Lezione 6

Prerequisiti: Lezione 5.

Estensioni semplici.

Dalle esercitazioni del corso di Algebra 2 è noto che, ad esempio, $\mathbf{Q}(\sqrt{2},\sqrt{3})=\mathbf{Q}(\sqrt{2}+\sqrt{3})$, $\mathbf{Q}(\sqrt{2},i)=\mathbf{Q}(\sqrt{2}+i)$: molte estensioni generate da più elementi algebrici sono, in realtà, estensioni semplici. Gli esempi citati sono casi particolari di una proprietà generale:

Teorema 6.1 (*Teorema dell'elemento primitivo*) Sia F un campo, e sia K una sua estensione. Siano $\alpha_1,\ldots,\alpha_n\in K$ elementi separabili su F. Allora esiste un elemento $\alpha\in K$ (detto primitivo) tale che $F(\alpha_1,\ldots,\alpha_n)=F(\alpha)$. Inoltre, se F è infinito, esistono $c_1,\ldots,c_n\in F$ tali che $\sum_{i=1}^{n} c_i\alpha_i$ sia un elemento primitivo.

Dimostrazione: Se F è finito, allora essendo $F(\alpha_1,\ldots,\alpha_n)$ di grado finito su F, anche $F(\alpha_1,\ldots,\alpha_n)$ è finito. Quindi il suo gruppo moltiplicativo è ciclico (vedi Algebra 2, Proposizione 24.8). Detto α un suo generatore, si avrà allora che $F(\alpha_1,\ldots,\alpha_n)=F(\alpha)$.
Supponiamo ora che F sia infinito. Chiaramente, basta provare l'enunciato per n = 2. Siano $f_1(x), f_2(x)\in F[x]$ i polinomi minimi di α_1,α_2 su F, di gradi r e s rispettivamente, sia, inoltre, L un campo di spezzamento del polinomio $f(x)=f_1(x)f_2(x)$ su $F(\alpha_1,\alpha_2)$. Siano $\alpha_1=u_1,\ldots,u_r$ e $\alpha_2=v_1,\ldots,v_s$ le radici in L di $f_1(x)$ e $f_2(x)$ rispettivamente. Poiché α_2 è separabile su F, queste ultime sono a due a due distinte. Sia $c\in F$ tale che per $x=c$ non sia verificata alcuna delle seguenti equazioni:

$$u_i+xv_j=u_1+xv_1,\qquad \text{dove } i=1,\ldots,r \quad \text{e} \quad j=2,\ldots,s.$$

Un elemento c siffatto esiste perché ogni equazione ha una ed una sola soluzione, e il campo F è infinito. Proviamo che $\alpha=\alpha_1+c\alpha_2$ è un elemento primitivo. L'inclusione $F(\alpha)\subset F(\alpha_1,\alpha_2)$ è ovvia. Per dimostrare l'altra, è sufficiente provare che $\alpha_2\in F(\alpha)$. I polinomi $f_2(x)$, $f_1(\alpha-cx)\in F(\alpha)[x]$ hanno in L la radice comune α_2. Non ne hanno altre in comune, in quanto, per come è stato scelto c, per ogni $j=2,\ldots,s$, si ha $\alpha-cv_j=u_1+cv_1-cv_j\neq u_i$, e quindi $f_1(\alpha-cv_j)\neq 0$. Conseguentemente, tenendo anche conto della separabilità di $f_2(x)$, si ha che $\mathrm{MCD}(f_2(x), f_1(\alpha-cx))=x-\alpha_2$ in $L[x]$ (osserviamo che entrambi i polinomi si decompongono su L nel prodotto di fattori lineari). Lo stesso vale in $F(\alpha)[x]$: infatti il $\mathrm{MCD}(f_2(x), f_1(\alpha-cx))$ in $F(\alpha)[x]$ divide il $\mathrm{MCD}(f_2(x), f_1(\alpha-cx))=x-\alpha_2$ in $L[x]$; in virtù del Lemma 5.3, non può però essere uguale a 1, perché altrimenti si avrebbe $\mathrm{MCD}(f_2(x), f_1(\alpha-cx))=1$ anche in $L[x]$. Se ne deduce che $\alpha_2\in F(\alpha)$, come volevasi. □

Corollario 6.2 Ogni estensione finita di un campo perfetto è semplice.

