ESTENSIONI DI GALOIS

Definizione Siano $E \supseteq F$ campi

- E si dice *algebrico* su F se per ogni $a \in E$ a è algebrico su F

(osservazione: $[E:F] < \infty \Rightarrow E$ algebrico su F)

Supponiamo E algebrico su F:

- E si dice *separabile* su F se per ogni $a \in E$ il polinomio minimo di a su F è separabile

(osservazione: F perfetto $\Rightarrow E$ separabile)

- E si dice *normale* su F se per ogni $q(x) \in F[x]$ $q(x)$ irriducibile tale che esiste $u \in E$ radice di $q(x)$, allora abbiamo che $q(x) = a \prod_{i=1}^{n} (x - k_i)$ in $E[x]$

Osservazione: 1) E è normale su F se e solo se il campo di spezzamento di un polinomio minimo di $a \in E$ è contenuto in E

2) E è normale e separabile su F se e solo se per ogni $a \in E$ il polinomio minimo di a si scompone in $E[x]$ in fattori lineari distinti

Teorema: Siano $E \supseteq F$ campi, sono equivalenti

1) E è un campo di spezzamento di un polinomio sep $q(x) \in F[x]$
2) Esiste $G \leq Aut(E)$ con $|G| < \infty$ tale che $F = Fix(G)$
3) $[E:F] < \infty$ e E è normale e separabile su F

Se queste condizioni sono verificate abbiamo che:

- $Fix(Gal(E/F)) = F$
- se $G \leq Aut(E)$ è tale che $F = Fix(G)$ allora $G = Gal\left(\frac{E}{Fix(G)}\right)$

Definizione Se un'estensione $E \supseteq F$ soddisfa le condizioni 1) e) e 3) del teorema, allora $E \supseteq F$ viene chiamata **estensione di Galois**

Dim. teorema:

1) $\Rightarrow$ 2) Sia $G = Gal(E/F)$ e $F' = Fix(G)$ allora $F' = Fix(G) = Fix(Gal(E/F)) \supseteq F$

(verificata lezione precedente)

Dimostriamo $F = F'$ (da cui segue anche il primo punto della seconda parte delle tesi)

Per ipotesi E è un campo di spezzamento di $q(x)$ su F e quindi anche su F'

$G \subseteq Gal(E/F')$ perchè $F' = Fix(G)$

$F \subseteq F' \Rightarrow Gal(E/F') \subseteq Gal(E/F) = G$

$\Rightarrow \boxed{Gal(E/F') = G}$

Per il Lemma 1 della precedente lezione

$[E : F'] = [E : F] = |G|$

Inoltre $[E : F] = [E : F'][F' : F]$ da cui

$|G| \quad\quad |G|$

Otteniamo $[F' : F] = 1$ concludendo $F = F'$

2) $\Rightarrow$ 3) Per il Lemma di Artin (Lemma 2 precedente lezione) abbiamo che $[E : F] \leq |G| < \infty$

Siccome $[E : F] < \infty$, E è algebrico su F

Sia $q(x)$ irriducibile in $F[x]$ con u radice in E ($q(u) = 0$)

Sia $f \in G$, siccome $\mathcal{F} = Im\,\sigma(G)$ l'automorfismo f manda radici di $q(x)$ in radici di $q(x)$

Consideriamo $\{u = u_1, \dots, u_k\}$ orbita di u sotto l'azione di G (supponiamo $u_i \neq u_j$ per $i \neq j$)

Il polinomio $q(x)$ è divisibile per

$h(x) \overset{def}{=} (x - u_1) \dots (x - u_k)$

Per $f \in G$ consideriamo l'estensione $\tilde{f} : E[x] \to E[x]$ tale che $\tilde{f}(c) = c$ per ogni $c \in E$ e $\tilde{f}(x) = x$

$$\tilde{f}(h(x)) = (x - \tilde{f}(u_1)) \dots (x - \tilde{f}(u_k))$$
$$= (x - f(u_1)) \dots (x - f(u_k))$$
$$= (x - u_1) \dots (x - u_k) = h(x)$$

$\{u_1, \dots, u_k\}$ orbita di u rispetto all'azione di G

u

$\{u_1, \dots, u_k\}$ è G-invariante quindi $\{u_1, \dots, u_k\} = \{f(u_1), \dots f(u_k)\}$

e quindi riordinando i fattori otteniamo l'uguaglianza

Inoltre

$$h(x) = a_0 + \dots + a_{k-1}x^{k-1} + x^k \text{ con } a_i \in E$$

e

$$\tilde{f}(h(x)) = f(a_0) + \dots + f(a_{k-1})x^{k-1} + x^k$$

Siccome $h(x) = \tilde{f}(h(x)) \Rightarrow f(a_i) = a_i \ \forall i$

Per genericità di f otteniamo che $a_i \in \mathrm{Fix}\, G = F$

Concludiamo che:

$$\left.\begin{array}{l} h(x) \in F[x] \text{ e } h(x) \mid q(x) \\ q(x) \text{ irriducibile in } F[x] \end{array}\right\} \Rightarrow q(x) = h(x)$$

Per cui $q(x)$ è scomponibile in fattori lineari distinti in $E[x]$ ◢

3) $\Rightarrow$ 1) Siccome $[E:F] < \infty$ allora

$E = F(r_1, r_2, \dots, r_k)$ con r_i algebrico su F

$(r_i \neq r_j$ per $i \neq j)$

Problema: Dato E estensione di F dimostrare che

$$[E:F] < \infty$$

se e solo se

esistono $r_1, r_2, \dots, r_k \in E$ elementi algebrici su F tali che $E = F(r_1, \dots, r_k)$

Sia $f_i(x)$ il polinomio minimo di r_i su F

$\Rightarrow$

$f_i(x)$ prodotto di fattori lineari distinti in $E[x]$

E campo di spezzamento di $g(x) = \prod f_i(x)$

che è separabile

Rimane il secondo punto della seconda parte della tesi:

sia G tale che $F = \mathcal{Y}_{inv}(G)$

per il Lemma di Artin $[E:F] \leq G$ e siccome

E campo di spezzamento di un polinomio separabile (condizione 1) possiamo applicare il Lemma 1 e otteniamo $|Gal(E/F)| = [E:F]$

$\Rightarrow$ $\boxed{|Gal(E/F)| \leq |G|}$

D'altra parte $G \subseteq Gal(E/F)$ perchè gli elementi di G fissano F

Possiamo concludere $G = Gal(E/F) = Gal\left(\frac{E}{\mathcal{Y}_{inv}(G)}\right)$

Problema: trovare un'estensione di $\mathbb{Q}$ che non è di Galois