

ESERCIZI DI ALGEBRA CAMPI (3)

N.B.: il simbolo $\hat{\otimes}$ contrassegna gli esercizi (relativamente) più complessi.

— * —

- 1** — Si consideri l'anello quoziente $\mathbb{F} := \mathbb{Z}_5[x]/(x^3 - x^2 + x + 1)$.
- (a) Dimostrare che \mathbb{F} è un campo.
 - (b) Calcolare la caratteristica e la cardinalità di \mathbb{F} .
 - (c) Determinare esplicitamente un generatore del gruppo moltiplicativo $(\mathbb{F}^*; \cdot)$ del campo \mathbb{F} , dove $\mathbb{F}^* := \mathbb{F} \setminus \{0\}$.

- 2** — Sia $K \subseteq L$ un'estensione di campi in cui L sia algebricamente chiuso. Posto $K^a := \{ \ell \in L \mid \ell \text{ è algebrico su } K \}$, dimostrare che:
- (a) K^a è un sottocampo di L , che contiene K .
 - (b) K^a è una chiusura algebrica di K .

- 2** — Siano p_1, p_2 due primi distinti in \mathbb{N}_+ . Dimostrare che:
- (a) l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ ha grado 4;
 - (b) $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) = \mathbb{Q}(\sqrt{p_1} + \sqrt{p_2})$, cioè $\sqrt{p_1} + \sqrt{p_2}$ è un elemento primitivo per l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$.

3 — Dato un campo K con chiusura algebrica K^a e dato $n \in \mathbb{N}_+$ che non sia multiplo della caratteristica di K , sia $\zeta_n \in K^a$ una radice n^a primitiva dell'unità — cioè ζ_n è un generatore del gruppo ciclico delle radici n -esime dell'unità in K^a .

Dimostrare che il gruppo di Galois $G(K(\zeta_n)/K)$ dell'estensione $K(\zeta_n)/K$ si immerge in modo naturale nel gruppo moltiplicativo $U(\mathbb{Z}_n)$ delle unità dell'anello \mathbb{Z}_n .

4 — Sia K un campo e $n \in \mathbb{N}_+$; supponiamo che n non sia multiplo della caratteristica di K , e che K contenga una radice primitiva dell'unità; sia dato infine $a \in K$ tale che il polinomio $(x^n - a) \in K[x]$ sia *irriducibile*.

Posto $K(\alpha) := K[x]/(x^n - a)$, dimostrare che:

- (a) $K(\alpha)$ è estensione finita di K , di grado n ;
- (b) $K(\alpha)$ è campo di spezzamento di $(x^n - a)$ su K (in particolare, $K(\alpha)/K$ è un'estensione normale);
- (c) il gruppo di Galois $G(K(\alpha)/K)$ di $K(\alpha)/K$ è isomorfo al gruppo delle radici n -esime dell'unità in K ;
- (d) il gruppo di Galois $G(K(\alpha)/K)$ di $K(\alpha)/K$ è ciclico di ordine n .

5 — Dato un campo K di caratteristica $p > 0$, siano $s \in \mathbb{N}_+$ e $a \in K$ tali che il polinomio $(x^{p^s} - a) \in K[x]$ sia *irriducibile*.

Posto $K(\alpha) := K[x]/(x^{p^s} - a)$, dimostrare che:

- (a) $K(\alpha)$ è estensione finita e normale di K , di grado p^s ;
- (b) $|G(K(\alpha)/K)| = |I(K(\alpha)/K)| = 1$.

6 — Dato un campo K di caratteristica $p > 0$, si consideri il suo (*mono*)*morfismo di Frobenius* $\phi : K \rightarrow K$ dato da $a \mapsto \phi(a) := a^p$ per ogni $a \in K$, e per ogni $n \in \mathbb{N}_+$ si ponga $K^{(n)} := \text{Im}(\phi^n)$. Dimostrare che:

- (a) ϕ è un endomorfismo di K (come anello);
- (b) ϕ è iniettivo;
- (c) per ogni $n \in \mathbb{N}_+$, ogni $\alpha \in K$ è radice di un polinomio della forma $(x^{p^n} - c_\alpha)$ per un certo $c_\alpha \in K^{(n)}$;
- (d) per ogni $n \in \mathbb{N}_+$, l'estensione $K/K^{(n)}$ è algebrica;
- (e) per ogni $n \in \mathbb{N}_+$ si ha $|G(K/K^{(n)})| = |I(K/K^{(n)})| = 1$.

7 — Dato un campo K di caratteristica $p > 0$, sia $f(x) \in K[x]$ un polinomio *irriducibile*. Dimostrare che le seguenti proprietà sono equivalenti:

- (a) $f(x)$ ha radici multiple (in un suo qualsiasi campo di spezzamento);
- (b) $f'(x) = 0$, cioè la derivata (formale) di $f(x)$ è il polinomio nullo;
- (c) esiste un polinomio $\ell(x) \in K[x]$ tale che $f(x) = \ell(x^p)$.

