Università degli studi Roma Tre
Corso di laurea in Matematica A.A. 2010-2011
Istituzioni di Algebra Superiore
12 Ottobre 2010 - Esercitazione n.3
Antonio Cigliola

Esercizio 1. *Sia V uno $\mathbb{Z}_p$-spazio vettoriale di dimensione finita. Dimostrare che la cardinalità di V è p^m, per qualche $m \in \mathbb{N}$.*

Esercizio 2. *Al variare di $n \in \mathbb{N}^*$, si consideri l'insieme $\mathbb{C}_n = \{z \in \mathbb{C} \,|\, z^n = 1\}$.*

(i) Dimostrare che $\mathbb{C}_n$ è un sottogruppo di $\mathbb{C}$.

(ii) Provare che $\mathbb{C}_n$ è isomorfo a $\mathbb{Z}_n$. Dedurre che si tratta di un grupo ciclico e dire quali e quanti sono i suoi generatori.

(iii) Dimostrare che se $m \mid n$ allora $\mathbb{C}_m \subset \mathbb{C}_n$.

(iv) Siano $m, n \geqslant 1$ interi distinti. Dire se $\mathbb{C}_m \cup \mathbb{C}_n = \mathbb{C}_{mn}$.

Esercizio 3. *Sia $(a, b) \in \mathbb{R} \times \mathbb{R}^*$. Dimostrare che $\mathbb{C} = \mathbb{R}(a + ib)$. Dedurre che i polinomi di $\mathbb{R}[x]$ irriducibili su $\mathbb{R}$ hanno al più grado 2.*

Esercizio 4. *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducible su $\mathbb{Q}$ di grado positivo con radici tutte distinte. Trovare un rappresentante della classe di isomorfismo di $\frac{\mathbb{R}[x]}{(f(x))}$ e di $\frac{\mathbb{C}[x]}{(f(x))}$. Cosa accade abolendo l'ipotesi sulla semplicità delle radici del polinomio?*

Esercizio 5. *Esibire almeno due $\mathbb{Q}$-basi dell'estensione $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Determinare le matrici di passaggio da una base all'altra.*

Esercizio 6. *Sia $F \subseteq K$ un ampliamento di campi. Siano $\alpha, \beta \in K$ algebrici su F di gradi rispettivamente m ed n, tali che $\mathrm{MCD}(m, n) = 1$. Provare che:*

(i) $[F(\alpha, \beta) : F] = mn$;

(ii) $F(\alpha) \cap F(\beta) = F$

(iii) $F(\alpha, \beta) = F(\alpha + \beta)$.

Siano $p(x)$ e $q(x)$ i polinomi minimi su $\mathbb{Q}$ di α e β rispettivamente. Provare che:

(iii) $q(x)$ non ha radici in $F(\alpha)$ e che $p(x)$ non ha radici in $F(\beta)$.

(iv) $q(x)$ è irriducibile su $F(\alpha)$ e che $p(x)$ è irriducibile su $F(\beta)$;

Esercizio 7. *Sia* $\zeta_5 \in \mathbb{C}$ *una radice quinta primitiva dell'unità. Sia* F *il campo* $\mathbb{Q}(\sqrt[5]{7}, \zeta_5)$.

(i) *Usando i risultati dell'esercizio precedente calcolare* $[F:\mathbb{Q}]$.

(ii) *Determinare, se esistono, tre campi distinti* F_1, F_2, F_3 *tali che* $\mathbb{Q} \subsetneq F_1 \subsetneq F_2 \subsetneq F_3 \subsetneq F$.

Esercizio 8. *Siano* p *un numero primo e* $k \geqslant 1$ *un intero. Sia* $F \subseteq K$ *un'estensione di campi di grado* p^k. *Sia* $f(x) \in F[x]$ *un polinomio irriducibile su* F *di grado strettamente compreso tra* 1 *e* p. *Dimostrare che* $f(x)$ *non ha radici in* K.

Esercizio 9. *Sia* F *un campo. Si consideri il polinomio*

$$f(x) = f_1(x)^{m_1} \cdot f_2(x)^{m_2} \cdots f_s(x)^{m_s} \in F[x]$$

decomposto canonicamente nel prodotto dei polinomi irriducibili $f_i(x) \in F[x]$. *Dimostrare che* $f(x)$ *ed* $f_{rid}(x) \overset{def}{=} f_1(x) \cdot f_2(x) \cdots f_s(x)$ *hanno lo stesso campo di spezzamento su* F. *Sia poi* $g(x) \overset{def}{=} f_1(x)^{n_1} \cdot f_2(x)^{n_2} \cdots f_s(x)^{n_s}$, *scelti come si voglia gli interi* $n_1, n_2, \ldots, n_s \geqslant 1$. *Provare che* $f(x)$ *e* $g(x)$ *hanno lo stesso campo di spezzamento su* F.

