14.2 The Fundamental Theorem of Galois Theory.

Definition. A (linear) *character* of a group G over a field F is a homomorphism

$$\chi : G \to F^*.$$

Example. det: $GL(n, F) \to F^*$

sign: $S_n \to \mathbb{R}^*$

Definition. Characters $\chi_1, \dots, \chi_n$ of G are *linearly independent* over F if

$$\forall a_1, \dots, a_n \in F : \sum_{i=1}^{n} a_i \chi_i = 0 \Rightarrow a_1 = \dots = a_n = 0,$$

(linearly independent in the space of functions F^G) $= \{ f : G \to F \}$.

Theorem (Dirichlet). *Any set $\chi_1, \dots, \chi_n$ of distinct characters of G over F is linearly independent.*

Proof. see book.

Corollary. *Distinct automorphisms of a field K are linearly independent (in K^K).*

Proof. Every $\varphi \in \mathrm{Aut}\, K$ restricts to a character $\varphi|_{K^*}$ over K. $\square$

Theorem. *Let H be a finite subgroup of* $\mathrm{Aut}\,(K)$ *and* $F := \mathrm{Fix}(H)$*. Then*

$$[K : F] = |H|.$$

Proof. Let $H = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$, let $\alpha_1, \dots, \alpha_r$ a basis of K over F.

1) Suppose $n > r$. Then

$$\begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \\ \sigma_1(\alpha_r) & \cdots & \sigma_n(\alpha_r) \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

has nontrivial solution $\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \neq 0$ over K.

Let $a_1, \dots, a_r \in F$ arbitrary

$$(*) \qquad [a_1, \dots, a_r] \cdot \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_r) & \cdots & \sigma_n(\alpha_r) \end{bmatrix} = \Big[\underbrace{\sum_{i=1}^r a_i \sigma_1(\alpha_i)}_{\sigma_1(\underbrace{\sum a_i \alpha_i}_{=:b})}, \dots, \underbrace{\sum_{i=1}^r a_i \sigma_n(\alpha_i)}_{\sigma_n(\underbrace{\sum a_i \alpha_i}_{=b})}\Big]$$

because $a_i \in \mathrm{Fix}\, H$.

Multiply $(*)$ by $\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$ yields

$\sigma_1(b)\beta_1 + \dots + \sigma_n(b)\beta_n = 0$ for each $b \in K$.

Hence $\sigma_1, \dots, \sigma_n$ are lin dependent contradicting the previous Thm.

2) Suppose $n < r$. See book. □

Corollary. *Let K/F be a finite extension. Then*

$$|\mathrm{Aut}\,(K/F)| \text{ divides } [K : F]$$

with equality iff K/F is Galois

Proof. Let $E := \mathrm{Fix}\,(\mathrm{Aut}\,(K/F))$.

Then $F \subseteq E \subseteq K$ and

$[K : F] = \underbrace{[K : E]} \cdot [E : F]$

$= |\mathrm{Aut}\,(K/F)|$ by previous Thm □

Corollary. *Let H be a finite subgroup of* $\mathrm{Aut}\,(K)$ *and* $F := \mathrm{Fix}(H)$*. Then* $\mathrm{Aut}\,(K/F) = H$

Proof. $|H| = |K : F|$ by previous Thm

$= |\mathrm{Aut}\,(K/F)|$ since K/F is Galois by Closure Lemma
$\mathrm{Fix}\,(\mathrm{Aut}\,(K/\underbrace{\mathrm{Fix}(H)}_{F})) = \underbrace{\mathrm{Fix}\,(H)}_{F}$

Together with
$H \leq \mathrm{Aut}\,(K/F)$ we get $H = \mathrm{Aut}\,(K/F)$. □

Definition. If K/F is Galois, then

$$\mathrm{Gal}(K/F) := \mathrm{Aut}\,(K/F)$$

is the *Galois group* of K/F.

If $f(x) \in F[x]$ is separable with splitting field K, then $\mathrm{Gal}(K/F)$ is the *Galois group* of $f(x)$.

The Fundamental Theorem of Galois Theory.
Let K/F be a finite Galois extension with $G := Gal(K/F)$. Then

(1) $\mathrm{Fix}\colon \{H \leq G\} \to \{E : \ F \leq E \leq K\}$ *is a bijection with inverse* $\mathrm{Aut}\,(K/.)$.
(2) *For $H_1, H_2 \leq G$ with $E_1 := \mathrm{Fix}(H_1), E_2 := \mathrm{Fix}(H_2)$*
  (a) $H_1 \leq H_2$ *iff* $E_1 \geq E_2$,
  (b) $E_1 \cap E_2 = \mathrm{Fix}(\langle H_1 \cup H_2 \rangle)$,
  (c) $E_1 E_2 = \mathrm{Fix}(H_1 \cap H_2)$.

order reversing ? lattice anti- isomorphism

$$\begin{tikzcd} & E_1E_2 \arrow[dl, dash] \arrow[dr, dash] & \\ E_1 \arrow[dr, dash] & & E_2 \arrow[dl, dash] \\ & E_1 \cap E_2 & \end{tikzcd} \qquad \begin{tikzcd} & H_1 \cap H_2 \arrow[dl, dash] \arrow[dr, dash] & \\ H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\ & \langle H_1 \cup H_2 \rangle & \end{tikzcd}$$

(3) *For $H \leq G$ with $E := \mathrm{Fix}(H)$*
  (a) K/E *is Galois with* $\mathrm{Gal}(K/E) = H$,
  (b) $[K : E] = |H|$, $[E : F] = |G : H|$,
  (c) *For $\sigma \in G$,* $\mathrm{Aut}\,(K/\sigma(E)) = \sigma H \sigma^{-1}$,
  (d) *E/F is Galois iff H is normal in G. In this case* $\mathrm{Gal}(E/F) \cong G/H$.

$$\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \qquad \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array}$$

Proof. 1) By previous Corollaries

- $\mathrm{Aut}(K/\mathrm{Fix}(H)) = H$ for all $H \leq G$ (general)
- $\mathrm{Fix}(\underbrace{\mathrm{Aut}(K/E)}_{\leq G}) = E$ for all $F \leq E \leq K$ since K/E is Galois.

