PARTE SECONDA
Complementi su polinomi e campi

Lezione 4

Prerequisiti: Estensioni algebriche. Radici coniugate. Campi di spezzamento**.**

Campi di spezzamento ed omomorfismi di campi.

Richiamo: Sia *F* un campo, sia *K* una sua estensione, siano $\alpha, \beta \in K$ algebrici su *F*. Allora α e β si dicono coniugati su *F* se hanno lo stesso polinomio minimo su *F*.

Proposizione 4.1 Sia *F* un campo, sia *K* una sua estensione, siano $\alpha, \beta \in K$ algebrici su *F*. Allora α e β sono coniugati su *F* se e solo se esiste un isomorfismo di campi

$$\varphi : F(\alpha) \to F(\beta)$$

che lascia fissi gli elementi di *F* (ovvero: che è un isomorfismo di spazi vettoriali su *F*) e tale che $\varphi(\alpha) = \beta$.

Dimostrazione: Se esiste un isomorfismo di campi con le proprietà date, allora detto $p(x)$ il polinomio minimo di α su *F*, $p(x) = \sum_{i=0}^{n} a_i x^i$, si ha

$$p(\beta) = \sum_{i=0}^{n} a_i \beta^i = \sum_{i=0}^{n} \varphi(a_i)\varphi(\alpha)^i = \varphi(\sum_{i=0}^{n} a_i \alpha^i) = \varphi(p(\alpha)) = 0 .$$

Quindi $p(x)$ è il polinomio minimo di β su *F*.
Viceversa, supponiamo che $p(x)$ sia il polinomio minimo di α e β su *F*. Consideriamo gli omomorfismi di valutazione in α e β:

$$\begin{array}{ll} \varphi_\alpha : F[x] \to K & \varphi_\beta : F[x] \to K \\ f(x) \mapsto f(\alpha) & f(x) \mapsto f(\beta) \end{array}$$

Questi sono anche omomorfismi di *F*-spazi vettoriali. Essi inducono, come noto, isomorfismi di campo, e di *F*-spazi vettoriali

$$\varphi_\alpha^* : F[x]/(p(x)) \to F(\alpha) \qquad \varphi_\beta^* : F[x]/(p(x)) \to F(\beta) .$$

Allora $\varphi = \varphi_\beta^* \circ (\varphi_\alpha^*)^{-1}$ è l'isomorfismo cercato. □

Osservazione 4.2 Ogni isomorfismo di campi $\sigma : F \to \widetilde{F}$ si estende, in modo naturale, ad un isomorfismo di anelli $\overline{\sigma} : F[x] \to \widetilde{F}[x]$, ponendo, per ogni $f(x) \in F[x]$, $f(x) = \sum_{i=0}^{n} a_i x^i$, $\overline{\sigma}(f(x)) = \sum_{i=0}^{n} \sigma(a_i) x^i$.

Lemma 4.3 Sia dato un isomorfismo di campi $\sigma : F \to \widetilde{F}$, e siano K e $\widetilde{K}$ estensioni di F e $\widetilde{F}$ rispettivamente. Siano $\alpha \in K$, $\widetilde{\alpha} \in \widetilde{K}$ elementi algebrici su F e $\widetilde{F}$ rispettivamente, di polinomi minimi $p(x)$ e $\tilde{p}(x) = \overline{\sigma}(p(x))$ rispettivamente. Allora esiste un isomorfismo di campi

$$\varphi : F(\alpha) \to \widetilde{F}(\widetilde{\alpha})$$

che estende σ e tale che $\varphi(\alpha) = \widetilde{\alpha}$.

Dimostrazione: È facile vedere che σ induce un isomorfismo di campi

$$\hat{\sigma} : F[x] \big/ (p(x)) \to \tilde{F}[x] \big/ (\tilde{p}(x))$$

che estende σ. Allora l'isomorfismo cercato è, con ovvio significato dei simboli,

$$\varphi_{\widetilde{\alpha}} * \circ \hat{\sigma} \circ (\varphi_{\alpha} *)^{-1}. \qquad \square$$

Teorema 4.4 Siano F e $\widetilde{F}$ campi, sia $\sigma : F \to \widetilde{F}$ un isomorfismo di campi. Sia $f(x) \in F[x]$ non costante. Posto $\widetilde{f}(x) = \overline{\sigma}(f(x))$, sia K un campo di spezzamento di $f(x)$ su F, e sia $\widetilde{K}$ un campo di spezzamento di $\widetilde{f}(x)$ su $\widetilde{F}$. Esiste allora un isomorfismo di campi $\eta : K \to \tilde{K}$ che estende σ.

