Corso di Laurea in Matematica

Soluzioni II compito di ALGEBRA II

8 gennaio 2012

Esercizio 1. *Sia F campo e sia E campo di spezzamento su F del polinomio $x^4+1 \in F[x]$. Si determini il grado $[E:F]$ nei casi*:

1. $F = \mathbb{Q}$;
2. $F = \mathbb{Z}/2\mathbb{Z}$;
3. $F = \mathbb{Z}/5\mathbb{Z}$.

Soluzione. Nel caso $F = \mathbb{Q}$, sia $\zeta = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$ (è una radice primitiva 8-va dell'unità); allora, le radici di x^4+1 sono $\zeta, i\zeta, -\zeta, -i\zeta$ (cioè $\zeta, \zeta^3, \zeta^5, \zeta^7$, le radici primitive 8-ve). Quindi, $E = \mathbb{Q}[\zeta]$ e $[E:\mathbb{Q}] = 4$ (il fatto che x^4+1 è irriducibile in $\mathbb{Q}[x]$ si può provare direttamente facendo la sostituzione $x = y+1$ e applicando Eisenstein).

Sia $F = \mathbb{Z}/2\mathbb{Z}$; allora, applicando l'omomorfismo di Frobenius in $(\mathbb{Z}/2\mathbb{Z})[x]$, si ha $x^4+1 = (x+1)^4$. Quindi $E = \mathbb{Z}/2\mathbb{Z}$.

Nel caso $F = \mathbb{Z}/5\mathbb{Z}$ osserviamo che $x^4+1 = x^4-4 = (x^2+1)(x^2-1)$, e che x^2+1 non ha radici in $\mathbb{Z}/5\mathbb{Z}$. Quindi E coincide con il campo di spezzamento di x^2+2 e pertanto $[E:F] = 2$.

Esercizio 2. *Siano F un campo, E un campo di spezzamento del polinomio $0 \neq f \in F[x]$, e $a \in E$ una radice multipla (cioè con molteplicità ≥ 2) di f. Sia g il polinomio minimo di a su F; si provi che ogni radice di g è una radice multipla di f.*

Soluzione. Poiché a è una radice multipla di f, a è radice del polinomio derivato $f' \in F[x]$. Ne segue che il polinomio minimo g di a divide sia f che f'. Quindi ogni radice di g è radice comune di f e di f', e pertanto, in particolare, è radice multipla di f.

Esercizio 3. *Sia $f = 2x^3+6x^2-9 \in \mathbb{Q}[x]$ e sia E campo di spezzamento di f su $\mathbb{Q}$.*

1. *Si provi che $u = \sqrt[3]{2} + \sqrt[3]{\frac{1}{2}} - 1$ è l'unica radice reale di f;*
2. *si determini - come tipo di isomorfismo - il gruppo $G = Gal(E|\mathbb{Q})$;*
3. *si provi che esiste un'unico campo intermedio L con $[L:\mathbb{Q}] = 2$ e che f è irriducibile in $L[x]$;*
4. *si dica se E contiene una radice primitiva terza dell'unità.*

Soluzione. 1. Si ha $u+1 = \sqrt[3]{2}+\sqrt[3]{1/2}$: elevando alla terza e moltiplicando per due:

$$2u^3 + 6u^2 + 6u + 2 = 4 + 6\sqrt[3]{2} + 6\sqrt[3]{1/2} + 1 = 6u + 11$$

da cui $f(u) = 0$. Dalla studio del segno della derivata $f' = 6x^2 + 12x$ si ricava che il grafico della funzione reale associata ad f ha un massimo locale in $x = -2$, dove $f(-2) = -1 < 0$, ed un minimo locale per $x = 0$ dove $f(0) = -9$; da ciò si conclude che il grafico ha una sola intersezione con l'asse delle ascisse; quindi che u è l'unica radice reale di f.