8 — Dato un campo K di caratteristica $p > 0$, sia $f(x) \in K[x]$ un polinomio *irriducibile*. Dimostrare che esistono un $s \in \mathbb{N}_+$ e un polinomio $h(x) \in K[x]$ tali che $f(x) = h(x^{p^s})$ e $h(x)$ non ha radici multiple.

9 — Dato un campo K di caratteristica zero, e un polinomio $f(x) \in K[x]$, supponiamo che $f(x)$ si fattorizzi in $K[x]$ come $f(x) = h(x)\ell(x)$. Detto K_f il campo di spezzamento di $f(x)$ su K , e similmente indichiamo i campi di spezzamento K_h e K_ℓ relativi ad $h(x)$ e ad $\ell(x)$. Dimostrare che:

- (a) le funzioni di restrizione $G(K_f/K_\ell) \xrightarrow{\rho_h} G(K_h/(K_h \cap K_\ell))$, $\sigma \mapsto \rho_h(\sigma) := \sigma|_{K_h}$ e $G(K_f/K_h) \xrightarrow{\rho_\ell} G(K_\ell/(K_\ell \cap K_h))$, $\sigma \mapsto \rho_\ell(\sigma) := \sigma|_{K_\ell}$ sono morfismi di gruppi;
- (b) i morfismi ρ_h e ρ_ℓ di cui al punto (a) sono iniettivi;
- (c) $\hat{\cong}$ i morfismi ρ_h e ρ_ℓ di cui al punto (a) sono suriettivi.

((Suggerimento: Per il punto (b), si sfrutti il fatto che, se $\alpha_1, \dots, \alpha_r \in K^a$ e $\beta_1, \dots, \beta_s \in K^a$ sono le radici di $h(x)$ e di $\ell(x)$ rispettivamente, allora $K_h = K(\alpha_1, \dots, \alpha_r)$, $K_\ell = K(\beta_1, \dots, \beta_s)$ e $K_f = K(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$.)

Per il punto (c), si sfrutti il *Teorema di Corrispondenza di Galois* per ottenere che il sottogruppo $\text{Im}(\rho_h)$ di $G(K_h/(K_h \cap K_\ell))$ coincide con tutto il gruppo perché entrambi hanno come *sottocampo dei punti fissi* associato il campo K_h . Analogamente si dimostra che il sottogruppo $\text{Im}(\rho_\ell)$ di $G(K_\ell/(K_\ell \cap K_h))$ coincide con tutto $G(K_\ell/(K_\ell \cap K_h))$.)

10 $\hat{\diamond}$ — Dato un campo K di caratteristica zero, e un polinomio $f(x) \in K[x]$, supponiamo che $f(x)$ si fattorizzi in $K[x]$ come $f(x) = h(x)\ell(x)$. Detto K_f il campo di spezzamento di $f(x)$ su K , sia $G_f := G(K_f/K)$ il gruppo di Galois di $f(x)$, e similmente indichiamo i campi di spezzamento K_h e K_ℓ e i gruppi di Galois G_h e G_ℓ relativi ad $h(x)$ e ad $\ell(x)$. Dimostrare che:

- (a) esiste un morfismo naturale $G_f \xrightarrow{\mu} G_h \times G_\ell$ da G_f al gruppo prodotto $G_h \times G_\ell$;
- (b) il morfismo μ di cui al punto (a) è iniettivo;
- (c) $\hat{\diamond}$ se $K_h \cap K_\ell = K$, allora il morfismo μ di cui al punto (a) è suriettivo;
- (d) $\hat{\diamond}$ $\hat{\diamond}$ se il morfismo μ di cui al punto (a) è suriettivo, allora $K_h \cap K_\ell = K$;
- (e) se $K_h \cap K_\ell = K$, allora $G_f := G(K_f/K)$ è prodotto diretto interno dei suoi due sottogruppi normali $G(K_f/K_\ell)$ e $G(K_f/K_h)$.

((Suggerimento: Si osservi che, se $\alpha_1, \dots, \alpha_r \in K^a$ e $\beta_1, \dots, \beta_s \in K^a$ sono le radici di $h(x)$ e di $\ell(x)$ rispettivamente, allora $K_h = K(\alpha_1, \dots, \alpha_r)$, $K_\ell = K(\beta_1, \dots, \beta_s)$ e $K_f = K(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$. Ciò detto, per il punto (a) si ottenga μ “accoppiando” i morfismi di “restrizione da K_f a K_h ” e di “restrizione da K_f a K_ℓ ”. Per il punto (b), si sfrutti ancora il fatto che $K_h = K(\alpha_1, \dots, \alpha_r)$, $K_\ell = K(\beta_1, \dots, \beta_s)$ e infine $K_f = K(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$. Per i punti (c) e (d), si utilizzino gli isomorfismi ρ_h e ρ_ℓ di cui all'Esercizio 5.32 qui sopra — in un verso — e l'osservazione che l'estensione $(K_h \cap K_\ell)/K$ è anch'essa normale.))