2 a) clear

b) $E_1 \cap E_2 \subseteq \mathrm{Fix}(\langle H_1 \cup H_2 \rangle)$ since fixed by H_1 and H_2.
Conversely, if $a \in K$ is fixed by H_1 and H_2. Then $a \in \mathrm{Fix}(H_1) \cap \mathrm{Fix}(H_2)$.

c) similar to 2b)

3 a) by 1)

b) follows from 3a)

c) Since H fixes E, $\sigma H \sigma^{-1}$ fixes $\sigma(E)$.
So $\sigma H \sigma^{-1} \subseteq \mathrm{Aut}(K/\sigma(E))$. But also
$|\sigma H \sigma^{-1}| = |H| = [K:E] = [K:\sigma(E)] \geq |\mathrm{Aut}(K/\sigma(E))|$.

d) Assume E/F is Galois. Then E is the splitting field of some $f(x) \in F[x]$.
For $\sigma \in G$, $\sigma(E)$ is the splitting field of $\sigma(f) = f$.
Since E is the unique smallest subfield of K in which f splits, $E = \sigma(E)$.
By 3c) this implies $\sigma H \sigma^{-1} = H$.

Conversely, assume $H \trianglelefteq G$. For $\sigma \in G$,
$E = \mathrm{Fix}(H) = \mathrm{Fix}(\sigma H \sigma^{-1}) = \sigma(E)$

So the restriction $\mathrm{Res}^K_E : G \to \mathrm{Aut}(E/F)$, $\sigma \mapsto \sigma|_E$ is a group hom.

i) $\ker \mathrm{Res}^K_E = \mathrm{Aut}(K/E) = H$

ii) Res^K_E is onto: Since K/E is Galois, i.e., the splitting field of some $g(x) \in E[x]$, every $\tau \in \mathrm{Aut}(E/F)$ can be extended to some $\sigma \in \mathrm{Aut}(K/F)$.

By Isomorphism Thm

$$\mathrm{Aut}(E/F) \cong G/H.$$

Since $[E:F] = \dfrac{|K:F|}{|K:E|} = \dfrac{|G|}{|H|} = |\mathrm{Aut}(E/F)|$,

E/F is Galois. $\square$

Ex K .. the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

zeros $Z = \{\alpha, i\alpha, -\alpha, -i\alpha\}$ for $\alpha = \sqrt[4]{2}$.

$K = \mathbb{Q}(Z) = \mathbb{Q}(\alpha, i)$ is Galois

For $G := \mathrm{Gal}(K/\mathbb{Q})$

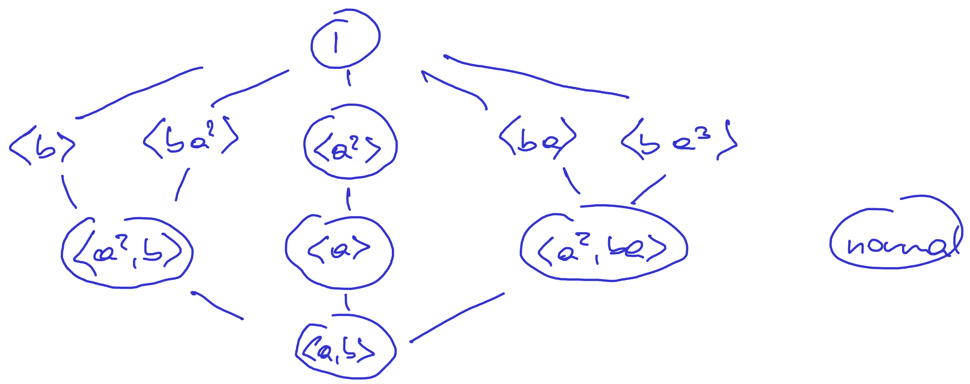
$$|G| = |K:\mathbb{Q}| = \underbrace{|K:\mathbb{Q}(i)|}_{=4} \cdot \underbrace{|\mathbb{Q}(i):\mathbb{Q}|}_{=2} = 8$$

Note: K has basis $1, \alpha, \alpha^2, \alpha^3$ over $\mathbb{Q}(i)$ since $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$.

G embeds into $S_Z \cong S_4$ because K is a splitting field.

Hence G is a Sylow 2-subgroup of S_4, i.e. isomorphic to the dihedral group

$$D_8 = \langle a, b \mid a^4 = 1,\ b^2 = 1,\ \underbrace{a^b}_{b^{-1}ab} = a^{-1} \rangle$$



Wlog choose $a(\alpha) = i\alpha$ $\quad b(\alpha) = \alpha$

$a(i) = i$ $\quad b(i) = -i$