Corso di Algebra 2 – a.a. 2012-2013

Prova scritta del 24.9.2013

1. Poniamo $\alpha = \sqrt{4+2\sqrt{3}}$ e $\beta = \sqrt{3+2\sqrt{3}}$.

   (a) Calcolare il grado $\big[\mathbb{Q}[\alpha]{:}\mathbb{Q}\big]$ e il gruppo di Galois $Gal(\mathbb{Q}[\alpha]/\mathbb{Q})$; decidere se $\mathbb{Q}[\alpha]$ è o no una estensione galoisiana di $\mathbb{Q}$.

   (b) Stesse domande per $\mathbb{Q}[\beta]$.

2. Sia $P(X)$ il polinomio X^4+2X^2+2 sul campo $K = \mathbb{F}_p$, dove p è un numero primo. Rispondere alle seguenti domande per $p = 3$ e per $p = 7$:

   (a) Dire se P è irriducibile su K

   (b) Calcolare il gruppo di Galois di P su K

3. Sia p un numero primo. Ricordiamo che, a meno di isomorfismo, esistono esattamente due gruppi di ordine p^2, il gruppo ciclico C_{p^2} e il prodotto $C_p \times C_p$ di due gruppi ciclici di ordine p. Posto $p = 5$ ndichiamo con H il primo di questi gruppi e con K il secondo. Sia m un intero primo con 5. Indichiamo con G un gruppo di ordine $25m^2$.

   (a) Esistono un intero m e un gruppo G che abbia sia H che K come sottogruppi?

   (b) Posto $m = 3$, esistono dei gruppi G non abeliani che contengono H? E che contengono K?

   (c) Posto $m = 13$, esistono dei gruppi G non abeliani che contengono H? E che contengono K?

Soluzioni

1. (a) Notiamo che $\sqrt{3} = (\alpha^2-4)/2$ e quindi $\sqrt{3} \in \mathbb{Q}[\alpha]$. Inoltre $(1+\sqrt{3})^2 = 4+2\sqrt{3}$. Quindi $\alpha = 1+\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$. In conclusione $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}]$. Ne segue che $\big[\mathbb{Q}[\alpha]{:}\mathbb{Q}\big] = 2$, che $Gal(\mathbb{Q}[\alpha]/\mathbb{Q})$è ciclico di ordine 2 e dunque che $\mathbb{Q}[\alpha]$ è di Galois su $\mathbb{Q}$.

   (b) Dato che $\sqrt{3} = (\beta^2-3)/2$, $\mathbb{Q}[\sqrt{3}] \subset \mathbb{Q}[\beta]$. Però $\beta \notin \mathbb{Q}[\sqrt{3}]$. Infatti supponiamo che $3+2\sqrt{3}$ abbia una radice quadrata $\gamma \in \mathbb{Q}[\sqrt{3}]$. Si può scrivere in un unico modo $\gamma = x+y\sqrt{3}$, dove x, y sono numeri razionali. Allora

   $$3+2\sqrt{3} = \gamma^2 = x^2+3y^2+2xy\sqrt{3}$$

   Ne segue che $x^2+3y^2 = 3$ e che $xy = 1$. La seconda di queste relazioni dice che $y = x^{-1}$; sostituendo nella prima e moltiplicando per x^2 si ricava che $x^4-3x^2+3 = 0$. Se ne deduce che

   $$x^2 = \frac{3 \pm \sqrt{9-12}}{2}$$

   Quindi x^2 non è razionale (e nemmeno reale), contro l'ipotesi. In definitiva $\big[\mathbb{Q}[\beta] : \mathbb{Q}[\sqrt{3}]\big] = 2$, e quindi $\big[\mathbb{Q}[\beta]{:}\mathbb{Q}\big] = \big[\mathbb{Q}[\beta]{:}\mathbb{Q}[\sqrt{3}]\big]\,\big[\mathbb{Q}[\sqrt{3}]{:}\mathbb{Q}\big] = 4$.

   Dato che $\mathbb{Q}[\sqrt{3}]$ è una estensione normale di $\mathbb{Q}$, se $\mathbb{Q}[\beta]$ fosse di Galois su $\mathbb{Q}$ ogni elemento di $Gal(\mathbb{Q}[\sqrt{3}]/\mathbb{Q})$ si estenderebbe a un elemento di $Gal(\mathbb{Q}[\beta]/\mathbb{Q})$. Il solo automorfismo

non banale di $\mathbb{Q}[\sqrt{3}]$ è l'automorfismo φ dato da $\varphi(x+y\sqrt{3}) = x - y\sqrt{3}$. Se esistesse un automorfismo η di $\mathbb{Q}[\beta]$ che estende φ dovrebbe valere

$$\eta(\beta)^2 = \eta(\beta^2) = \eta(3+2\sqrt{3}) = \varphi(3+2\sqrt{3}) = 3-2\sqrt{3}$$

Dato che $3-2\sqrt{3} < 0$, $\eta(\beta)$ non può essere reale. Questo è assurdo dato che $\mathbb{Q}[\beta] \subset \mathbb{R}$. Quindi $\mathbb{Q}[\beta]$ non è una estensione di Galois di $\mathbb{Q}$, e $Gal(\mathbb{Q}[\beta]/\mathbb{Q}) = Gal(\mathbb{Q}[\beta]/\mathbb{Q}[\sqrt{3}])$. Quest'ultimo gruppo è il gruppo ciclico di ordine 2 generato dall'automorfismo ξ definito da $\xi(u+v\beta) = u - v\beta$, dove $u, v \in \mathbb{Q}[\sqrt{3}]$.

