Lezione 11

Prerequisiti: Lezione 5.

Estensioni normali.

Sia F un campo, sia K una sua estensione algebrica.

Definizione 11.1 Si dice che K è un'estensione *normale* di F se per ogni $\alpha \in K$ il polinomio minimo di α su F si spezza su K nel prodotto di fattori lineari (equivalentemente, se per ogni $\alpha \in K$ tutte le sue radici coniugate su F appartengono a K).

Osservazione 11.2
a) Se K è algebricamente chiuso, allora è un'estensione normale di F.
b) Se L è un campo intermedio tra F e K, e K è normale su F, allora K è normale su L: basta osservare che, per ogni $\alpha \in K$ il polinomio minimo di α su L è un fattore del suo polinomio minimo su F.
c) Se K è il campo di spezzamento di un polinomio $f(x) \in F[x]$ su F, e $\alpha \in K$, allora, in base alla Proposizione 4.1 ed al Teorema di estensione degli isomorfismi, forma forte (Teorema 4.6) $\widetilde{\alpha} \in K$ è una radice coniugata di α su F se e solo se esiste un F-automorfismo φ di K tale che $\varphi(\alpha) = \widetilde{\alpha}$.

Esempi 11.3
a) $\mathbf{C}$ è un'estensione normale di $\mathbf{R}$.
b) $\mathbf{Q}(\sqrt{2})$ è un'estensione normale di $\mathbf{Q}$. Infatti, per ogni $a, b \in \mathbf{Q}$, l'altra radice coniugata di $a + b\sqrt{2}$ è $a - b\sqrt{2}$.
c) $\mathbf{Q}(\sqrt[3]{2})$ non è un'estensione normale di $\mathbf{Q}$. Infatti a $\mathbf{Q}(\sqrt[3]{2})$ non appartengono $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ (dove ω è una radice cubica primitiva dell'unità), che sono le radici coniugate di $\sqrt[3]{2}$ su $\mathbf{Q}$.

Il prossimo enunciato chiarirà la natura delle estensioni normali. Ricordiamo che, come stabilito dalla Proposizione 22.6 di Algebra 2, ogni estensione finita è algebrica.

Teorema 11.4 Sia K un'estensione finita di F. Sono equivalenti le seguenti condizioni:

a) K è un'estensione normale di F.
b) K è il campo di spezzamento su F di un polinomio $f(x) \in F[x]$.
c) Per ogni estensione L di K, ogni F-omomorfismo di campi da K in L induce un F-automorfismo di K.

Dimostrazione: Proviamo che a) $\Rightarrow$ b). Sia K un'estensione normale di F. In base alla Proposizione 4.10, esiste $f(x) \in F[x]$ tale che il suo campo di spezzamento L su F contenga K, ed ogni fattore irriducibile di $f(x)$ in $F[x]$ possieda una radice in K. A causa della normalità di K su F, segue che ognuno di questi fattori irriducibili si spezza su K nel prodotto di fattori lineari. Quindi, per la condizione di minimalità contenuta nella definizione di campo di spezzamento (vedi Algebra 2, Definizione 23.1), $K = L$.
Proviamo che b) $\Rightarrow$ c). Sia K il campo di spezzamento su F di un polinomio $f(x) \in F[x]$, e sia L una sua estensione. Sia $\varphi : K \to L$ un F-omomorfismo. Poiché questo è necessariamente iniettivo,

resta indotto un F-isomorfismo di campi $K \to \varphi(K)$, che si estende ad un F-isomorfismo di anelli $\overline{\varphi} : K[x] \to \varphi(K)[x]$, nel modo visto nella Lezione 4. Allora, naturalmente, $\varphi(K)$ è un campo di spezzamento di $\overline{\varphi}(f(x)) = f(x)$ su F che è, come K, contenuto in L. Allora, in virtù della Proposizione 4.7, $\varphi(K) = K$.
Proviamo infine che c) $\Rightarrow$ a). Sia $\alpha \in K$ e sia $f(x) \in F[x]$ il suo polinomio minimo su F. In base alla Proposizione 4.10, esiste $g(x) \in F[x]$ tale che il suo campo di spezzamento L su F contenga K, e $g(\alpha) = 0$. Allora, per le proprietà del polinomio minimo (vedi Algebra 2, Lezione 22), $f(x)$ divide $g(x)$, quindi L contiene un campo di spezzamento L' di $f(x)$ su F. Per il Teorema di estensione degli isomorfismi, forma forte (Teorema 4.6) per ogni radice β di $f(x)$ in L esiste allora un F-automorfismo $\varphi : L \to L$ tale che $\varphi(\alpha) = \beta$. In virtù di c), si ha $\varphi(K) = K$, e quindi $\beta \in K$. Ciò prova che ogni radice di $f(x)$ in L' appartiene a K. Quindi K è normale su F. □

Il Teorema precedente caratterizza le estensioni normali come i campi di spezzamento. In particolare abbiamo scoperto che

Esempio 11.5 $\mathbf{Q}(\sqrt[3]{2})$ non è il campo di spezzamento su **Q** di alcun polinomio.