2. Dal punto precedente si ha, in particolare, che f non ha radici in $\mathbb{Q}$ e dunque che è irriducibile in $\mathbb{Q}[x]$. Quindi, $[\mathbb{Q}[u] : \mathbb{Q}] = 3$. Poiché $\mathbb{Q}[u] \leq \mathbb{R}$ e f ha radici non reali, si deduce che $\mathbb{Q}[u] \neq E$ e dunque $[E : \mathbb{Q}] = 6$ dato che, per la teoria generale, $[E : \mathbb{Q}]$ divide $3! = 6$. Pertanto, siccome G è isomorfo ad un sottogruppo del gruppo simmetrico S_3, si conclude $G \simeq S_3$

3. L'estensione $E|\mathbb{Q}$ è di Galois; quindi, per il Teorema fondamentale, i campi intermedi di grado 2 su $\mathbb{Q}$ corrispondono - nella connessione di Galois - ai sottogruppi di G di indice 2. Ora, $G \simeq S_3$ ha un unico tale sottogruppo, che è A_3; quindi c'è un unico campo intermedio, $L = Inv_E(A_3)$, tale che $[L : \mathbb{Q}] = 2$.
Ora, E è campo di spezzamento su L di f e $[L : \mathbb{Q}] = 2$. Quindi, L non contiene alcuna radice di f (dato che queste hanno grado 3 su $\mathbb{Q}$); ne segue che, essendo un polinomio di terzo grado, f è irriducibile su L.

4. Si osserva che $u = \sqrt[3]{2}+(\sqrt[3]{2})^{-1}-1 \in \mathbb{Q}[\sqrt[3]{2}]$; quindi che $Q[u] \subseteq \mathbb{Q}[\sqrt[3]{2}]$ e, poiché $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3 = [\mathbb{Q}[u] : \mathbb{Q}]$, $Q[\sqrt[3]{2}] = \mathbb{Q}[u] \subseteq E$. Poiché $E|F$ è normale, E contiene un campo di spezzamento per $x^3 - 2$ (che è il polinomio minimo di $\sqrt[3]{2}$), e quindi contiene le radici terze dell'unità.

Esercizio 4. *Sia $E|F$ un'estensione di Galois e sia $G = Gal(E|F)$. Sia $u \in E$; si provi che le seguenti condizioni sono equivalenti:*

1. *$E = F[u]$.*
2. *$\sigma(u) \neq u$ per ogni $1 \neq \sigma \in G$.*

Soluzione. Sie $E = F[u]$ estensione di Galois di F. Sia $\sigma \in G = Gal(E|F)$. Se $\sigma(u) = u$ allora $E = F[u] \leq Inv_E(\sigma)$ e dunque $\sigma = 1$.

Viceversa, sia $E|F$ un'estensione di Galois e sia $u \in E$. Supponiamo $F[u] \neq E$; allora $F[u]$ è un campo intermedio proprio di $E|F$; dunque, nella connessione di Galois, $F[u] = Inv_E(H)$ per qualche sottogruppo $H \neq 1$ di $Gal(E|F)$; quindi esiste $1 \neq \sigma \in Gal(E|F)$ tale che $\sigma(u) \neq u$.

Esercizio 5. *Sia $F = \mathbb{Z}/p\mathbb{Z}$ con p primo, $p \neq 5$. Si provi che il polinomio $x^4 + x^3 + x^2 + x + 1$ è irriducibile in $F[x]$ se e solo se $p \not\equiv \pm 1 \pmod 5$.*

Soluzione. Sia p un primo, $p \neq 5$, e $F = \mathbb{Z}/p\mathbb{Z}$. Sia E un campo di ordine p^4. Per il Teorema di Fermat, il gruppo moltiplicativo E^* (che ha ordine $p^4 - 1$) contiene un sottogruppo C di ordine 5. Gli elementi diversi da 1 di tale sottogruppo sono le radici del nostro polinomio $f = x^4 + x^3 + x^2 + x + 1$. Se u è un generatore del sottogruppo C (una radice primitiva), allora $F[u]$ è un campo di spezzamento (contenuto in E) del polinomio e $5 = |C|$ divide $|F[u]|$. Siccome l'ordine di $F[u]$ divide $|E| = p^4$, si verifica uno dei casi seguenti: $|F[u]| = p, p^2, p^4$. Ora, si ha che f è irriducibile in $F[x]$ se e soltanto se f è il polinomio minimo su F di u, ovvero se e solo se $[F[u] : F] = 4$ (cioè $F[u] = E$). Cioè equivale a dire che 5 non divide l'ordine del gruppo moltiplicativo di nessuna estensione di F di grado 1 o 2, cioè che 5 non divide $p^2 - 1 = (p-1)(p+1)$, e questo è equivalente a $p \not\equiv \pm 1 \pmod 5$.