GRUPPI DI GALOIS

Sia F sottocampo di E (E estensione di F)

Def: Sia $f: E \to E$ automorfismo;
f si dice **automorfismo di E/F**
se $f(a) = a$ per ogni $a \in F$

Considero $Gal(E/F) = \{f: E \to E \mid f \text{ autom. di } E/F\}$
con la composizione di applicazioni.

$Gal(E/F)$ è un gruppo e viene chiamato
il **gruppo di Galois** di E su F.

Esempi 1) Sia $E = F[u]$ con $\text{char } F \neq 2$
$u \notin F$ e $u^2 = a \in F$ (per esempio $E = \mathbb{Q}[\sqrt{2}]$)

Dalle condizioni imposte si vede facilmente
che u algebrico di grado 2 su F con
polinomio minimo $x^2 - a \in F[x]$

Sia $f \in Gal(E/F)$,
[sappiamo $f(a) = a$ $\forall a$ e vogliamo capire chi è $f(u)$]

$u^2 - a = 0 \Rightarrow f(u^2 - a) = a \Rightarrow f(u^2) - f(a) = 0$

$\Rightarrow [f(u)]^2 - \underbrace{f(a)}_{\| \; a} = 0 \Rightarrow f(u)$ radice di $x^2 - a$

Le radici di $x^2 - a$ sono $u, -u$ quindi $f(u) = \pm u$

[$u \neq -u$ perché char $F \neq 2$]

Consideriamo $\{1, u\}$ base di E su F

Sappiamo che $E = \{ c + d u \mid c, d \in F \}$

Abbiamo due possibilità:

- se $f(u) = u$

  $f(c + du) = f(c) + f(d) f(u) = c + du = Id(c + du)$

  $(\Rightarrow f = Id_{|E})$

- se $f(u) = -u$

  $f(c + du) = f(c) + f(d) f(u) = c - du$

Entrambe le possibilità danno un automorfismo di E/F Otteniamo che $Gal(E/F)$ ha due elementi ($Gal(E/F) \cong \mathbb{Z}_2$)

2) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ estensione di grado 4 di $\mathbb{Q}$

base di E su $\mathbb{Q} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

x^2-2 polinomio minimo di $\sqrt{2}$

x^2-3 polinomio minimo di $\sqrt{3}$

analogamente all'esempio precedente abbiamo che se $f \in Gal(E/\mathbb{Q})$ allora $f(\sqrt{2})$ (risp. $f(\sqrt{3})$) è una radice di x^2-2 (risp. x^2-3)

Abbiamo quindi quattro possibilità:

Id_E: $\sqrt{2} \longrightarrow \sqrt{2}$, $\sqrt{3} \longrightarrow \sqrt{3}$

f_1: $\sqrt{2} \longrightarrow -\sqrt{2}$, $\sqrt{2} \longrightarrow -\sqrt{3}$

f_2: $\sqrt{2} \longrightarrow -\sqrt{2}$, $\sqrt{2} \longrightarrow +\sqrt{3}$

f_3: $\sqrt{2} \longrightarrow \sqrt{2}$, $\sqrt{3} \longrightarrow -\sqrt{3}$

tutte e quattro le possibilità danno un automorfismo di campo

$$|Gal(E/\mathbb{Q})| = 4$$

Ci sono due possibilità $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

oppure $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_4$

Si può facilmente calcolare che

$$f_i^2(u_1+u_2\sqrt{2}+u_3\sqrt{3}+u_4\sqrt{2}\sqrt{3})$$

$$= u_1+u_2\sqrt{2}+u_3\sqrt{3}+u_4\sqrt{2}\sqrt{3}$$

da cui $f_i^2 = Id_E$

Possiamo concludere $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

3) Sia F di caratteristica p tale che $F \neq F^p$

(F non è perfetto)

Consideriamo $a \in F \setminus F^p \underset{\text{Lemma}}{\Rightarrow} x^p - a$ irriducibile in $F[x]$

▶ Consideriamo $E \overset{def}{=} \frac{F[x]}{(x^p-a)}$ estensione di F che contiene

$u \overset{def}{=} x + (x^p-a)$ radice di x^p-a

▶ Sappiamo che $E = F(u)$

($in\ E[x]\ x^p-a = (x-u)^p \Rightarrow E$ campo di spezz di x^p-a)

Se $\eta \in Gal(E/F)$ allora $\eta(u)$ radice di x^p-a

($\eta(u)^p = \eta(u^p) = \eta(a) = a$)

$\Rightarrow \eta(u) = u \underset{E=F(u)}{\Rightarrow} \eta = Id_E \Rightarrow \boxed{Gal(E/F) = \{Id_E\}}$

u unica radice di (x^p-a)

(Osserviamo $[E:F] = p$)

Def

Sia $G \leq Aut(E)$ definiamo:

$$Inv(G) \overset{def}{=} \{a \in E \mid \eta(a) = a \ \forall \eta \in G\}$$

che è un sottocampo di E chiamato il campo fissato da G o il campo dei G-invarianti

Osservazione: Fisso un campo E abbiamo due applicazioni:

$$\{\text{sottogruppi di } Aut\,E\} \longrightarrow \{\text{sottocampi di } E\}$$
$$G \longrightarrow Inv(G)$$

$$\{\text{sottocampi di } E\} \longrightarrow \{\text{sottogruppi di } Aut\,E\}$$
$$F \longrightarrow Gal(E/F)$$

