Corso di Algebra 2 - a.a. 2014-2015

Prova scritta del 8.7.2015

Esercizio 0.1. *Sia* $P(X) = X^7 - 3X^5 - X^4 - 3X^3 + 3X^2 + 3 \in \mathbb{Q}[X]$.

1. *Determinare una fattorizzazione di* $P(X)$ *in fattori irriducibili su* $\mathbb{Q}[X]$.
2. *Determinare un campo di spezzamento* K *di* $P(X)$ *su* $\mathbb{Q}$.
3. *Determinare il gruppo di Galois di* $P(X)$.
4. *Dire se* $P(X)$ *è risolubile per radicali.*

Soluzione. Osserviamo che

$$P(X) = (X^3 - 1)(X^4 - 3X^2 - 3) = (X - 1)(X^2 + X + 1)(X^4 - 3X^2 - 3).$$

Il polinomio di quarto grado $Q(X) = X^4 - 3X^2 - 3$ è irriducibile per il criterio di Eisenstein, mentre $X^2 + X + 1 = \Phi_3(X)$ è il terzo polinomio ciclotomico. Abbiamo dunque trovato una fattorizzazione di $P(X)$ in fattori irriducibili.

Ora, troviamo le radici del polinomio biquadratico $Q(X)$. Effettuiamo il cambio variabile $Y = X^2$ e risolviamo l'equazione quadratica

$$Y^2 - 3Y - 3 = 0,$$

trovando le soluzioni

$$Y_{1,2} = \frac{3 \pm \sqrt{21}}{2}.$$

Siano allora $\alpha, \beta \in \mathbb{C}$ tali che

$$\alpha^2 = \frac{3 + \sqrt{21}}{2},$$
$$\beta^2 = \frac{3 - \sqrt{21}}{2}$$

Troviamo che $(\alpha\beta)^2 = -3$. Notiamo che $\frac{3+\sqrt{21}}{2} > 0$. Possiamo scegliere $\alpha \in \mathbb{R}$ tale che

$$\alpha\beta = i\sqrt{3}.$$

Quindi, le radici di $Q(X)$ sono date da $\{\pm\alpha, \pm\frac{i\sqrt{3}}{\alpha}\}$, e un suo campo di spezzamento è dato da $K = \mathbb{Q}(\alpha, i\sqrt{3})$. D'altra parte, un campo di spezzamento di $\Phi_3(X)$ è dato da $\mathbb{Q}(i\sqrt{3})$, dunque K è un campo di spezzamento dell'intero polinomio $P(X)$. Calcoliamo il grado dell'estensione:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8,$$

osservando che $[\mathbb{Q}(\alpha, i\sqrt{3}) : \mathbb{Q}(\alpha)] = 2$ poiché $\mathbb{Q}(\alpha)$ è un sottocampo di $\mathbb{R}$ e $i\sqrt{3} \notin \mathbb{R}$.

Ora, poniamo $G = \mathrm{Gal}(K/\mathbb{Q})$, che è un gruppo di ordine 8. Cerchiamo elementi di G definendoli sui generatori α e $i\sqrt{3}$. Iniziamo ponendo:

$$\rho : \begin{cases} \alpha & \mapsto \frac{i\sqrt{3}}{\alpha}, \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases},$$

troviamo un ben definito elemento di G, tale che $\rho^4 = 1$. Poniamo poi

$$\sigma : \begin{cases} \alpha & \mapsto \alpha, \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases}.$$

Abbiamo che $\sigma^2 = 1$. Inoltre, con un calcolo diretto otteniamo la relazione

$$\sigma\rho = \rho^3\sigma.$$

Questo ci assicura che il gruppo G è isomorfo al gruppo diedrale D_4. Da ciò possiamo anche concludere che $P(X)$ è sicuramente risolubile per radicali, poiché il suo gruppo di Galois è risolubile. □

Esercizio 0.2. *Sia $P(X) = X^3 - X + 2 \in \mathbb{F}_7[X]$.*

1. *Determinare il gruppo di Galois di P su $\mathbb{F}_7$.*
2. *Sia $L = \mathbb{F}_7(\alpha)$, dove α è un elemento trascendente su $\mathbb{F}_7$. Mostrare che P è irriducibile su L.*
3. *Determinare il gruppo di Galois di P su L.*

Risoluzione. 1) P è irriducibile in $\mathbb{F}_7[X]$ perché si verifica che non ha radici in $\mathbb{F}_7$, quindi sappiamo che il suo gruppo di Galois è isomorfo ad un sottogruppo transitivo di S_3. Poiché deve anche essere ciclico, è isomorfo ad $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

2) Dato che P ha grado 3 per mostrare che P è irriducibile su L, basta dimostrare che non ha radici in L. Sia $\beta \in L$ una radice di P. Allora esistono due polinomi $g, h \in \mathbb{F}_7[X]$, $h \neq 0$ tali che $\beta = \frac{g(\alpha)}{h(\alpha)}$ e tali che $P(\frac{g(\alpha)}{h(\alpha)}) = 0$. Esplicitando si ottiene

$$\left(\frac{g(\alpha)}{h(\alpha)}\right)^3 - \frac{g(\alpha)}{h(\alpha)} + 2 = 0.$$

