Abstract Algebra III

This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat.

If $[K:F] = \#\mathrm{Aut}(K/F)$ then we say

K/F is Galois.

In that case we write $\mathrm{Aut}(K/F) = \mathrm{Gal}(K/F)$

the Galois gp of K/F.

"over"

This is a gp.

Today 2 directions of inquiry

① Computing the Galois gp

② Galois correspondence

① Computing the Galois gp

→ see Campuswire for an example

f irreducible in $F[x]$

$f(\alpha)=0$

$F(\alpha)=K$ iff every root of f is in $F(\alpha)$

(most of the time this doesn't happen)

$$\begin{tikzcd}[arrows=dash]
 & K \arrow[d] \\
F(\alpha) \arrow[r] & F
\end{tikzcd}$$

K splitting field of f

If so ($F(\alpha)=K$) elements of $Gal(K/F)$ are one for each root of f $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$

$\sigma_1(\alpha_1)=\alpha_1$, $\sigma_i(\alpha_1)=\alpha_i$

Suppose that $F(\alpha) \neq K$

$$\begin{tikzcd}[column sep=small] & & K \arrow[dll, dash, "\neq"'] \arrow[dl, dash] \\ F(\alpha) \arrow[r, dash] & F & \end{tikzcd}$$

To compute $\mathrm{Gal}(K/F)$ the principle is that everything possible does happen. It's up to you to figure out what is possible.

E.g. HW 8 #1 $F(\alpha) = K$ case Roots of f $\{\alpha, -\alpha, \beta, -\beta\}$

f irreducible
of deg 4
$f(x) \in \mathbb{Q}[x] = F[x]$

$\alpha\beta = 1$

$\beta = \frac{1}{\alpha}$

Restrictions on what is possible:

They are given by the relations between the roots i.e.

if $\beta = \frac{1}{\alpha}$ then $\sigma(\beta) = \frac{1}{\sigma(\alpha)}$

Another example: $\alpha\beta = \sqrt{d}$ $\quad d \in \mathbb{Z}$

This relationship must be respected by $Gal(K/F)$

$\sigma(\alpha\beta) = \underline{\sigma}(\sqrt{d})$

always sends an element to another root of its minimal polynomial

$$\sigma(\alpha\beta) = \begin{cases} \sqrt{d} \\ -\sqrt{d} \end{cases}$$

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$$

Tip: Know your small gps e.g. on Campuswire

know $\# Gal(K/F) = 4$

2 gps of size 4 $\quad C_4, \quad C_2 \times C_2 = V_4$

Recall that D_n is characterized (is the unique gp with) by having 2 elements one which we call r and one which we call s,

r has order n
s has order 2

$rsrs = 1$

If you can find such automorphisms

$$\langle r, s \rangle \leq \mathrm{Gal}(K/F)$$
$$\cong$$
$$D_n$$

get $=$ by comparing sizes

Two more important facts:

If $f \in F[x]$ and is irreducible with one root in K which is Galois over F (then all the roots of f are in K)

then $Gal(K/F)$ acts transitively on the roots of f.

• If $f \in F[x]$ irreducible of degree n
K splitting field of f over F

then $Gal(K/F)$ acts transitively on the roots $\{\alpha_1, \ldots, \alpha_n\}$ of f

the permutation representation gives an injective hom

$$Gal(K/F) \underset{\text{subgp}}{\hookrightarrow} S_n \quad \begin{matrix} A_n \\ C_n \end{matrix}$$

HW8 #1 $\{\alpha_1=\alpha,\ \alpha_2=-\alpha,\ \alpha_3=\beta,\ \alpha_4=-\beta\}$

$-\alpha \quad \beta=\frac{1}{\alpha} \quad -\beta=-\frac{1}{\alpha}$

$\sigma_1(\alpha)=\alpha$ ← identity

$\sigma_2(\overset{1}{\alpha})=\overset{3}{\beta}$ $\quad \sigma_2(\overset{3}{\beta})=\overset{1}{\alpha}$ $\quad \sigma_2(-\overset{2}{\alpha})=-\overset{4}{\beta}$ $\quad \sigma_2(-\beta)=-\alpha$

$\sigma_3(\alpha)=-\alpha \quad \sigma_3(-\alpha)=\alpha \quad \sigma_3(\beta)=-\beta \quad \sigma_3(-\beta)=\beta$

$\sigma_4(\alpha)=-\beta \quad \sigma_4(-\alpha)=\beta \quad \sigma_4(\beta)=-\alpha \quad \sigma_4(-\beta)=\alpha$

