

Section 12.1 part 1

12.1 The Galois Group

F a field $\underline{K \supseteq F}$ - field extension

Def $\text{Gal}_F K$ - the group of F -automorphisms of K .

$$\text{Gal}_F K = \{ \sigma: K \xrightarrow{\cong} K \mid \sigma(c) = c \text{ for every } c \in F \}$$

field isomorphism

$\sigma|_F = \text{identity}$

The group law (operation) is the composition of maps

Th 12.1 $\text{Gal}_F K$ is indeed a group

Th 12.2 Let $K \supseteq F$ be a field extension. Let $f \in F[x]$

Let $u \in K$ be a root of f : $f(u) = 0$

Let $\sigma \in \text{Gal}_F K$.

Then $f(\sigma(u)) = 0_F$.

Elements of $\text{Gal}_F K$
take roots of $f \in F[x]$
to roots of f .

Pf Let $f = c_0 + \dots + c_n x^n$.

$$\text{Then } c_0 + c_1 u + \dots + c_n u^n = 0_F \quad \} \quad f(u) = 0_F$$

$$\sigma(c_0 + c_1 u + \dots + c_n u^n) = \sigma(0_F)$$

$$\sigma(c_i) = c_i \text{ because } c_i \in F$$

$$c_0 + c_1 \sigma(u) + \dots + c_n \sigma(u)^n = 0_F$$

$$\begin{aligned} \sigma(c_i u^i) &= \sigma(c_i) \sigma(u^i) \\ &= c_i \sigma(u)^i \end{aligned}$$

$$f(\sigma(u)) = 0_F$$

Let $u \in K$ be a root of $f \in F[x]$

$v \in K$ _____

Is there $\sigma \in \text{Gal}_F K$ such that $\sigma(u) = v$?

Th 12.3 Let K be a splitting field of a polynomial over F .

Let $u, v \in K$.

There exists $\sigma \in \text{Gal}_F K$ such that $\sigma(u) = v$ if and only if $\begin{cases} u \text{ and } v \\ \text{have the same} \\ \text{minimal polynomial} \end{cases}$

Pf If there exists σ , then u and v have same min poly follows from Th 12.2

In Cor 1.8: $\sigma: F(u) \xrightarrow{\sim} F(v)$ $\sigma(u) = v$ simple extensions

$$\begin{array}{ccc} \sigma & & \\ \downarrow & & \downarrow \\ F & \xrightarrow{\text{id}} & F \end{array}$$

Being a splitting of $f \in F[x] \subset F(u)[x]$,

K is a splitting field of f over $F(u)$ or, similarly, $F(x)$

Th 11.14: (all splitting field of the same polynomial are isomorphic)

$\sigma(u) = v$

$$\begin{array}{ccc} K & \xrightarrow{\sim} & K \\ \downarrow & \sigma & \downarrow \\ U & & U \\ F(u) & \xrightarrow{\sim} & F(v) \\ \downarrow & \sigma & \downarrow \\ U & & U \\ F & \xrightarrow{\text{id}} & F \end{array}$$

σ (from Th 11.14) extends identity on F .

That means

$\sigma \in \text{Gal}_F K$

Th 12.4 Let $K = F(u_1, \dots, u_n)$ be an algebraic extension

Let $\sigma, \tau \in \text{Gal}_F K$

If $\sigma(u_i) = \tau(u_i)$ for $i = 1, \dots, n$

then $\sigma = \tau$.

Images of generators
determine an element
of Galois group uniquely

Pf Write $F(u_1, \dots, u_n) = F(u_1)(u_2) \dots (u_n)$ as a series of simple extensions

For a simple extension, by Th 11.7 (2), we have a basis

$F(u)$ $1, u, u^2, \dots, u^n$ - a basis for $F(u)$ over F $\left\{ \begin{array}{l} F(u) = F[x] / (f) \end{array} \right.$

$$v = c_0 + c_1 u + c_2 u^2 + \dots + c_n u^n \quad c_i \in F$$

$$\tau^{-1} \sigma(v) = v.$$

$$\begin{aligned} \tau^{-1} \sigma(u^2) &= \tau^{-1} \sigma(u) \cdot \tau^{-1} \sigma(u) \\ &= u \cdot u = u^2 \end{aligned}$$

Cor 12.5 Let K be a splitting field of a separable polynomial $f \in F[x]$.

Then $\text{Gal}_F K$ is isomorphic to a subgroup of S_n , where $n = \deg f$.

$$K = F(\text{roots of } f)$$

Now look at $F \subseteq E \subseteq K$

Intermediate fields
give us subgroups

Observe $\text{Gal}_E K \subseteq \text{Gal}_F K$ - a subgroup

Th 12.6 Let $K \supseteq F$ be a field extension

Let H be a subgroup of $\text{Gal}_F K$.

Let $E_H = \{k \in K \mid \sigma(k) = k \text{ for every } \sigma \in H\}$

Immediately:

$$F \subseteq E_H \subseteq K$$

as sets

Then E_H is an intermediate subfield

Terminology: E_H is the fixed field of H .

Pf To check: E_H is a subfield of K .

Let $c, d \in E_H$ $\sigma(c) = c$ $\sigma(d) = d$ for every $\sigma \in H$ imply $\sigma(c+d) = \sigma(c) + \sigma(d) = c+d$
for every $\sigma \in H$

...

We thus have got a correspondence between

Intermediate subfields



Subgroups of $\text{Gal}_F K$

$$F \subseteq E \subseteq K$$

Galois correspondence

Ex $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ (non-trivial $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$) extension

$\text{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \langle \iota \rangle$ "iota" trivial group; contains nothing but identity

Minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2 \in \mathbb{Q}[x]$

In $\mathbb{Q}(\sqrt[3]{2})$, we have $x^3 - 2 = (x - \sqrt[3]{2}) \underbrace{(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})}_{\text{irreducible in } \mathbb{Q}(\sqrt[3]{2})}$