Lemma 11.6 Si ha $G(K, K_{G(K,F)}) = G(K, F)$.

Dimostrazione: Basta osservare che, per definizione di campo fisso, e in base all'Osservazione 10.9, un automorfismo di K lascia fissi gli elementi di F se e solo se lascia fissi gli elementi di $K_{G(K,F)}$. □

Vediamo ora il legame tra la normalità di un'estensione e il campo fisso del relativo gruppo di Galois.

Teorema 11.7 Sia K un'estensione finita di F. Sono equivalenti le seguenti condizioni:

a) K è normale e separabile su F.
b) $|G(K, F)| = [K : F]$.
c) $K_{G(K,F)} = F$.

Dimostrazione: Proviamo a) $\Rightarrow$ b). Supponiamo che K sia normale e separabile su F. Allora, in base al Teorema 11.4, K è un campo di spezzamento di un polinomio $f(x) \in F[x]$. In base al Teorema 10.7 basta provare che $|G(K, F)| \geq [K : F]$. Per l'ipotesi di separabilità si può applicare il Teorema dell'elemento primitivo (Teorema 6.1), quindi esiste $\alpha \in K$ tale che $K = F(\alpha)$. Sia $p(x)$ il polinomio minimo di α su F, sia $n = \deg p(x)$. Allora, come abbiamo visto in Algebra 2, Lezione 22, $n = [K : F]$. Inoltre $p(x)$ ha n radici distinte $\alpha_1, ..., \alpha_n$ in K. Per il Teorema di estensione degli isomorfismi, forma forte (Teorema 4.6), per ogni $i = 1, ..., n$ esiste $\varphi_i \in G(K, F)$ tale che $\varphi_i(\alpha) = \alpha_i$. Quindi $|G(K, F)| \geq n$, come volevasi.
Proviamo che b) $\Rightarrow$ c). Sia $|G(K, F)| = [K : F]$. Sia $L = K_{G(K,F)}$. Sappiamo dall'Osservazione 10.9 che $F \subset L$. Inoltre, per il Lemma 11.6, si ha $G(K, L) = G(K, F)$. Quindi, in virtù del Teorema 10.7,

$$[K : F] = |G(K, F)| = |G(K, L)| \leq [K : L] \leq [K : F],$$

quindi vale ovunque l'uguaglianza, ovvero $F = L$.
Proviamo che c) $\Rightarrow$ a). Supponiamo che $K_{G(K,F)} = F$. Sia $\alpha \in K$. In virtù del Teorema 10.7, $G(K,F)$ è finito, e quindi lo è anche l'insieme $S = \{\varphi(\alpha) | \varphi \in G(K,F)\} \subset K$. Sia

$$f(x) = \prod_{\beta \in S} (x - \beta) \in K[x].$$

Poiché ogni $\varphi \in G(K,F)$ induce una permutazione su *S*, i coefficienti di *f*(*x*), che, in virtù delle formule di Viète (Proposizione 7.11), sono espressioni polinomiali simmetriche dei β, appartengono al campo fisso di $G(K,F)$, cioè, per ipotesi, $f(x) \in F[x]$. Inoltre $f(\alpha) = 0$. Sia *p*(*x*) il polinomio minimo di α su *F*. Allora *p*(*x*) divide *f*(*x*). Inoltre ogni $\beta \in S$ è radice di *p*(*x*). Segue che *f*(*x*) divide *p*(*x*). Siccome i due polinomi sono entrambi monici, si ha allora $f(x) = p(x)$. Ciò prova che $\alpha \in K$ è separabile su *F*, ed il suo polinomio minimo su *F* si spezza su *K* nel prodotto di fattori lineari. Quindi *K* è normale e separabile su *F*. □

Definizione 11.8 Un'estensione finita normale e separabile si dice *galoisiana* (o *di Galois*).

Osservazione 11.9 Se *L* è un campo intermedio tra *F* e *K*, e *K* è galoisiano su *F*, allora *K* è galoisiano su *L*. Ciò segue dalle Osservazioni 5.8 a) e 11.2 b).

