Algebra n. 3 - NOTE ALLA LEZIONE 13

Polinomi di grado 2

In base alle formule risolutive per l'equazione $ax^2+bx+c=0,$ un campo di spezzamento di $f(x)$ su F è

$$F(-\frac{b}{2a}+\frac{\sqrt{\Delta}}{2a},-\frac{b}{2a}-\frac{\sqrt{\Delta}}{2a})=F(\sqrt{\Delta}).$$

Si tenga presente che $a,b\in F.$ Inoltre $f(x)$ è privo di radici in F se e solo se Δ è privo di radici quadrate in F. In tal caso il polinomio minimo di $\sqrt{\Delta}$ su F è $p(x)=x^2-\Delta,$ così che $[F(\sqrt{\Delta}):F]=2.$

Polinomi di grado 3

Dalle uguaglianze

$$\begin{aligned} -\alpha_1\alpha_2\alpha_3 &= q && (1)\\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= p && (2)\\ \alpha_1+\alpha_2+\alpha_3 &= 0 && (3)\end{aligned}$$

si deriva:

$$p=\alpha_1(\alpha_2+\alpha_3)+\alpha_2\alpha_3=-(\alpha_2+\alpha_3)^2+\alpha_2\alpha_3=-(\alpha_2-\alpha_3)^2-3\alpha_2\alpha_3=-(\alpha_2-\alpha_3)^2+\frac{3q}{\alpha_1}.$$

(2) (3) (1)

Inoltre

$$(\alpha_2-\alpha_3)^2=-p+\frac{3q}{\alpha_1}=-4p+3p-3\alpha_2\alpha_3=-4p+3\alpha_1(\alpha_2+\alpha_3)+3\alpha_2\alpha_3-3\alpha_2\alpha_3=-4p-3\alpha_1^2.$$

Infine:

$$\begin{aligned}\beta^2(\beta^2+3p)^2 &= (-3\alpha_1^2-4p)(-3\alpha_1^2-p)^2=(-3\alpha_1^2-4p)(9\alpha_1^4+6\alpha_1^2p+p^2)\\ &=-27\alpha_1^6-36p\alpha_1^4-18p\alpha_1^4-24\alpha_1^2p^2-3\alpha_1^2p^2-4p^3\\ &=-27\alpha_1^2(\alpha_1^4+2p\alpha_1^2+p^2)-4p^3=-27\alpha_1^2(\alpha_1^2+p)^2-4p^3\\ &\underset{(3)}{=}-27\alpha_1^2(p-\alpha_1(\alpha_2+\alpha_3))^2-4p^3\\ &\underset{(2)}{=}-27\alpha_1^2\alpha_2^2\alpha_3^2-4p^3\underset{(1)}{=}-27q^2-4p^3\\ &=\Delta\end{aligned}$$

Polinomi di grado 4

In base alle formule di Viète (Teorema 7.11), coefficienti di $r(x)$ sono, a meno del "segno", i polinomi simmetrici elementari (in tre indeterminate) valutati nella terna $(\beta_1,\beta_2,\beta_3).$ D'altra parte

ogni permutazione di $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ ha l'effetto di permutare $\beta_1, \beta_2, \beta_3$. Pertanto le permutazioni di $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ lasciano invariati i coefficienti di $r(x)$. Questi sono, in altri termini, espressioni polinomiali simmetriche in $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ (a coefficienti in *F*), e dunque, alla luce del Corollario 7.12, sono espressioni polinomiali dei coefficienti di $f(x)$, e pertanto appartengono a *F*.

Dimostrazione del **Corollario 13.7**:

Un calcolo diretto mostra che:

$$(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) = \beta_2 - \beta_3$$
$$(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4) = \beta_1 - \beta_3$$
$$(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) = \beta_1 - \beta_2$$

Polinomi ciclotomici

Ogni $\sigma \in G(K, \mathbb{Q})$ induce un automorfismo del gruppo moltiplicativo K^*, il quale conserva i periodi degli elementi. Dunque ogni radice primitiva *n*-esima dell'unità viene inviata in una radice primitiva *n*-esima dell'unità.

L'applicazione φ è un omomorfismo di gruppi, in quanto, per ogni $\sigma, \tau \in G(K, \mathbb{Q})$, se $1 \le k, h \le n-1$ sono tali che $\sigma(\omega) = \omega^k, \tau(\omega) = \omega^h$, allora $\sigma\tau(\omega) = \sigma(\tau(\omega)) = \sigma(\omega^h) = \omega^{kh}$, e dunque

$$\varphi(\sigma\tau) = [kh]_n = [k]_n[h]_n = \varphi(\sigma)\varphi(\tau).$$

L'iniettività risulta dal fatto che $\sigma \in \operatorname{Ker}\varphi$ se e solo se $\sigma(\omega) = \omega$, ossia se e solo se $\sigma = \mathrm{id}_{\mathbb{Q}(\omega)}$.