2. (a) Se P ha radici in K lo stesso è vero per $Q = X^2 + 2X + 2$. Questo accade se e solo se il discriminante di Q è un quadrato in K o anche, dato che il discriminante vale $4 - 8 = -4 = -2^2$, se e solo se -1 è un quadrato in K. Si verifica direttamente che -1 non è un quadrato né modulo 3 né modulo 7. Questo ragionamento mostra anche che non è possibile una fattorizzazione $P = (X^2 - h)(X^2 - k)$ dato che in questo caso h e k sarebbero radici di Q. Resta la possibilità che

$$P = (X^2+aX+b)(X^2+cX+d) = X^4+(a+c)X^3+(ac+b+d)X^2+(ad+bc)X+bd \quad (1)$$

con $a \neq 0$. Se questo accade deve essere $c = -a$ e di conseguenza $ad - ab = 0$, cioè, dato che a non è nullo, $d = b$. Ma allora $2 = b^2$. Ora 2 non è un quadrato modulo 3, e quindi la fattorizzazione (1) è impossibile quando $p = 3$. In conclusione P è irriducibile su $\mathbb{F}_3$. Invece per $p = 7$ si ha che $2 \equiv 3^2 \equiv (-3)^2 \mod p$. Allora la (1) dà $2 = 2b - a^2$ che in quanto equazione in a ha soluzioni $a = \pm 2$ se $b = 3$ (e nessuna soluzione se $b = -3$). In definitiva la decomposizione di P in fattori irriducibili modulo 7 è

$$P = (X^2 + 2X + 3)(X^2 - 2X + 3) \quad (2)$$

(b) Supponiamo che $p = 3$, sia α una radice di P e poniamo $F = K[\alpha]$. Segue da (a) che $[F : K] = 4$. Inoltre F è una estensione di Galois di K e quindi coincide con il campo di spezzamento di P su K. Ne segue che il gruppo di Galois di P è ciclico di ordine 4, generato dall'omomorfismo di Frobenius.

Supponiamo invece che $p = 7$. Il discriminante di ognuno dei due fattori di (2) è $\Delta = 4 - 4 \cdot 3 = -1$. Quindi i due fattori si spezzano completamente su $L = K[\beta]$, dove β è una radice quadrata di -1. D'altra parte $[L : K] = 2$ e quindi in questo caso il gruppo di Galois di P su K è ciclico di ordine 2, sempre generato dall'omomorfismo di Frobenius.

3. (a) No. Infatti H e K sarebbero due 5-sottogruppi di Sylow e perciò dovrebbero essere coniugati, e quindi isomorfi.

(b) Il numero dei 5-sottogruppi di Sylow è congruo a 1 modulo 5 e divide $3^2 = 9$; l'unica possibilità è che valga 1, cioè che vi sia un unico 5-sottogruppo di Sylow, normale, che indichiamo con A. Indichiamo inoltre con B un 3-sottogruppo di Sylow. Il gruppo G è isomorfo al prodotto semidiretto $A \rtimes_\varphi B$, dove φ è un omomorfismo $B \to \mathrm{Aut}(A)$. Questo prodotto è non abeliano se e solo se φ non è l'omomorfismo banale.

Supponiamo dapprima che A sia isomorfo a H, cioè al gruppo ciclico $\mathbb{Z}/(25)$. Si sa che il gruppo degli automorfismi di questo gruppo si identifica al gruppo moltiplicativo $(\mathbb{Z}/(25))^*$, che ha ordine $5(5-1) = 20$. Dato che 20 è primo con 9 l'omomorfismo φ

è necessariamente banale. Non esistono quindi gruppi non abeliani di ordine $5^2 3^2$ che contengano H come sottogruppo.

Supponiamo invece che A sia isomorfo a K, cioè al prodotto $\mathbb{Z}/(5) \times \mathbb{Z}/(5)$. Il gruppo degli automorfismi di questo gruppo si identifica al gruppo delle matrici invertibili 2×2 a coefficienti nel campo $\mathbb{F}_5 = \mathbb{Z}/(5)$. Questo gruppo contiene elementi di ordine 3, ad esempio la matrice

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

e quindi sottogruppi di ordine 3, cioè isomorfi a $\mathbb{Z}/(3)$. D'altra parte B è isomorfo a $\mathbb{Z}/(9)$ o a $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$. In ciascuno di questi due casi vi è un omomorfismo suriettivo $B \to \mathbb{Z}/(3)$, nel primo caso il passaggio al quoziente $\mathbb{Z}/(9) \to (\mathbb{Z}/(9))/((3)/(9)) \cong \mathbb{Z}/(3)$, nel secondo la proiezione su uno dei fattori. Quindi esiste sempre un omomorfismo φ non banale. In altre parole vi è sempre un gruppo non abeliano di ordine $5^2 3^2$ che ha K come sottogruppo.

(c) Il numero dei 5-sottogruppi di Sylow è congruo a 1 modulo 5 e divide $13^2 = 169$; l'unica possibilità è che valga 1, cioè che vi sia un unico 5-sottogruppo di Sylow, normale. Il numero dei 13-sottogruppi di Sylow è congruo a 1 modulo 13 e divide $5^2 = 15$; l'unica possibilità è che valga 1, cioè che vi sia un unico 13-sottogruppo di Sylow, normale. In questo caso dunque G contiene solo due sottogruppi di Sylow, A di ordine 25 e B di ordine 169. Inoltre A e B sono normali. Dato che hanno ordini primi fra loro la loro intersezione è ridotta all'elemento neutro. Ne segue che G è necessariamente isomorfo al prodotto diretto $A \times B$, ed è quindi abeliano dato che sia A che B sono gruppi di ordine p^2 e quindi abeliani.