Corso di Algebra 2 – a.a. 2012-2013

Prova scritta del 28.1.2014

1. Trovare tutti gli interi che sono ordini del centro di qualche gruppo con 63 elementi.

2. Poniamo $P(X) = X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$. Sia L un campo di spezzamento di P su $\mathbb{Q}$.

   (a) Mostrare che $\sqrt{2-\sqrt{2}} \in \mathbb{Q}\left[\sqrt{2+\sqrt{2}}\right]$.

   (b) Calcolare il grado $[L{:}\mathbb{Q}]$ e il gruppo di Galois $Gal(L/\mathbb{Q})$.

   (c) Trovare un elemento primitivo per L su $\mathbb{Q}$.

   (d) Mostrare che P è irriducibile su $\mathbb{Q}[i]$.

3. Sia K un campo e sia L una sua estensione normale. Sia F una estensione finita di K contenuta in L. Sia $\mathcal{I}$ l'insieme degli omomorfismi $\varphi : F \to L$ tali che $\varphi(x) = x$ per ogni $x \in K$. Poniamo

$$E = \bigcap_{\varphi \in \mathcal{I}} \varphi(F)$$

   (a) Mostrare che E è un sottocampo di F contenente K.

   (b) Mostrare che, se M è una estensione normale di K contenuta in F, allora $M \subset E$.

   (c) Mostrare che E è una estensione normale di K.

Soluzioni

1. Sappiamo che il centro di un gruppo finito non può avere indice primo. Quindi a priori il centro di un gruppo G con $63 = 3^2 7$ elementi potrebbe avere ordine 1, 3, 7 o 63. Quest'ultimo caso corrisponde al caso in cui G è abeliano, e quindi si presenta sicuramente. Il numero dei 7-sottogruppi di Sylow di G è congruo a 1 modulo 7 e divide 9, quindi deve essere 1. Ne segue che in ogni caso G ha un unico 7-sottogruppo di Sylow H, che è normale. Indichiamo con K un 3-sottogruppo di Sylow. Il gruppo K ha ordine 3^2 e quindi è abeliano. Il numero dei 3-sottogruppi di Sylow è della forma $1 + 3k$ e divide 7; può quindi valere 1 o 7. Nel primo caso G è prodotto diretto di H e di K e quindi è abeliano, caso che abbiamo già considerato. Resta quindi da vedere se il numero dei 3-sottogruppi di Sylow può essere 7 e quale è l'ordine del centro in questo caso.

   Il gruppo G è un prodotto semidiretto $H \rtimes_f K$, dove $f : K \to \mathrm{Aut}(H)$ è un omomorfismo, non banale se e solo se G non è abeliano. Ora H è ciclico di ordine 7, quindi $\mathrm{Aut}(H)$ si identifica a $(\mathbb{Z}/(7))^*$, che è ciclico di ordine 6. L'ordine di $f(K)$ deve dividere sia l'ordine di K che quello di $\mathrm{Aut}(H)$; quindi se f non è banale $f(K)$ è l'unico sottogruppo di ordine 3 di $\mathrm{Aut}(H)$ e il nucleo di f è un sottogruppo $L < K$ di ordine 3. Questo caso si presenta senz'altro. Infatti K ha un sottogruppo L di ordine 3, ad esempio per il teorema di Cauchy, e K/L ha ordine 3, quindi è isomorfo al sottogruppo di ordine 3 di $\mathrm{Aut}(H)$, e si può prendere come f la composizione di questo isomorfismo con il passaggio al quoziente $K \to K/L$. Dico che il gruppo L, o più esattamente l'insieme degli elementi di $H \rtimes_f K$ della forma $(1, \ell)$ con $\ell \in L$, è il centro di G. Per quanto osservato all'inizio per dimostrarlo basta mostrare che è contenuto nel centro. In effetti

$$(h,k)(1,\ell) = (hf_k(1), k\ell) = (h, k\ell) \quad \text{mentre} \quad (1,\ell)(h,k) = (1 f_\ell(h), \ell k) = (h, k\ell)$$

perché f_ℓ è l'identità e K è abeliano.

In conclusione il centro di G può avere ordine 63 oppure 3.

2. (a) Poniamo $\alpha = \sqrt{2+\sqrt{2}}$ e $\beta = \sqrt{2-\sqrt{2}}$. Notiamo che $\alpha\beta = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{2}$. Inoltre $\alpha^2 = 2+\sqrt{2}$, quindi $\sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}[\alpha]$. Quindi $\beta = \sqrt{2}/\alpha \in \mathbb{Q}[\alpha]$.