Dimostrazione della **Proposizione 13.11**:

Si dice *chiusura algebrica* di un campo *F* una sua estensione algebrica che sia algebricamente chiusa. Ogni campo *F* possiede una chiusura algebrica, univocamente determinata a meno di *F*-isomorfismi.

In generale, l'omomorfismo $\varphi : G(K, F) \to U(\mathbb{Z}_n)$ non è surgettivo, in quanto non è detto che sia $|G(K, F)| = \phi(n)$. Infatti il numero $[K : F]$, ossia il grado del polinomio minimo di ω su *F*, non è necessariamente uguale a $\phi(n)$. L'**Esempio 13.12** presenta un caso di questo tipo.

Dimostrazione della **Proposizione 13.13**:

Si ha $(\alpha^m)^n = (\alpha^n)^m = a^m$, quindi α^m è una radice *n*-esima di a^m.

Ogni *F*- automorfismo di *K* lascia fisso *a*, e quindi, conservando le potenze, invia ogni radice *n*-esima di *a* in una radice *n*-esima di *a*.

L'applicazione $\varphi : G(K, F) \to \mathbb{Z}_n$ è un omomorfismo di gruppi, in quanto, per ogni $\sigma, \tau \in G(K, F)$, se $0 \le k, h \le n-1$ sono tali che $\sigma(\alpha) = \alpha\omega^k, \tau(\alpha) = \alpha\omega^h$, allora

$$\sigma\tau(\alpha)=\sigma(\tau(\alpha))=\sigma(\alpha\omega^h)=\sigma(\alpha)\sigma(\omega^h)=\sigma(\alpha)\omega^h=\alpha\omega^k\omega^h=\alpha\omega^{k+h},$$

e dunque

$$\varphi(\sigma\tau)=[k+h]_n=[k]_n+[h]_n=\varphi(\sigma)+\varphi(\tau).$$

Inoltre, $\sigma\in\operatorname{Ker}\varphi$ se e solo se $\sigma(\alpha)=\alpha\omega^0=\alpha$, ossia se e solo se $\sigma=\mathrm{id}_K$.

Esempio 13.14

Ogni automorfismo di $\mathbb{Q}(i,\sqrt[4]{2})$ è univocamente determinato dalle immagini di i e $\sqrt[4]{2}$. La prima può essere scelta tra i e $-i$, la seconda è una fra $\sqrt[4]{2},-\sqrt[4]{2},i\sqrt[4]{2},-i\sqrt[4]{2}$. Ad esempio, all'automorfismo riportato nella seconda riga della tabella

	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
id	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
(13)	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$

corrispondono le seguenti scelte:

$$\sqrt[4]{2}\mapsto\begin{cases}\sqrt[4]{2}\\ -\sqrt[4]{2}\\ i\sqrt[4]{2}\\ -i\sqrt[4]{2}\end{cases}\qquad i\mapsto\begin{cases}i\\ -i\end{cases}$$

Le immagini delle restanti radici quarte di 2 si determinano applicando le proprietà di omomorfismo.

Il campo $\mathbb{Q}(\sqrt[4]{2})$ non è un'estensione normale di $\mathbb{Q}$, in quanto non vi appartengono le (due) radici quarte di 2 che sono complesse non reali.

Osservazione 13.17

In sintesi, le principali definizioni e proprietà:

1. Data un'estensione di campi $F \subset K$, si dice che un sottoinsieme S di K

- è *algebricamente indipendente* su F se, comunque presi $\alpha_1,...,\alpha_n \in S$ elementi distinti, non esiste un polinomio non nullo $f(x_1,...,x_n) \in F[x_1,...,x_n]$ tale che $f(\alpha_1,...,\alpha_n) = 0$. Se S è ridotto ad un solo elemento α, ciò avviene se e solo se α è trascendente su F.
  In tal caso si dice che S
- è una *base di trascendenza* di K su F se, inoltre, K è algebrico su $F(S)$.

2. Se T è un sottoinsieme di K tale che $F(T) = K$, T contiene una base di trascendenza di K su F. In particolare, ogni estensione di campi ammette una base di trascendenza.

3. Le basi di trascendenza di una medesima estensione di campi $F \subset K$ sono a due a due equipotenti. Se sono finite, la loro comune cardinalità si dice *grado di trascendenza* di K su F.

Ad esempio, il campo delle frazioni dell'anello dei polinomi a coefficienti in F in n indeterminate, $F(x_1,...,x_n)$, ha come base di trascendenza su F l'insieme $\{x_1,...,x_n\}$. Il grado di trascendenza è n.
Un altro esempio è il seguente: il campo $\mathbb{Q}(i)(x)$ (con x indeterminata) ha $\{x\}$ come base di trascendenza su $\mathbb{Q}$: infatti $\mathbb{Q}(i)(x) = \mathbb{Q}(x)(i)$ è algebrico su $\mathbb{Q}(x)$.

Esercizio 13.18

Nelle ipotesi date, si ha:

$$(\alpha+1)^2 + (\alpha+1) + 1 = \alpha^2 + 1 + \alpha + 1 + 1 = \alpha^2 + \alpha + 1 = 0 .$$