$\sigma_1=1$

$\sigma_4=(14)(23)$

$\sigma_2=(13)(24)$

$\sigma_3=(12)(34)$

$C_2\times C_2\leq S_4$

$$
\begin{tikzcd}
 & K=\mathbb{Q}(\sqrt[3]{2},\zeta) \arrow[dl, dash, "2"'] \arrow[dd, dash, "6"] \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & \\
 & \mathbb{Q}
\end{tikzcd}
$$

$$\left.\begin{aligned}\sigma_1(\sqrt[3]{2})&=\sqrt[3]{2}\\ \sigma_1(\zeta)&=\zeta\end{aligned}\right\}\ \text{identity}$$

$$\sigma_1(\zeta\sqrt[3]{2})=\zeta\sqrt[3]{2}$$

$$\left.\begin{aligned}\sigma_2(\sqrt[3]{2})&=\sqrt[3]{2}\\ \sigma_2(\zeta)&=\zeta^2\end{aligned}\right\}\ \sigma_2(\zeta\sqrt[3]{2})=\zeta^2\sqrt[3]{2}$$

$$\left.\begin{aligned}\sigma_3(\sqrt[3]{2})&=\zeta\sqrt[3]{2}\\ \sigma_3(\zeta)&=\zeta\end{aligned}\right\}$$

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

$$\sqrt[3]{2},\ \zeta\sqrt[3]{2},\ \zeta^2\sqrt[3]{2}$$

$\zeta=\dfrac{-1+i\sqrt{3}}{2}$ $\quad\zeta^2=\dfrac{-1-i\sqrt{3}}{2}$ $\leftarrow$ primitive 3rd roots of unity min poly ζ $x^2 - x + 1$

$$\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$$
$$\sigma_1(\zeta) = \zeta$$

$$\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}$$
$$\sigma_2(\zeta) = \zeta^2$$

$$\sigma_3(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$$
$$\sigma_3(\zeta) = \zeta$$

$$\sigma_4(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$$
$$\sigma_4(\zeta) = \zeta^2$$

$$\sigma_5(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$
$$\sigma_5(\zeta) = \zeta$$

$$\sigma_6(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$
$$\sigma_6(\sqrt[3]{2}) = \zeta^2$$

$$\mathrm{Gal}(K/\mathbb{Q}) \subseteq S_3$$

$$\left.\begin{aligned}\sigma_1(\sqrt[3]{2}) &= \sqrt[3]{2}\\ \sigma_1(\zeta) &= \zeta\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_2(\sqrt[3]{2}) &= \sqrt[3]{2}\\ \sigma_2(\zeta) &= \zeta^2\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_3(\sqrt[3]{2}) &= \zeta\sqrt[3]{2}\\ \sigma_3(\zeta) &= \zeta\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_4(\sqrt[3]{2}) &= \zeta\sqrt[3]{2}\\ \sigma_4(\zeta) &= \zeta^2\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_5(\sqrt[3]{2}) &= \zeta^2\sqrt[3]{2}\\ \sigma_5(\zeta) &= \zeta\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_6(\sqrt[3]{2}) &= \zeta^2\sqrt[3]{2}\\ \sigma_6(\sqrt[3]{2}) &= \zeta^2\end{aligned}\right\}$$

$$\mathrm{Gal}(K/\mathbb{Q}) \subseteq S_3$$

$$\alpha_1 = \sqrt[3]{2}$$
$$\alpha_2 = \zeta\sqrt[3]{2}$$
$$\alpha_3 = \zeta^2\sqrt[3]{2}$$

$$\sigma_1 = 1$$

$$\sigma_2(\zeta\sqrt[3]{2}) = \sigma_2(\zeta)\sigma_2(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$

$$\sigma_2 = (23)$$

$$\sigma_3(\zeta\sqrt[3]{2}) = \sigma_3(\zeta)\sigma_3(\sqrt[3]{2}) = \zeta\cdot\zeta\sqrt[3]{2} = \zeta^2\sqrt[3]{2}$$

$$\sigma_3 = (123)$$

$$\left.\begin{aligned}\sigma_1(\sqrt[3]{2}) &= \sqrt[3]{2}\\ \sigma_1(\zeta) &= \zeta\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_2(\sqrt[3]{2}) &= \sqrt[3]{2}\\ \sigma_2(\zeta) &= \zeta^2\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_3(\sqrt[3]{2}) &= \zeta\sqrt[3]{2}\\ \sigma_3(\zeta) &= \zeta\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_4(\sqrt[3]{2}) &= \zeta\sqrt[3]{2}\\ \sigma_4(\zeta) &= \zeta^2\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_5(\sqrt[3]{2}) &= \zeta^2\sqrt[3]{2}\\ \sigma_5(\zeta) &= \zeta\end{aligned}\right\}$$

$$\left.\begin{aligned}\sigma_6(\sqrt[3]{2}) &= \zeta^2\sqrt[3]{2}\\ \sigma_6(\sqrt[3]{2}) &= \zeta^2\end{aligned}\right\}$$

$$\mathrm{Gal}(K/\mathbb{Q}) \subseteq S_3$$

$$\sigma_4(\zeta\sqrt[3]{2}) = \zeta^2\zeta\sqrt[3]{2}$$
$$= \zeta^3\sqrt[3]{2} = \sqrt[3]{2}$$

$$\sigma_4 = (12)$$

$$\alpha_1 = \sqrt[3]{2}$$
$$\alpha_2 = \zeta\sqrt[3]{2}$$
$$\alpha_3 = \zeta^2\sqrt[3]{2}$$

Note: $C_3 \cong A_3$

$D_3 \cong S_3$

2 Galois correspondence

That’s all for today!