Nota Alcuni autori usano il termine *normale* come sinonimo di *galoisiano*. Ciò è giustificato dalla seguente

Osservazione 11.10 In base alla Proposizione 5.11 (e al Corollario 5.13) un'estensione finita di un campo di caratteristica 0 (o di un campo finito) è normale se e solo se è galoisiana. In particolare, per il Teorema 11.4, le estensioni galoisiane di tali campi sono esattamente i campi di spezzamento dei polinomi.

Esempio 11.11 Il Teorema 11.7 è utile alla determinazione dei gruppi di Galois.

a) Determiniamo $G(\mathbf{Q}(\sqrt{2},\sqrt{3}),\mathbf{Q})$. A questo gruppo avevamo dedicato l'Osservazione 4.9. Poiché $\mathbf{Q}(\sqrt{2},\sqrt{3})$ è un campo di spezzamento di un polinomio $f(x) \in \mathbf{Q}[x]$ su **Q**, che è un campo di caratteristica 0, per l'Osservazione 11.10, è un'estensione galoisiana di **Q.** Quindi, per il Teorema 11.7,

$$\left|G(\mathbf{Q}(\sqrt{2},\sqrt{3}),\mathbf{Q})\right| = [\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}] = 4.$$

D'altra parte, per il Corollario 10.3, $G(\mathbf{Q}(\sqrt{2},\sqrt{3}),\mathbf{Q})$ è isomorfo ad un sottogruppo di S_4, essendo ogni suo elemento univocamente determinato dalla permutazione che esso induce sulle quattro radici di

$$f(x) = (x^2 - 2)(x^2 - 3).$$

Le permutazioni ammissibili (ossia compatibili col fatto che **Q** viene lasciato fisso) sono comprese tra le seguenti:

$$\begin{array}{cccc} \sqrt{2}\mapsto\sqrt{2} & \sqrt{2}\mapsto-\sqrt{2} & \sqrt{2}\mapsto\sqrt{2} & \sqrt{2}\mapsto-\sqrt{2} \\ -\sqrt{2}\mapsto-\sqrt{2} & -\sqrt{2}\mapsto\sqrt{2} & -\sqrt{2}\mapsto-\sqrt{2} & -\sqrt{2}\mapsto\sqrt{2} \\ \sqrt{3}\mapsto\sqrt{3} & \sqrt{3}\mapsto\sqrt{3} & \sqrt{3}\mapsto-\sqrt{3} & \sqrt{3}\mapsto-\sqrt{3} \\ -\sqrt{3}\mapsto-\sqrt{3} & -\sqrt{3}\mapsto-\sqrt{3} & -\sqrt{3}\mapsto\sqrt{3} & -\sqrt{3}\mapsto\sqrt{3} \end{array}$$

Quindi sono tutte le permutazioni cercate. $G(\mathbf{Q}(\sqrt{2},\sqrt{3}),\mathbf{Q})$ è dunque isomorfo al seguente sottogruppo di S_4:

$$\{\mathrm{id},(12),(34),(12)(34)\},$$

che è isomorfo al gruppo di Klein.

b) Determiniamo $G(\mathbf{Q}(\sqrt[3]{2},\omega),\mathbf{Q})$, ove ω è una radice primitiva cubica dell'unità. Ricordiamo che $\mathbf{Q}(\sqrt[3]{2},\omega)$ è il campo di spezzamento su $\mathbf{Q}$ del polinomio

$$f(x)=x^3-2,$$

ed è dunque un'estensione galoisiana di $\mathbf{Q}$. Quindi, in base al Teorema 10.7,

$$\left|G(\mathbf{Q}(\sqrt[3]{2},\omega),\mathbf{Q})\right|=[\mathbf{Q}(\sqrt[3]{2},\omega):\mathbf{Q}]=6.$$

Poiché $G(\mathbf{Q}(\sqrt[3]{2},\omega),\mathbf{Q})$ è isomorfo ad un sottogruppo di S_3, si ha $G(\mathbf{Q}(\sqrt[3]{2},\omega),\mathbf{Q})\cong S_3$.

Nella prossima lezione determineremo esplicitamente tutti gli elementi di $G(\mathbf{Q}(\sqrt[3]{2},\omega),\mathbf{Q})$, identificandoli con le permutazioni che essi inducono sulle radici $\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$. Indicheremo, per ciascuno di essi, le immagini degli elementi $1,\sqrt[3]{2},\sqrt[3]{4},\omega,\omega\sqrt[3]{2},\omega\sqrt[3]{4}$, che formano una base di $\mathbf{Q}(\sqrt[3]{2},\omega)$ su $\mathbf{Q}$.