   (b) Il polinomio P è di Eisenstein rispetto al primo 2, quindi è irriducibile. Le radici del polinomio $X^2 - 4X + 2$ sono $2 \pm \sqrt{2}$, quindi le quattro radici di P sono $\pm\sqrt{2 \pm \sqrt{2}}$. Per il punto precedente tutte queste radici appartengono al campo $\mathbb{Q}[\alpha]$. Quindi $L = \mathbb{Q}[\alpha]$. Ne segue che $[L:\mathbb{Q}] = \deg(P) = 4$ e dunque che il gruppo di Galois di L su $\mathbb{Q}$ ha ordine 4. Si tratta solo di decidere se è ciclico e un prodotto di due gruppi di ordine 2. Osserviamo che $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset L = \mathbb{Q}[\sqrt{2}][\alpha]$ e che $\alpha^2 \in \mathbb{Q}[\sqrt{2}]$. Quindi $Gal(L/\mathbb{Q}[\sqrt{2}])$ ha ordine 2 ed è generato dall'automorfismo σ che lascia fisso $\mathbb{Q}[\sqrt{2}]$ e manda α in $-\alpha$. Dato che $\mathbb{Q}[\sqrt{2}]$ è normale su $\mathbb{Q}$ il suo automorfismo non banale, che manda $\sqrt{2}$ in $-\sqrt{2}$, si estende a un automorfismo ρ di L. Ora $\rho(\sqrt{2}) = -\sqrt{2}$ e $\rho(\alpha)^2 = \rho(\alpha^2) = 2 - \sqrt{2} = \beta^2$. Quindi $\rho(\alpha) = \pm\beta$. Se $\rho(\alpha) = -\beta$, allora

$$\rho(\beta) = \rho\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{-\sqrt{2}}{-\beta} = \alpha$$

   Dunque, salvo rimpiazzare ρ con ρ^{-1}, possiamo supporre che $\rho(\alpha) = \beta$. Un calcolo analogo a quello appena effettuato mostra che allora $\rho(\beta) = -\alpha$. Ora $\rho^2(\sqrt{2}) = \sqrt{2}$ mentre $\rho^2(\alpha) = \rho(\beta) = -\alpha$. In altre parole, $\rho^2 = \sigma$. Ne concludiamo che ρ ha ordine 4 e che quindi $Gal(L/\mathbb{Q})$ è ciclico di ordine 4 e generato da ρ.

   (c) Per quanto mostrato nel punto precedente un elemento primitivo è $\alpha = \sqrt{2+\sqrt{2}}$.

   (d) Il numero 2 non è primo in $\mathbb{Z}[i]$ dato che $2 = (1+i)(1-i)$. D'altra parte $1+i$ e $1-i$ sono primi e distinti. Quindi il primo $1+i$ divide il termine noto di P ma lo stesso non è vero del suo quadrato, e divide anche 4 dato che divide 2. Il criterio di Eisenstein, relativamente a $1+i$, si applica dunque anche su $\mathbb{Q}[i]$ e prova l'irriducibilità di P.

3. (a) È chiaro che $K \subset E$. Inoltre $\varphi(F)$ è un sottocampo di L per ogni φ. E è un sottocampo di L perché è intersezione di sottocampi.

   (b) Dato che M è normale su K, se $x \in M$ e $\varphi \in \mathcal{I}$ anche $\varphi(x)$ appartiene a M. In altre parole $\varphi(M) \subset M$. Dato però che $[M:K]$ è finito e che $[\varphi(M):K] = [M:K]$ se ne deduce che in effetti $\varphi(M) = M$. Dunque

$$M = \bigcap_{\varphi \in \mathcal{I}} \varphi(M) \subset E$$

   (c) Bisogna mostrare che $\rho(E) \subset E$ per ogni omomorfismo $\rho : E \to L$ che lascia fissi tutti gli elementi di K. Osserviamo innanzitutto che, se N è la chiusura normale di F in L, $[N:K] < +\infty$ e inoltre $\rho(E) \subset N$ per la normalità di N. Salvo rimpiazzare L con N possiamo quindi supporre che L sia finito su K. Sia ρ come sopra. Per la normalità di L su K, ρ si estende a un elemento di $Gal(L/K)$, che continueremo a indicare con ρ. Sia x un elemento di E e sia φ un elemento di $\mathcal{I}$. Vogliamo mostrare che esiste un elemento $a \in F$ tale che $\rho(x) = \varphi(a)$. Osserviamo che $\rho^{-1} \circ \varphi$ è un omomorfismo di F in L. Quindi esiste $a \in F$ tale che $\rho^{-1}(\varphi(a)) = x$. Ma allora

$$\rho(x) = \rho(\rho^{-1}(\varphi(a))) = \varphi(a)$$