Esercizio 10. *Determinare il campo di spezzamento in* $\mathbb{C}$ *dei seguenti polinomi sul loro campo di definizione:*

(a) $x^4 + 2x^2 + 9$;

(b) $x^3 - 1$;

(c) $x^3 + 1$;

(d) $x^4 - 2$;

(e) $x^4 - 2x^2 + 49$;

(f) $x^5 - 1$;

(g) $x^5 - 3x^3 + 3x^2 - 9$;

(h) $x^5 - 3x^4 + 3x^3 - x^2 + \sqrt{5}x^3 - 3\sqrt{5}x^2 + 3\sqrt{5}x - \sqrt{5}$;

(i) $x^3 + 2ix^2 + x + 2i$;

(j) $x^3 - (6\sqrt{5} + 1)x^2 + (6\sqrt{5} + 47)x - 47$;

(k) $2x^3 - (2\sqrt{3} + 1)x^2 + (\sqrt{3} + 1)x - \sqrt{3}$;

(l) $x^7 + 2x^5 + 8x^3 + x - 8x^4 - x^6 - 2x^2 - 1^{\dagger}$;

---

†Si consiglia di ripetere la teoria delle equazioni reciproche e più in generale i metodi risolutivi delle equazioni algebriche studiati sui manuali di algebra del Liceo.

(m) $x^4 - 2x^2 + 3$;

(n) $x^4 - 5x^2 + 6$;

(o) $x^4 - 6x^2 + 1$;

(p) $x^4 - x^3 - 3x + 3$;

(q) $x^4 - 2x^3 + x^2 - x - 2$;

(r) $x^6 - 3x^3 + 2$.

Esercizio 11. *Determinare il grado su $\mathbb{Q}$ di ciascuno dei campi di spezzamento trovati nell'esercizio precedente.*

Esercizio 12. *Determinare per ciascuno dei seguenti polinomi di $\mathbb{Z}_p[x]$ un campo di spezzamento su $\mathbb{Z}_p$, per i valori di p a fianco indicati.*

(a) $x^3 + 2x + 1,\ p = 3$;

(b) $x^3 + 2x + 1,\ p = 5$;

(c) $x^4 + 5,\ p = 2$;

(d) $x^4 + 5,\ p = 3$;

(e) $x^4 + 5,\ p = 5$;

(f) $x^4 + 5,\ p = 7$;

(g) $x^3 + x + 1,\ p = 2$;

(h) $x^3 + x^2 + 1,\ p = 2$;

(i) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1^\dagger,\ p = 2$;

(j) $x^4 - x^3 - x - 1,\ p = 3$;

(k) $x^4 + x + 1,\ p = 2$;

(l) $x^3 - 3,\ p = 7$;

(m) $x^3 - 5,\ p = 13$;

(n) $x^4 + x^2 + x^3 + x + 1,\ p = 2$.

Esercizio 13. *Determinare il grado su $\mathbb{Z}_p$ di ciascuno dei campi di spezzamento trovati nell'esercizio precedente per i valori di p indicati.*

Esercizio 14. *Determinare tutti gli automorfismi del campo di spezzamento in $\mathbb{C}$ dei seguenti polinomi di $\mathbb{Q}[x]$:*

---

†Si suggerisce di calcolare il prodotto dei polinomi del punto *(g)* e del punto *(h)*...

(a) $x^2 + x + 2$;

(b) $x^3 - 7$;

(c) $x^4 + x^2 + 2x + 2$;

(d) $x^4 - 5x^2 + 6$;

(e) $x^5 + x^3 + x^2 + 1$;

(f) $x^6 - 3x^3 + 2$;

(g) $x^6 - 8x^3 + 7$.

Esercizio 15. *Determinare la struttura del gruppo di Galois dei polinomi dell'esercizio precedente.*

Esercizio 16. *Determinare tutti gli isomorfismi in $\mathbb{C}$ dei seguenti campi specificando quali tra essi sono automorfismi:*

(a) $\mathbb{Q}(\sqrt[4]{\sqrt[3]{3} + \sqrt{2}})$;

(b) $\mathbb{Q}(\sqrt{13})$;

(c) $\mathbb{Q}(\sqrt{2}, i)$;

(d) $\mathbb{Q}(\sqrt[3]{5})$;

(e) $\mathbb{Q}(\sqrt[3]{5}, \sqrt{11})$;

(f) $\mathbb{Q}(\sqrt[3]{7}, \sqrt{17}, \zeta_3)$.