Dimostrazione: Procediamo per induzione su $n = \deg f(x)$. Se n=1, allora $F = K$ e $\widetilde{F} = \widetilde{K}$, quindi l'enunciato è banalmente vero. Supponiamo allora che sia n>1, e la tesi vera per i polinomi di grado al più $n-1$. Sia $p(x)$ un fattore irriducibile di $f(x)$, e sia α una sua radice in K. Posto $\tilde{p}(x) = \overline{\sigma}(p(x))$, sia $\widetilde{\alpha}$ una radice di $\tilde{p}(x)$ in $\widetilde{K}$. In virtù del Lemma 4.3 esiste un isomorfismo di campi $\varphi : F(\alpha) \to \tilde{F}(\tilde{\alpha})$ che estende σ e tale che $\varphi(\alpha) = \tilde{\alpha}$. Si hanno allora le decomposizioni:

$$f(x) = (x - \alpha) q(x) \quad \text{in } F(\alpha)[x] \qquad\qquad \widetilde{f}(x) = (x - \widetilde{\alpha}) \widetilde{q}(x) \quad \text{in } \widetilde{F}(\widetilde{\alpha})[x],$$

dove $\overline{\varphi}(q(x)) = \tilde{q}(x)$. I polinomi $q(x)$ e $\widetilde{q}(x)$ hanno grado $n-1$ (e sono quindi non costanti), ed i loro campi di spezzamento (su $F(\alpha)$ e $\widetilde{F}(\widetilde{\alpha})$ rispettivamente) sono, nell'ordine, K e $\widetilde{K}$. Per l'ipotesi induttiva esiste allora un isomorfismo di campi $\eta : K \to \tilde{K}$ che estende φ. Esso, evidentemente, estende σ. $\square$

Dalla dimostrazione del Teorema 4.4 discende immediatamente il seguente risultato:

Corollario 4.5 (*Teorema di estensione degli isomorfismi*) Siano F e $\widetilde{F}$ campi, sia $\sigma : F \to \widetilde{F}$ un isomorfismo di campi. Sia $p(x) \in F[x]$ irriducibile. Posto $\tilde{p}(x) = \overline{\sigma}(p(x))$, sia K un campo di spezzamento di $p(x)$ su F, e sia $\widetilde{K}$ un campo di spezzamento di $\tilde{p}(x)$ su $\widetilde{F}$. Siano $\alpha \in K$ e $\widetilde{\alpha} \in \widetilde{K}$ radici di $p(x)$ e $\tilde{p}(x)$ rispettivamente. Esiste allora un isomorfismo di campi $\eta : K \to \tilde{K}$ che estende σ e tale che $\eta(\alpha) = \tilde{\alpha}$.

Questo risultato, in realtà, può essere migliorato:

****Teorema 4.6** (*Teorema di estensione degli isomorfismi, forma forte*) Siano F e $\widetilde{F}$ campi, sia $\sigma : F \to \widetilde{F}$ un isomorfismo di campi. Sia $f(x) \in F[x]$. Posto $\widetilde{f}(x) = \overline{\sigma}(f(x))$, sia K un campo di spezzamento di $f(x)$ su F, e sia $\widetilde{K}$ un campo di spezzamento di $\widetilde{f}(x)$ su $\widetilde{F}$. Sia $\alpha \in K$, sia $p(x)$ il suo polinomio minimo su F, e sia $\widetilde{\alpha} \in \widetilde{K}$ una radice di $\tilde{p}(x) = \overline{\sigma}(p(x))$. Esiste allora un isomorfismo di campi $\eta : K \to \tilde{K}$ che estende σ e tale che $\eta(\alpha) = \tilde{\alpha}$.

Dimostrazione: Una dimostrazione, basata sul Lemma di Zorn, può essere trovata in [Mo], Theorem 3.20.

Proposizione 4.7 Sia F un campo, sia $f(x) \in F[x]$ non costante. Allora i campi di spezzamento di $f(x)$ su F sono a due a due isomorfi. Inoltre, se L è un'estensione di F sulla quale $f(x)$ si spezza nel prodotto di fattori lineari, allora esiste un unico campo di spezzamento di $f(x)$ su F contenuto in L.