Moltiplicando per $h(\alpha)^3$ si ottiene

$$(g(\alpha))^3 - g(\alpha)(h(\alpha))^2 + 2(h(\alpha))^3 = 0.$$

Se poniamo $f(X) = (g(X))^3 - g(X)(h(X))^2 + 2(h(X))^3 \in \mathbb{F}_7[X]$, abbiamo $f(\alpha) = 0$ e poiché α è trascendente su $\mathbb{F}_7$ si deve avere $f = 0$ in $F_7[X]$. In particolare il termine

di grado massimo in X di f deve essere nullo. Sia n il grado di g e m il grado di h, supponiamo che $g(X) = \sum_{i=0,\dots,n} a_i X^i$, $h(X) = \sum_{j=0,\dots,m} b_j X^j$. Se $n > m$ il termine di grado massimo di f è $a_n^3 X^{3n}$, quindi dobbiamo avere $a_n = 0$ che è impossibile perché g ha grado n. Se $m > n$ il termine di grado massimo di f è $2b_m^3 X^{3m}$, quindi dovremmo avere $b_m = 0$ che è impossibile perché h ha grado m. Resta il caso $n = m$. In questo caso il termine di grado massimo di f è

$$x^{3n}(a_n^3 - a_n b_n^2 + 2b_n^3).$$

Pertanto dobbiamo avere $a_n^3 - a_n b_n^2 + 2b_n^3 = 0$. Dividendo per b_n^3 e ponendo $\gamma := \frac{a_n}{b_n} \in \mathbb{F}_7$ otteniamo

$$\gamma^3 - \gamma + 2 = 0,$$

ossia γ è una radice di P in $\mathbb{F}_7$, ma questo è assurdo perché P non ha radici in $\mathbb{F}_7$. Abbiamo quindi dimostrato che P non ha radici in L e quindi è irriducibile in $L[X]$.

3) Sappiamo che P è irriducibile su L quindi il suo gruppo di Galois è isomorfo ad un sottogruppo transitivo di S_3, pertanto o è isomorfo a S_3 o a $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Poiché il discriminante di P è $\Delta = -104 = -7 \cdot 15 + 1 = 1$ perché la caratteristica di L è 7, abbiamo che Δ ha una radice quadrata in L, quindi il gruppo di Galois di P su L è $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

□

Esercizio 0.3. *Sia G un gruppo di cardinalità $25 \cdot 7 \cdot 11$.*

1. *Dimostrare che G ha un sottogruppo normale N ciclico di ordine 77.*
2. *Dimostrare che G è un prodotto semidiretto di N con un gruppo di ordine 25.*
3. *Dare un esempio di un gruppo di cardinalità $25 \cdot 7 \cdot 11$ che non sia abeliano.*

Risoluzione. 1) Il numero degli 11-Sylow è congruo a 1 modulo 11 e divide $|G|$, quindi deve dividere $25 \cdot 7$ e pertanto può solo essere uguale a 1. Dunque esiste un unico 11 - Sylow H che è normale in G.

Il numero dei 7-Sylow è congruo a 1 modulo 7 e divide $|G|$, quindi deve dividere $25 \cdot 11$ e pertanto può solo essere uguale a 1. Dunque esiste un unico 7 - Sylow M che è normale in G.

Allora si ha $HM = MH$ è un sottogruppo di G e M, H sono normali in G. Inoltre $|H \cap M|$ deve dividere sia $|H| = 11$, sia $|M| = 7$, dunque $H \cap M = (e)$ e quindi il sottogruppo $N := HM = MH$ è isomorfo al prodotto diretto $H \times M \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/(77)\mathbb{Z}$. Quindi N è un sottogruppo di G ciclico di ordine 77. Dimostramo che N è normale in G. Sia $g \in G$, $x = hm \in HM$, con $h \in H$, $m \in M$. Abbiamo $gxg^{-1} = (ghg^{-1})(gmg^{-1}) \in HM$ perché $ghg^{-1} \in H$ per la normalità di H, $gmg^{-1} \in M$ per la normalità di M. Quindi N è normale in G e abbiamo visto che è ciclico di ordine 77.

2) Sia K un 5-Sylow di G. La cardinalità di K è 25 e poiché N è normale in G, $NK = KN$ è un sottogruppo di G. Inoltre $|N \cap K|$ deve dividere sia $|N| = 77$ che $|K| = 25$, pertanto $|N \cap K| = 1$ e si ha $|NK| = |N| \cdot |K| = 77 \cdot 25 = |G|$. Quindi G è un prodotto semidiretto di N con K.

3) Consideriamo la seguente azione di $K := \mathbb{Z}/(25)\mathbb{Z} = \langle x \rangle$, con x di ordine 25, sul gruppo $N := \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \langle y, z \mid y^7 = 1,\ z^{11} = 1,\ yz = zy \rangle$:

$$\phi : K \to Aut(\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}),$$

$$\phi(x)(y) = y,\ \phi(x)(z) = z^4.$$

Si vede subito che l'ordine di $\phi(x)$ è 5, quindi l'omomorfismo ϕ è ben definito e non banale, pertanto il prodotto semidiretto $N \rtimes_\phi K$ è un gruppo di ordine $25 \cdot 7 \cdot 11$ non abeliano.

□