt{2}\}$.

2. Sia ζ una radice primitiva quattordicesima dell'unità.

   (a) Il gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\zeta), \mathbb{Q})$ è isomorfo a:
   C_{14} $\square$ C_8 $\square$ C_6 $\square$ V $\square$ S_3 $\square$

   (b) Scrivere a fianco di ognuno dei seguenti elementi di $\mathbb{Q}(\zeta)$ il corrispondente grado di algebricità su $\mathbb{Q}$:

   $\alpha = \zeta + \zeta^{13}$ ....

   $\beta = \zeta^2 + \zeta^{12}$ ....

   $\gamma = \sum_{n=1}^{6} \zeta^{2n}$ ....

   $\delta = \zeta + \zeta^9 + \zeta^{11}$ ....

   Soluzione. L'estensione $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ è galoisiana di grado 6, poiché $\phi(14) = 6$ (dove ϕ è la funzione di Eulero). I $\mathbb{Q}$-automorfismi di $\mathbb{Q}(\zeta)$, formano un gruppo $G = \mathrm{Gal}(\mathbb{Q}(\zeta), \mathbb{Q})$ isomorfo al gruppo degli invertibili di $\mathbb{Z}_{14}$, $U(\mathbb{Z}_{14}) = \langle \bar{3} \rangle$. Quindi $G = \langle \sigma \rangle$, dove $\sigma : \zeta \to \zeta^3$.

   $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{13})] = 2$, quindi $[\mathbb{Q}(\zeta + \zeta^{13}) : \mathbb{Q}] = 6/2 = 3$ e $\zeta + \zeta^{13}$ è algebrico di grado 3 su $\mathbb{Q}$.

   ζ^2 è una radice primitiva settima dell'unità e $\phi(7) = 6$, quindi la settima e la quattordicesima estensione ciclotomica di $\mathbb{Q}$ coincidono, da cui, ragionando come sopra, si ha che $\zeta^2 + \zeta^{12}$ è algebrico di grado $6/2 = 3$ su $\mathbb{Q}$. $\sum_{n=1}^{6} = \zeta^{2n}\zeta^2 + \zeta^4 + \zeta^6 + \zeta^8 + \zeta^{10} + \zeta^{12}$ è uguale a -1 quindi è algebrico di grado 1 su $\mathbb{Q}$. Infine $\zeta + \zeta^9 + \zeta^{11}$ è fissato da σ^2 che genera un sottogruppo di indice 2 in G. Quindi $\zeta + \zeta^9 + \zeta^{11}$ è algebrico di grado 2 su $\mathbb{Q}$.

3. Sia$K$ un'estensione di grado n di un campo F a caratteristica zero. Allora:

   Esiste in K un elemento α algebrico di grado n su F.

   vero $\bowtie$ falso $\square$

   Ogni elemento di K è algebrico su F

   vero $\bowtie$ falso $\square$

Per ogni divisore d di n esiste in K un elemento algebrico di grado d su F

vero $\square$ falso $\bowtie$

Se esiste in K un elemento algebrico di grado d su F allora d divide n

vero $\bowtie$ falso $\square$

4. Sia α una radice di $x^2 - x + 1 \in \mathbb{Z}_5[x]$, β una radice di $x^2 + x + 1 \in \mathbb{Z}_5[x]$ e γ una radice di $x^2 - 3x + 2 \in \mathbb{Z}_5[x]$.

   Stabilire quali tra i campi $\mathbb{Z}_5(\alpha)$, $\mathbb{Z}_5(\beta)$, $\mathbb{Z}_5(\gamma)$ sono isomorfi tra loro e, in caso di campi isomorfi, costruire esplicitamente un isomorfismo.

