Galois Theory

Def: An <u>automorphism</u> of a ring R is a homomorphism $\varphi: R \to R$ which is bijective.

Ex: $\varphi: \mathbb{Q} \longrightarrow \mathbb{Q}$, $x \longmapsto x$ is an automorphism of $\mathbb{Q}$.

Ex: $\varphi: \mathbb{C} \longrightarrow \mathbb{C}$, $a+ib \longmapsto a-ib$ is an automorphism.

$$\varphi((a+ib)+(c+id)) \overset{?}{=} \varphi(a+ib)+\varphi(c+id)$$
$$\varphi(a+c+i(b+d)) \overset{?}{=} (a-ib)+(c-id)$$
$$a+c-i(b+d) = a+c-i(b+d) \checkmark$$
$$\varphi((a+ib)(c+id)) \overset{?}{=} \varphi(a+ib)\varphi(c+id)$$
$$\varphi(ac-bd+i(ad+bc)) \overset{?}{=} (a-ib)(c-id)$$
$$ac-bd-i(ad+bc) \overset{?}{=} ac-ibc-iad-bd \checkmark$$

$\varphi(\varphi(z)) = z$ so $\varphi = \varphi^{-1}$ $\therefore$ φ bijection.

Ex: $F = \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$\varphi: F \to F$, $\varphi(a+b\sqrt{2}) = a-b\sqrt{2}$ is a field automorphism.

Theorem: The set $\mathrm{Aut}(F)$ of all automorphisms of a field F is a group w/ binary operation is composition.

Ex: $F = \mathbb{Q}[\sqrt{2}]$, $\mathrm{Aut}(F) = ?$

$F = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

S'pose $\varphi: F \to F$ is an automorphism.

- $\varphi(1) = 1$
- $\varphi(\sqrt{2}) = u + v\sqrt{2}$ where $u, v \in \mathbb{Q}$.

Any conditions on u, v?

$$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1+1 = 2$$

$$\varphi(2) = \varphi(\sqrt{2}\cdot\sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2})$$

$$2 = (u+v\sqrt{2})(u+v\sqrt{2})$$

$$2 = u^2 + 2v^2 + 2uv\sqrt{2}$$

David: $u = 0$ or $v = 0$

$v = 0$: $2 = u^2 \Rightarrow \sqrt{2} = u \Rightarrow\Leftarrow$

$u = 0$:

$2 = 2v^2$

$1 = v^2$

$\pm 1 = v$

$$\varphi(\sqrt{2}) = \sqrt{2} \quad \text{or} \quad \varphi(\sqrt{2}) = -\sqrt{2}$$

$$\varphi(m + n\sqrt{2}) = \varphi(m) + \varphi(n)\varphi(\sqrt{2}) \qquad m, n \in \mathbb{Z}$$

$$= m + n\,\varphi(\sqrt{2})$$

$$\varphi\left(\frac{a_1}{a_2} + \frac{b_1}{b_2}\sqrt{2}\right) = \varphi\left(\frac{a_1}{a_2}\right) + \varphi\left(\frac{b_1}{b_2}\right)\varphi(\sqrt{2})$$

$$= \frac{\varphi(a_1)}{\varphi(a_2)} + \frac{\varphi(b_1)}{\varphi(b_2)}\varphi(\sqrt{2})$$

$$= \frac{a_1}{a_2} + \frac{b_1}{b_2}\varphi(\sqrt{2})$$

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2}]) = \{\mathrm{id},\ \varphi: a+b\sqrt{2} \to a-b\sqrt{2}\}$$

conjugation automorphism

Ex: $\mathrm{Aut}(\mathbb{Q}) = ?$

$$\varphi(n) = \varphi(\overbrace{1+1+1+\dots+1}^{n \text{ times}})$$
$$= \varphi(1)+\varphi(1)+\varphi(1)+\dots+\varphi(1) = n\varphi(1) = n.$$

$$\varphi\left(\frac{m}{n}\right) = \frac{\varphi(m)}{\varphi(n)} = \frac{m}{n}$$

every element looks like this!

$\varphi = id$

$\mathrm{Aut}(\mathbb{Q}) = \{id\}.$

<u>Ex</u>: $F = \mathbb{Q}[\sqrt{2},\sqrt{3}] = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}$

$\mathrm{Aut}(F) = ?$ $\varphi \in \mathrm{Aut}(F)$, then

$\varphi(\sqrt{2}) = ?$, $\varphi(\sqrt{3}) = ?$, $\varphi(\sqrt{6}) = ?$

$\varphi(\sqrt{2}) = \pm\sqrt{2}$, $\varphi(\sqrt{3}) = \pm\sqrt{3}$

$\varphi(\sqrt{6}) = \varphi(\sqrt{2})\varphi(\sqrt{3})$ determined by previous!

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2},\sqrt{3}]) = \begin{cases} \varphi_0 : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \to a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \\ \varphi_1 : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \to a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6} \\ \varphi_2 : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \to a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6} \\ \varphi_3 : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \to a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6} \end{cases}$$

Group w/ 4 elements + no elements of order 4

$\therefore \mathbb{Z}_2 \times \mathbb{Z}_2$

$\varphi_k \circ \varphi_k = \varphi_0 \Rightarrow \mathrm{ord}(\varphi_k) = 2$

Remember:

G group, $g \in G$ has order $k \Rightarrow g^k = e$ and $g^j \neq e$ for $0<j<k$.

