Corso di Algebra 2 – a.a. 2013-2014

Prova scritta del 7.7.2014

1. Si determini il gruppo di Galois sui razionali del polinomio $p(X) = X^4 + 4X^2 - 2$.
2. Sia $K = \mathbb{F}_{13}$ il campo con 13 elementi. Indichiamo con $\phi = \phi_{16} \in K[X]$ il sedicesimo polinomio ciclotomico e con L la sedicesima estensione ciclotomica di K, cioè un campo di spezzamento di ϕ su K.
   (a) Decomporre ϕ in fattori irriducibili.
   (b) Calcolare il grado di L su K.
   (c) Calcolare il gruppo di Galois di L su K e descrivere esplicitamente la sua azione sulle radici sedicesime dell'unità.
3. (a) Mostrare che ogni gruppo finito di ordine < 60 è risolubile.
   (b) Trovare un gruppo finito non semplice e non risolubile.

Soluzioni

1. Per cominciare, osserviamo che $p(X)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein applicato al primo 2. Effettuiamo il cambio variabile $Y = X^2$ e risolviamo l'equazione quadratica

$$Y^2 + 4Y - 2 = 0,$$

trovando le soluzioni

$$Y_{1,2} = -2 \pm \sqrt{6}.$$

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

$$\alpha^2 = -2 + \sqrt{6},$$
$$\beta^2 = -2 - \sqrt{6}.$$

Troviamo che $(\alpha\beta)^2 = -2$. Notiamo che $-2 + \sqrt{6} > 0$. Possiamo scegliere $\alpha \in \mathbb{R}$ tale che

$$\alpha\beta = i\sqrt{2}.$$

Allora, le radici di $p(X)$ sono date da $\{\pm\alpha, \pm\frac{i\sqrt{2}}{\alpha}\}$, e un campo di spezzamento è dato da $\mathbb{Q}(\alpha, i\sqrt{2})$. Abbiamo:

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

Sia $G = \mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$. Cerchiamo di fabbricare elementi di G definendoli sui generatori α e $i\sqrt{2}$. Ponendo:

$$\rho : \begin{cases} \alpha & \mapsto \frac{i\sqrt{2}}{\alpha}, \\ i\sqrt{2} & \mapsto -i\sqrt{2} \end{cases},$$

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

$$\sigma : \begin{cases} \alpha & \mapsto \alpha, \\ i\sqrt{2} & \mapsto -i\sqrt{2} \end{cases}.$$

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.

2. $X^{16} - 1 = (X-1)(X+1)(X^2+1)(X^4+1)(X^8+1) = \phi_1(X)\phi_2(X)\phi_4(X)\phi_8(X)(X^8+1)$. Quindi $\phi(X) = X^8 + 1$.

   (a) Il gruppo moltiplicativo di K è ciclico di ordine 12. Quindi -1 è una sesta potenza, e dunque un quadrato; più esattamente, $-1 = 5^2$ in K. Quindi

   $$\phi(X) = (X^4 - 5)(X^4 + 5)$$

   Mostriamo che $P = X^4 - 5$ e $Q = X^4 + 5$ sono irriducibili. Le quarte potenze in K^* sono le radici di $X^3 - 1$, e quindi sono $1, 3, 9$. Ne segue che P e Q non hanno radici in K. Se P o Q fossero della forma $(X^2 + aX + b)(X^2 + cX + d)$ si dovrebbe avere che $c = -a$, $b + d - a^2 = a(d - b) = 0$ e infine $bd = \pm 5$. Se $a \neq 0$ ne seguirebbe che $d = b$, mentre $d = -b$ se $a = 0$. In ogni caso $b^2 = \pm 5$. Ma ± 5 non sono quadrati, dato che $(\pm 5)^6 = (-1)^3 = -1$.

   (b) Sia η una radice di P (oppure di Q); è una radice sedicesima primitiva dell'unità e $L = K[\eta]$. Quindi $[L : K] = 4$.

   (c) Le radici di ϕ sono le potenze η^n con n primo con 16, cioè dispari. Inoltre $(\eta^{4k+1})^4 = 5^{4k+1} = (5^4)^k \cdot 5 = 5$ mentre $(\eta^{4k+3})^4 = 5^3 = -5$. Quindi le radici di P sono le potenze η^n con n congruo a 1 modulo 4 e quelle di Q le potenze η^n con n congruo a 3 modulo 4. Ne segue che il gruppo di Galois cercato è il sottogruppo del gruppo moltiplicativo di $\mathbb{Z}/16\mathbb{Z}$ costituito dalle classi degli interi congrui a 1 modulo 4. Questo gruppo è ciclico di ordine 4 e agisce sulle radici dell'unità per elevamento a potenza.

3. (a) Sia G un gruppo di ordine < 60. Se G ha ordine primo è ciclico, quindi risolubile. Ora procediamo per induzione sull'ordine di G. Se G non ha ordine primo si sa che non è semplice, cioè possiede un sottogruppo normale H diverso da $\{1\}$ e da G. Per ipotesi induttiva i gruppi H e G/H sono risolubili, e quindi anche G è risolubile.

   (b) Consideriamo un gruppo G della forma $A_n \times H$, dove $n \geq 5$ e H è un gruppo non banale. Allora A_n è un sottogruppo normale non banale di G, che quindi non è semplice. Però A_n non è risolubile in quanto è semplice e non abeliano. Quindi G non è risolubile.