Dimostrazione: La prima parte dell'enunciato segue direttamente dal Teorema 4.4. Proviamo la seconda. Sia $n = \deg f(x)$. Siano $\alpha_1, ..., \alpha_n$ le radici di $f(x)$ in L, contate con le rispettive molteplicità. Allora $F(\alpha_1, ..., \alpha_n)$ è un campo di spezzamento di $f(x)$ su F contenuto in L. Inoltre in $L[x]$ si ha la decomposizione

$$f(x) = c\prod_{i=1}^{n}(x - \alpha_i),$$

essendo $c \in F$ il coefficiente direttore di $f(x)$. Sia K un campo di spezzamento di $f(x)$ su F contenuto in L. Sia α una radice di $f(x)$ in K. Allora $\alpha - \alpha_i = 0$, per qualche i. Quindi le radici di $f(x)$ in K sono comprese tra $\alpha_1, ..., \alpha_n$. Segue che $K \subset F(\alpha_1, ..., \alpha_n)$. Ma, per la condizione di minimalità contenuta nella definizione di campo di spezzamento, l'inclusione non può essere stretta. Dunque $K = F(\alpha_1, ..., \alpha_n)$. □

Esempio 4.8 Sia $f(x) = x^2 + x + 1 \in \mathbf{Q}[x]$. Questo è un polinomio irriducibile su $\mathbf{Q}$, poiché privo di radici reali. Le radici complesse di $f(x)$ sono ω, ω^2, essendo $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ una radice primitiva cubica dell'unità. Un campo di spezzamento di $f(x)$ su $\mathbf{Q}$ è $\mathbf{Q}(\omega)$; una sua base su $\mathbf{Q}$ è formata da 1, ω. In base al Teorema di estensione degli isomorfismi (Corollario 4.5) esiste un automorfismo di campo

$$\varphi : \mathbf{Q}(\omega) \to \mathbf{Q}(\omega)$$

tale che $\varphi(\omega)=\omega^2$, (e, di conseguenza, $\varphi(\omega^2)=\omega$.) Tale isomorfismo è dunque definito sul generico elemento di $\mathbf{Q}(\omega)$ nel modo seguente:

$$\varphi(a+b\omega)=a+b\omega^2=a-b-b\omega.$$

Osservazione 4.9 Dato un polinomio non costante $f(x)\in F[x]$, se $\alpha_1,...,\alpha_n$ sono le sue radici in un'estensione di *F*, allora $K=F(\alpha_1,...,\alpha_n)$ è un campo di spezzamento di *f*(*x*) su *F*. Quindi ogni automorfismo φ di *K* che estende l'identità di *F* induce una permutazione su $\alpha_1,...,\alpha_n$, ed è univocamente determinato da questa. In generale, però, non tutte le permutazioni su $\alpha_1,...,\alpha_n$ definiscono un automorfismo di *K*: un campo di spezzamento del polinomio $f(x)=(x^2-2)(x^2-3)$ su $\mathbf{Q}$ è $\mathbf{Q}(\sqrt{2},\sqrt{3})$, dove esso ha le radici $\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}$, è chiaro che nessun automorfismo di $\mathbf{Q}(\sqrt{2},\sqrt{3})$ può inviare $\sqrt{2}$ in $\sqrt{3}$ (altrimenti 2 verrebbe inviato in 3, mentre $\mathbf{Q}$ deve essere lasciato fisso). Si potrebbe osservare che l'esempio prescelto è un polinomio riducibile, e che le permutazioni "non lecite", in fondo, sono quelle che scambiano tra loro radici di fattori irriducibili diversi. In realtà, si possono trovare anche polinomi irriducibili su $\mathbf{Q}$ per i quali soltanto certe permutazioni delle radici danno luogo ad automorfismi del campo di spezzamento. Un esempio è il polinomio $f(x)=x^3-3x+1$, irriducibile su $\mathbf{Q}$ in quanto privo di radici razionali. Per verificare questa affermazione, è però necessario conoscere la cosiddetta Teoria di Galois. La affronteremo in seguito.

Nella parte dedicata alla Teoria di Galois, ci sarà utile il seguente risultato:

Proposizione 4.10 Sia *F* un campo, e sia *K* una sua estensione finita. Allora per ogni $\alpha\in K$ esiste un'estensione *L* di *K* ed esiste un polinomio $f(x)\in F[x]$ tale che
a) *L* è un campo di spezzamento di $f(x)$ su *F*;
b) ogni fattore irriducibile di $f(x)$ in $F[x]$ ha una radice in *K*;
c) $f(\alpha)=0$.

Dimostrazione: Sia $\{u_1,...,u_n\}$ una base di *K* su *F*. Ricordiamo che *K* è un'estensione algebrica di *F* (vedi Algebra 2, Proposizione 22.6). Sia $f(x)\in F[x]$ il prodotto dei polinomi minimi di α e di u_i su *F*. Allora b) e c) valgono. Sia *L* un campo di spezzamento di $f(x)$ su *K*. Siano $\alpha_1,...,\alpha_m$ le (eventuali) radici di $f(x)$ in *L* distinte da $u_1,...,u_n$. Allora $L=K(\alpha_1,...,\alpha_m)=F(u_1,...,u_n,\alpha_1,...,\alpha_m)$ è il campo di spezzamento di $f(x)$ su *F*. Ciò prova a) e conclude la dimostrazione. □