Esempio 6.3 Determiniamo elementi primitivi di $\mathbf{Q}(\sqrt{2},\sqrt{3})$ secondo il procedimento seguito nella dimostrazione del Teorema 6.1. Sia $\alpha_1=\sqrt{2}$, $\alpha_2=\sqrt{3}$; i loro polinomi minimi su $\mathbf{Q}$ sono $f_1(x)=x^2-2$, le cui radici sono $u_1=\sqrt{2}, u_2=-\sqrt{2}$, e $f_2(x)=x^2-3$, le cui radici sono $v_1=\sqrt{3}, v_2=-\sqrt{3}$. Sono elementi primitivi tutti gli elementi $\alpha=\sqrt{2}+c\sqrt{3}$, dove $c\in\mathbf{Q}$ è tale che

$$\sqrt{2}-c\sqrt{3}\neq\sqrt{2}+c\sqrt{3} \qquad \text{e} \qquad -\sqrt{2}-c\sqrt{3}\neq\sqrt{2}+c\sqrt{3},$$

ossia,

$$c\notin\left\{0,-\frac{\sqrt{2}}{\sqrt{3}}\right\}, \quad \text{cioè} \quad c\neq 0.$$

Diamo ora alcune conseguenze del Teorema dell'elemento primitivo, che si riveleranno utili in seguito.

Proposizione 6.4 Sia *F* un campo, e sia *K* una sua estensione separabile di grado *n*. Detta *L* una chiusura algebrica di *F* contenente *K*, esistono esattamente *n* distinti monomorfismi di campi da *K* a *L* che lasciano fisso ogni elemento di *F*.

Dimostrazione: Per il Teorema dell'elemento primitivo, esiste $\alpha\in K$ tale che $F(\alpha)=K$. Allora il polinomio minimo di α su *F* ha grado *n* ed è separabile. Quindi esso ha in *L* *n* radici distinte $\alpha_1,\ldots,\alpha_n$. In virtù del Lemma 4.3, per ogni $i=1,\ldots,n$ esiste un isomorfismo di campi $\sigma_i\colon K=F(\alpha)\to F(\alpha_i)$ che lascia fisso ogni elemento di *F* e tale che $\sigma_i(\alpha)=\alpha_i$. Esso è evidentemente unico, e definisce un monomorfismo $\sigma_i\colon K=F(\alpha)\to L$. Viceversa, dato un monomorfismo σ siffatto, si ha che $\sigma(\alpha)=\alpha_i$ per qualche *i*, e quindi $\sigma=\sigma_i$. □

Osservazione 6.5 In base alla dimostrazione che abbiamo appena dato, gli *n* monomorfismi si trovano:
- determinando un elemento primitivo per l'estensione *K* di *F*;
- trovando le sue *n* radici coniugate su *F*;
- inviando l'elemento primitivo in ognuna delle sue radici coniugate.

Osserviamo che i monomorfismi di campo σ_i introdotti sopra inducono, in particolare, monomorfismi tra i rispettivi gruppi moltiplicativi. Il prossimo risultato mostrerà che tali monomorfismi sono linearmente indipendenti.

Teorema 6.6 (*Lemma di Dedekind*) Sia *G* un gruppo, e sia *K* un campo. Siano $\sigma_1,\ldots,\sigma_n$ omomorfismi di gruppi da *G* a *K** a due a due distinti. Allora questi sono linearmente indipendenti su *K*.

Dimostrazione: Supponiamo che *G* sia un gruppo moltiplicativo. Proviamo che per ogni *n*-upla di elementi $c_1,\ldots,c_n\in K$ tali che

$$\sum_{i=1}^{n}c_i\sigma_i=0, \tag{1}$$

si ha $c_1=\cdots=c_n=0$. Procediamo per induzione su *n*. Per *n*=1 non v'è nulla da provare. Supponiamo allora $n>1$ e la tesi vera per valori di *n* più piccoli. Per ogni $g\in G$ da (1) segue che

$$\sum_{i=1}^{n} c_i \sigma_i(g) = 0. \tag{2}$$

Fissiamo $h \in G$. Allora si ha

$$\sum_{i=1}^{n} c_i \sigma_i(gh) = \sum_{i=1}^{n} c_i \sigma_i(g)\sigma_i(h) = 0. \tag{3}$$

D'altra parte, moltiplicando (2) per $\sigma_j(h)$, si ottiene

$$\sum_{i=1}^{n} c_i \sigma_i(g)\sigma_j(h) = 0. \tag{4}$$

Sottraendo membro a membro la (4) dalla (3):