   Soluzione. $\mathbb{Z}_5(\alpha)$ e $\mathbb{Z}_5(\beta)$ sono isomorfi perché i corrispondenti polinomi di secondo grado sono irriducibili su $\mathbb{Z}_5$ e quindi sono entrambe isomorfi a $\mathbb{F}_{25}$. Se σ è un isomorfismo di

$$\mathbb{Z}_5[x]/(x^2 - x + 1) \cong \mathbb{Z}_5(\alpha) = \{a_0 + a_1\alpha; a_i \in \mathbb{Z}_5 \text{ e } \alpha^2 - \alpha + 1 = 0\}$$

   in

$$\mathbb{Z}_5[x]/(x^2 + x + 1) \cong \mathbb{Z}_5(\beta) = \{a_0 + a_1\beta; a_i \in \mathbb{Z}_5 \text{ e } \beta^2 + \beta + 1 = 0\}$$

   deve essere

$$0 = \sigma(0) = \sigma(\alpha^2 - \alpha + 1) = \sigma(\alpha)^2 - \sigma(\alpha) + 1$$

   cioè $\sigma(\alpha)$ deve essere una radice di $x^2 - x + 1$ in $\mathbb{Z}_5(\beta)$. Queste sono $-\beta$ e $1 + \beta$: la prima si ottiene facilmente e la seconda si ottiene dividendo $x^2 - x + 1$ per $x - \beta$ in $\mathbb{Z}_5(\beta)[x]$, oppure calcolando $(-\beta)^5$ in $\mathbb{Z}_5(\beta)$. Quindi un isomorfismo di $\mathbb{Z}_5(\alpha)$ in $\mathbb{Z}_5(\beta)$è per esempio quello che manda $a_0 + a_1\alpha$ in $a_0 - a_1\beta$. Si ha invece $\mathbb{Z}_5(\gamma) = \mathbb{Z}_5$ perché $x^2 - 3x + 2 = (x - 1)(x - 2)$.

5. A fianco di ciascun polinomio di $\mathbb{Q}[x]$ scrivere il suo gruppo di Galois (Ricordiamo che per un polinomio della forma $x^3 + px + q$ il discriminnte è $\Delta = -4p^3 - 27q^2$)

   $x^3 - 9x + 9$ ....

   $x^3 + x + 1$ ....

   $x^3 - 7x - 6$ ....

   $x^3 - 2x + 1$ ....

   Soluzione. $x^3 - 9x + 9$ è irriducibile su $\mathbb{Q}$ e il suo discriminante è un quadrato in $\mathbb{Q}$, quindi il gruppo di Galois è il gruppo alterno A_3 .

   $x^3 + x + 1$ è irriducibile su $\mathbb{Q}$, ha una radice reale e due complesse coniugate, quindi il gruppo di Galois è il gruppo simmetrico S_3 .

   $x^3 - 7x - 6 = (x + 1)(x + 2)(x - 3)$, quindi il gruppo di Galois è il gruppo banale $\{id\}$.

$x^3-2x+1=(x-1)(x^2+x-1)$ ha come gruppo di Galois C_2, il ciclico di ordine due.

L'altra versione è simile.

6. E' possibile costruire con riga e compasso:

   il lato di un cubo di volume triplo rispetto a un cubo dato:

   vero $\square$ falso $\bowtie$ Infatti x^3-3 è irriducibile su $\mathbb{Q}$

   il lato di un cubo di volume uguale a otto volte(o a un ottavo) rispetto a un cubo dato:

   vero $\bowtie$ falso $\square$ Infatti $x^3-8=(x-2)(x^2+2x+4)$ in $\mathbb{Q}[x]$ (o $x^3-\frac{1}{8}=(x-\frac{1}{2})(x^2+...)$)

   il lato di un quadrato di area doppia rispetto a un quadrato dato:

   vero $\bowtie$ falso $\square$

   il lato di un triangolo equilatero di area uguale a sette volte rispetto a un triangolo equilatero dato:

   vero $\bowtie$ falso $\square$ Infatti il lato cercato ha lunghezza x tale che $x^2\frac{\sqrt{3}}{2}=7$ cioè $x^2=\frac{14\sqrt{3}}{3}$. Ne segue che x è algebrico di grado 2 su $\mathbb{Q}(\sqrt{3})$, che a sua volta è un'estensione di grado 2 di $\mathbb{Q}$.