Some fields have **tons** of automorphisms! $\mathbb{R}$, $\mathbb{C}$

Main idea of Galois theory: study fields by studying their automorphisms!

Def: Let $S \subseteq \mathrm{Aut}(F)$. An element $a \in F$ is *fixed* by S if $\varphi(a) = a \ \forall \varphi \in S$.

Prop: Given $S \subseteq \mathrm{Aut}(F)$, the set of all elements of F which are fixed by S is a subfield of F.

Proof: Let $L = \{a \in F \mid \varphi(a) = a \ \forall \varphi \in S\}$

$\varphi(0) = 0$ so $0 \in L$.

If $a, b \in L$, then $\left.\begin{array}{l}\varphi(a) = a \ \forall \varphi \in S \\ \varphi(b) = b \ \forall \varphi \in S\end{array}\right\}$ $\varphi(a+b) = \varphi(a) + \varphi(b) = a + b$

$\therefore a + b \in L$

Likewise $-a \in L$, so L is a subgroup of F.

Also $ab \in L$, so L is a subring

$\varphi(a^{-1}) = \varphi(a)^{-1} \Rightarrow a^{-1} \in L$ so L is a subfield $\square$

Ex: $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ subfield fixed by $\varphi_2 : \begin{array}{l}\sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{2} \mapsto \sqrt{2}\end{array}$

is $\mathbb{Q}[\sqrt{2}]$

subfield fixed by $\varphi_1 : \begin{array}{l}\sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3}\end{array}$

is $\mathbb{Q}[\sqrt{3}]$

The subfield fixed by **everything** in $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}, \sqrt{3}])$ is $\mathbb{Q}$

Picture of invariant subfields!

$$\begin{tikzcd}
 & \mathbb{Q}[\sqrt{2}, \sqrt{3}] \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}[\sqrt{2}] \arrow[dr, dash] & & \mathbb{Q}[\sqrt{3}] \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

__Def__: Let $F \subseteq E$ be a field extension. The set

$$G(E/F) = \{\varphi \in \mathrm{Aut}(E) \mid \varphi(a) = a \ \forall\, a \in F\}$$

is called the __Galois group__ of E over F.

__Special case__: $G(E/\mathbb{Q}) = \mathrm{Aut}(E)$

__Example__: $\mathbb{R} \subseteq \mathbb{C}$ $\qquad G(\mathbb{C}/\mathbb{R}) = ?$

$\mathrm{Aut}(\mathbb{C}) \leftarrow$ scary big!!

$$\begin{aligned} \varphi(a+ib) &= \varphi(a) + \varphi(i)\varphi(b) \\ &= a + \varphi(i)b \end{aligned}$$

$\varphi(i) = \pm i \implies G(\mathbb{C}/\mathbb{R}) = \{\text{id, complex conj}\}$

__Ex__: $F = \mathbb{Q}[\sqrt{2}]$ $\qquad E = \mathbb{Q}[\sqrt{1+\sqrt{2}}]$

$F \subseteq E$

$$\left(\sqrt{1+\sqrt{2}}\right)^2 - 1 = (1+\sqrt{2}) - 1 = \sqrt{2}$$

Since $\mathbb{Q} \subseteq E$ and $\sqrt{2} \in E$, $\mathbb{Q}[\sqrt{2}] \subseteq E$.

$G(E/F) = ?$

To calculate this, lets see what E, F look like!

$F = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$E = \mathbb{Q}[\sqrt{1+\sqrt{2}}] = \text{span}\{1, \sqrt{1+\sqrt{2}}, 1+\sqrt{2}, (1+\sqrt{2})^{3/2}\}$

min poly is $(x^2-1)^2 - 2$, deg 4

$E = \{a + b\underline{\sqrt{1+\sqrt{2}}} + c\underline{\sqrt{2}} + d\underline{(1+\sqrt{2})^{3/2}} \mid a,b,c,d \in \mathbb{Q}\}$

$\varphi \in G(E/F)$.

$\varphi(\sqrt{2}) = \sqrt{2}$ $\quad \varphi((1+\sqrt{2})^{3/2}) = \varphi((1+\sqrt{2})^{1/2}(1+\sqrt{2}))$
$= \varphi((1+\sqrt{2})^{1/2})(1+\sqrt{2})$

φ is determined by where we send $\sqrt{1+\sqrt{2}}$

$\underline{1+\sqrt{2}} = \varphi(1+\sqrt{2}) = \varphi((\sqrt{1+\sqrt{2}})^2) = \underline{(\varphi(\sqrt{1+\sqrt{2}}))^2}$

$\varphi(\sqrt{1+\sqrt{2}}) = \pm\sqrt{1+\sqrt{2}}$

$Gal(E/F) = \{id, \varphi : \sqrt{1+\sqrt{2}} \mapsto -\sqrt{1+\sqrt{2}}\}$

$Gal(E/\mathbb{Q})$ in comparison has 4 elements!