Esercizio 17. *Determinare la struttura dei seguenti gruppi di Galois:*

(a) $\mathfrak{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{7}, \sqrt{17}, \zeta_3))$;

(b) $\mathfrak{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}))$;

(c) $\mathfrak{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, i))$.

Esercizio 18. *Determinare il gruppo di Galois di ciascuno dei seguenti polinomi di $\mathbb{Z}_p[x]$, per i valori di p a fianco indicati:*

(a) $x^4 + 2x^3 + 2x + 2$, $p = 3$;

(b) $x^5 + x^2 + 2x + 1$, $p = 3$;

(c) $x^2 + x + 1$, $p = 5$;

(d) $x^2 + 4x + 1$, $p = 5$;

(e) $x^3 + x + 1$, $p = 2$;

(f) $x^3 + x^2 + 1$, $p = 2$;

(g) $x^4 + x + 1$, $p = 2$;

(h) $x^4 + x^2 + x^3 + x + 1$, $p = 2$.

Esercizio 19. *Siano K ed L rispettivamente i campi di spezzamento su $\mathbb{Z}_5$ dei polinomi $x^2 + x + 1$ ed $x^2 + 4x + 1$ di $\mathbb{Z}_5[x]$. Mostrare che K ed L sono isomorfi e determinare tutti i possibili isomorfismi tra essi.*

Esercizio 20. *Siano K ed L rispettivamente i campi di spezzamento su $\mathbb{Z}_2$ dei polinomi $x^3 + x + 1$ ed $x^3 + x^2 + 1$ di $\mathbb{Z}_2[x]$. Mostrare che K ed L sono isomorfi e determinare tutti i possibili isomorfismi tra essi.*

Esercizio 21. *Mostrare che i gruppi $(\mathbb{Q}, +)$ e $(\mathbb{Q}^*, \cdot)$ non sono ciclici.*

Esercizio 22. *Siano F un campo ed x una indeterminata su F. Dimostrare che se un elemento $f \in F(x)$ è algebrico su F allora è in F; calcolare il suo polinomio minimo su F.*

Esercizio 23. *Determinare tutte le radici del polinomio*

$$f(x) = x^4 - 2x^3 + 5x^2 - 4x + 6 \in Q[x]$$

sapendo che una di queste è $i\sqrt{2}$. Determinare il gruppo di Galois di $f(x)$ su $\mathbb{Q}$.

Esercizio 24. *Può un automorfismo di $\mathbb{Q}(\sqrt{2})$ che manda $\sqrt{2}$ in $-\sqrt{2}$ essere esteso ad un automorfismo di $\mathbb{Q}(\sqrt{1+\sqrt{2}})$? In quanti modi?*

Esercizio 25. *Può un automorfismo di $\mathbb{Q}(\sqrt{6})$ che manda $\sqrt{6}$ in $-\sqrt{6}$ essere esteso ad un automorfismo di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$? In quanti modi?*

Esercizio 26. *Sia $\omega \neq 1$ una radice cubica dell'unità in $\mathbb{C}$. Può un automorfismo di $\mathbb{Q}(\omega)$ mandare ω in $-\omega$?*

Esercizio 27. *Sia $\omega \neq 1$ una radice quinta primitiva dell'unità in $\mathbb{C}$. Può un automorfismo di $\mathbb{Q}(\omega)$ mandare ω in $-\omega$? E in ω^{-1}*

Esercizio 28. *Determinare tutti gli automorfismi di $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \zeta_3)$ su*

(i) $\mathbb{Q}$;

(ii) $\mathbb{Q}(\sqrt[3]{2})$;

(iii) $\mathbb{Q}(\sqrt[3]{3})$;

(iv) $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$;

(v) $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$;

(vi) $\mathbb{Q}(\zeta_3)$.

Esercizio 29. *Determinare il numero di elementi di* $\mathfrak{Gal}_{\mathbb{Q}}(K)$ *dove* K *è il campo di spezzamento del polinomio:*

(i) $x^4 + x^2 + 1$;

(ii) $x^3 + 2x - 1$;

(iii) $x^4 + 1$;

(iv) $(x^2 + 2x - 1)^2(x^3 - 2)^6$;

(v) $(x^2 - 5x + 6)^{17}(x^3 + 3x^2 + 3x + 1)^6(x^6 - 9x^3 + 8)^{23}$.