Proposizione: Siano G_1, G_2 sottogr di $Aut\,E$ e F_1, F_2 sottocampi di E

1) $G_1 \supseteq G_2 \Rightarrow Inv\,G_1 \subseteq Inv\,G_2$
2) $F_1 \supseteq F_2 \Rightarrow Gal(E/F_1) \subseteq Gal(E/F_2)$
3) $Inv(Gal(E/F_1)) \supseteq F_1$
4) $Gal(E/Inv\,G_1) \supseteq G_1$

Dim: uso le definizioni

Consideriamo E campo di spezzamento di un polinomio $p(x)$ su F

$$Gal(E/F) = \{ \eta : E \to F \mid \eta(a) = a \quad a \in F \}$$

$$= \{ \text{estensioni a } E \text{ dell'identità di } F \}$$

Abbiamo dimostrato un teorema che stima il numero delle estensioni di questo tipo usando questo teorema otteniamo:

$$\boxed{|Gal(E/F)| \leq [E:F]}$$ [importante]

Inoltre se $p(x)$ è separabile e $p(x) = q_1(x)^{e_1} \cdot \ldots \cdot q_k(x)^{e_k}$ e la sua scomposizione in fattori irriducibili

F può essere visto come campo di spezzamento di $q(x) = q_1(x) \ldots q_k(x)$ che ha solo radici semplici ($q(x)$ ha $\deg q(x)$ radici distinte)

In questo caso il teorema ci dice che $|Gal(E/F)| = [E:F]$

Otteniamo quindi il seguente Lemma

Lemma 1 Se E campo di spezzamento di $p(x) \in F[x]$ polinomio separabile allora

$$|Gal(E/F)| = [E:F]$$

[Se F è perfetto vale per tutti i campi di spezzamento]

Consideriamo ora un altro importante Lemma

Lemma 2 (Artin) Sia E campo e $G \leq Aut E$ con $|G| < \infty$

Allora $$[E : Inv(G)] \leq |G|$$

Dim: Richiamo:

Prop $a_{ij} \in E$ campo e considero il seguente sist. lin.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m = 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m = 0 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nm}x_m = 0 \end{cases}$$

La dimensione dello spazio delle soluzioni è $m - rank(a_{ij})$

Se $n < m$ allora $m - rank(a_{ij}) > 0$,

in particolare esiste almeno una soluzione non banale

Dimostreremo che dati $n = |G|$ e $\{u_1, \dots, u_m\} \subseteq E$
se $m > n$ allora $\{u_1, \dots, u_m\}$ è linearmente dipendente su $\mathrm{Inv}(G)$

[questo implica la tesi del Lemma di Artin]

Sia $G = \{\eta_1, \dots, \eta_n\}$ con $\eta_1 = \mathrm{Id}_E$

Considero il sistema:

$$\begin{cases} \eta_1(u_1)x_1 + \eta_1(u_2)x_2 + \dots + \eta_1(u_m)x_m = 0 \\ \vdots \\ \eta_n(u_1)x_1 + \eta_n(u_2)x_2 + \dots + \eta_n(u_m)x_m = 0 \end{cases}$$

Siccome $m > n$ esistono soluzioni non banali

Sia $(b_1, \dots, b_m)$ una soluzione non banale con
il minimo numero di entrate non nulle

Riordinando possiamo supporre $b_1 \neq 0$

$\Rightarrow b_1^{-1}(b_1, \dots, b_m)$ soluzione non banale con minimo numero di entrate non nulle

$\Rightarrow$ posso supporre $b_1 = 1$

Claim: $b_i \in Ker\ G$ per ogni i

Questo implica la lineare dipendenza di $\{u_1, \dots, u_m\}$ perchè dalla I equazione del sistema otteniamo $\sum b_i u_i = 0$ perché $\eta_1 = Id_E$

dimostrazione del claim: si ragiona per assurdo supponendolo che esista $b_j \notin Ker(G)$

Possiamo assumere $b_2 \notin Ker(G)$, allora esiste k t.c. $\eta_k(b_2) \neq b_2$

$$\sum_{j=1}^{m} \eta_i(u_j) b_j = 0 \quad \text{per ogni } i$$

$$\Downarrow$$

$$\eta_k\left(\sum_{j=1}^{m} \eta_i(u_j) b_j\right) = 0 \quad \text{per ogni } i$$

$$\Downarrow$$

$$\sum_{j=1}^{m} \eta_k \circ \eta_i(u_j)\, \eta_k(b_j) = 0 \quad \text{per ogni } i$$

$$\Downarrow$$

$G \to G$ è una
$g \to \eta_k \circ g$ biezione

$$\sum_{j=1}^{m} \eta_i(u_i)\, \eta_k(b_j) \quad \text{per ogni } i$$

$(1, b_2, \dots, b_m)$ e $(1, \eta_k(b_2), \dots, \eta_k(b_m))$

Sono entrambe soluzioni del sistema

Facendo la differenza otteniamo un altra soluzione del sistema:

$(1, b_2, \dots, b_m) - (1, \eta_k(b_2), \dots, \eta_k(b_m)) =$

$= (\underbrace{1-1}_{=0}, \underbrace{b_2 - \eta_k(b_2)}_{\neq 0 \text{ perché } b_2 \neq \eta_k(b_2)}, \dots, b_m - \eta_k(b_m))$

$b_2 - \eta_k(b_2) \neq 0$ implica che ho una soluzione non banale

Siccome $b_j = 0 \Rightarrow b_j - \eta_k(b_j) = 0$, aumentano il numero di entrate nulle rispetto a quello di $(1, b_2, \dots, b_k)$ (nella nuova soluzione la prima entrata è nulla)

Però $(1, b_2, \dots, b_k)$ è una soluzione non banale con il numero minimo di entrate non nulle.

(del Claim e del Lemma)