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} c_i(\sigma_i(h) - \sigma_j(h))\sigma_i(g) = 0.$$

Data l'arbitrarietà di *g*, si ha:

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} c_i(\sigma_i(h) - \sigma_j(h))\sigma_i = 0.$$

Abbiamo così ottenuto una combinazione lineare nulla, a coefficienti in *K*, di $n-1$ omomorfismi. Per l'ipotesi induttiva segue che, per ogni $i = 1,\dots,n$, $i \neq j$,

$$c_i(\sigma_i(h) - \sigma_j(h)) = 0.$$

Se fosse $c_i \neq 0$, per qualche *i*, allora sarebbe $\sigma_i(h) - \sigma_j(h) = 0$, e quindi, data l'arbitrarietà di *h*, sarebbe $\sigma_i = \sigma_j$, contro l'ipotesi. Segue che $c_i = 0$ per ogni $i \neq j$. Data l'arbitrarietà di *j*, segue che $c_i = 0$ per ogni *i*. □

Proposizione 6.7 Sia *F* un campo, e sia *K* una sua estensione algebrica semplice. Allora il numero di sottocampi di *K* contenenti *F* (cioè, dei *campi* intermedi tra *F* e *K*) è finito.

<u>Dimostrazione:</u> Esiste, per ipotesi, un elemento $\alpha \in K$ tale che $K = F(\alpha)$. Sia *L* un campo intermedio tra *F* e *K*. Sia $p(x)$ il polinomio minimo di α su *F*, sia $q(x)$ il polinomio minimo di α su *L*. Allora $q(x)$ divide $p(x)$ in $K[x]$. Sia *H* il sottocampo di *K* generato da *F* e dai coefficienti del polinomio $q(x)$. Si ha

$$F \subset H \subset L \subset K,$$

e

$$K = F(\alpha) \subset H(\alpha) \subset L(\alpha) \subset K(\alpha) = K,$$

per cui vale ovunque l'uguaglianza. Osserviamo che $q(x)$ è anche il polinomio minimo di α su *H*. Dunque

$$[L(\alpha):L]=[H(\alpha):H],$$

da cui segue che $H=L$. Abbiamo così provato che ogni campo intermedio L è generato su F dai coefficienti di un polinomio (monico) che divide $p(x)$ in $K[x]$. Ma i polinomi siffatti sono in numero finito. Ciò basta per concludere. □

Il risultato si può invertire come segue nel caso di un campo infinito.

Proposizione 6.8 Sia F un campo infinito, e sia K un'estensione finita su F tale che il numero di campi intermedi tra F e K è finito. Allora K è un'estensione semplice di F.

Dimostrazione: Sia $K=F(\alpha_1,..,\alpha_n)$. Basta provare la tesi per n = 2, il resto è induzione. Per ogni $c,d\in F$ i campi $F(\alpha_1+c\alpha_2), F(\alpha_1+d\alpha_2)$ sono campi intermedi tra F e K. Essendo F infinito, esistono c,d distinti tali che $L=F(\alpha_1+c\alpha_2)=F(\alpha_1+d\alpha_2)$. Allora

$$\alpha_1+c\alpha_2-(\alpha_1+d\alpha_2)=(c-d)\alpha_2\in L, \quad \text{e quindi} \quad \alpha_2\in L, \text{ per cui } \alpha_1\in L.$$

Pertanto $K=L$. □

Per completezza, diamo ora un risultato sui campi intermedi in un'estensione *trascendente* semplice. Ne omettiamo la dimostrazione.

****Teorema 6.9** (*Lüroth*) Sia F un campo, e sia $F(\theta)$ una sua estensione trascendente. Allora per ogni campo $K\neq F$ tale che $F\subset K\subset F(\theta)$ esiste $\mu\in F(\theta)$, trascendente su F, tale che $K=F(\mu)$.

Dimostrazione: [Mo], Theorem 22.19, oppure [Mi2], Theorem 9.19.

$$H\subset L\subset L(\alpha)$$

$$\left.\begin{array}{l}[\mathbf{L(\alpha)}:H]=[\mathbf{L(\alpha):L}][L:H]\\ [\mathbf{H(\alpha)}:H]\quad[\mathbf{H(\alpha):H}]\end{array}\right\}\Rightarrow[L:H]=1$$