# Lecture 6.5: Galois group actions and normal field extensions

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

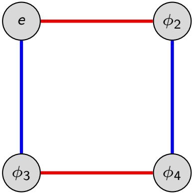
# The Galois group of $x^4 - 5x^2 + 6$ acting on its roots

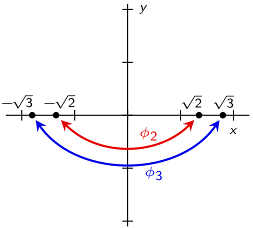
Recall the 4 automorphisms of $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the splitting field of $x^4 - 5x^2 + 6$:

$$\begin{aligned}
e\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\
\phi_2\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\
\phi_3\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
\phi_4\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\end{aligned}$$

They form the Galois group of $x^4 - 5x^2 + 6$. The multiplication table and Cayley diagram are shown below.

| | $e$ | $\phi_2$ | $\phi_3$ | $\phi_4$ |
|---|---|---|---|---|
| $e$ | $e$ | $\phi_2$ | $\phi_3$ | $\phi_4$ |
| $\phi_2$ | $\phi_2$ | $e$ | $\phi_4$ | $\phi_3$ |
| $\phi_3$ | $\phi_3$ | $\phi_4$ | $e$ | $\phi_2$ |
| $\phi_4$ | $\phi_4$ | $\phi_3$ | $\phi_2$ | $e$ |




**Key point**

There is a group action of $\mathrm{Gal}(f(x))$ on the set of roots $S = \{\pm\sqrt{2}, \pm\sqrt{3}\}$ of $f(x)$.

# The Galois group acts on the roots

**Theorem**

If $f \in \mathbb{Z}[x]$ is a polynomial with a root in a field extension $F$ of $\mathbb{Q}$, then any automorphism of $F$ permutes the roots of $f$.

Said differently, we have a group action of $\text{Gal}(f(x))$ on the set $S = \{r_1, \dots, r_n\}$ of roots of $f(x)$.

That is, we have a homomorphism

$$\psi\colon\ \text{Gal}(f(x)) \longrightarrow \text{Perm}(\{r_1, \dots, r_n\})\,.$$

If $\phi \in \text{Gal}(f(x))$, then $\psi(\phi)$ is a permutation of the roots of $f(x)$.

This permutation is what results by "pressing the $\phi$-button" – it permutes the roots of $f(x)$ via the automorphism $\phi$ of the splitting field of $f(x)$.

**Corollary**

If the degree of $f \in \mathbb{Z}[x]$ is $n$, then the Galois group of $f$ is a subgroup of $S_n$.

# The Galois group acts on the roots

The next results says that "$\mathbb{Q}$ can't tell apart the roots of an irreducible polynomial."

### The "One orbit theorem"

Let $r_1$ and $r_2$ be roots of an irreducible polynomial over $\mathbb{Q}$. Then

(a) There is an isomorphism $\phi\colon \mathbb{Q}(r_1) \longrightarrow \mathbb{Q}(r_2)$ that fixes $\mathbb{Q}$ and with $\phi(r_1) = r_2$.

(b) This remains true when $\mathbb{Q}$ is replaced with any extension field $F$, where $\mathbb{Q} \subset F \subset \mathbb{C}$.

### Corollary

If $f(x)$ is irreducible over $\mathbb{Q}$, then for any two roots $r_1$ and $r_2$ of $f(x)$, the Galois group $\mathrm{Gal}(f(x))$ contains an automorphism $\phi\colon r_1 \longmapsto r_2$.

In other words, if $f(x)$ is irreducible, then the action of $\mathrm{Gal}(f(x))$ on the set $S = \{r_1, \dots, r_n\}$ of roots has only one orbit.

# Normal field extensions

**Definition**

An extension field $E$ of $F$ is normal if it is the splitting field of some polynomial $f(x)$.

If $E$ is a normal extension over $F$, then every irreducible polynomial in $F[x]$ that has a root in $E$ splits over $F$.

Thus, if you can find an irreducible polynomial that has one root, but not all of its roots in $E$, then $E$ is *not* a normal extension.

**Normal extension theorem**

The degree of a normal extension is the order of its Galois group.

**Corollary**

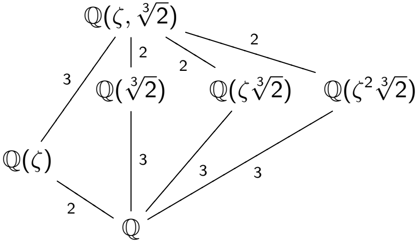
The order of the Galois group of a polynomial $f(x)$ is the degree of the extension of its splitting field over $\mathbb{Q}$.

# Normal field extensions: Examples

Consider $\mathbb{Q}(\zeta, \sqrt[3]{2}) = \mathbb{Q}(\alpha)$, the splitting field of $f(x) = x^3 - 2$.

It is also the splitting field of $m(x) = x^6 + 108$, the minimal polynomial of $\alpha = \sqrt[3]{2}\sqrt{-3}$.

Let's see which of its intermediate subfields are normal extensions of $\mathbb{Q}$.




- $\mathbb{Q}$: Trivially normal.
- $\mathbb{Q}(\zeta)$: Splitting field of $x^2 + x + 1$; roots are $\zeta, \zeta^2 \in \mathbb{Q}(\zeta)$. Normal.
- $\mathbb{Q}(\sqrt[3]{2})$: Contains only one root of $x^3 - 2$, not the other two. Not normal.
- $\mathbb{Q}(\zeta\sqrt[3]{2})$: Contains only one root of $x^3 - 2$, not the other two. Not normal.
- $\mathbb{Q}(\zeta^2\sqrt[3]{2})$: Contains only one root of $x^3 - 2$, not the other two. Not normal.
- $\mathbb{Q}(\zeta, \sqrt[3]{2})$: Splitting field of $x^3 - 2$. Normal.

By the normal extension theorem,

$$|\operatorname{Gal}(\mathbb{Q}(\zeta))| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2, \qquad |\operatorname{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))| = [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 6.$$

Moreover, you can check that $|\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}))| = 1 < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

# The Galois group of $x^3 - 2$

We can now conclusively determine the Galois group of $x^3 - 2$.

By definition, the Galois group of a polynomial is the Galois group of its splitting field, so $\text{Gal}(x^3 - 2) = \text{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))$.

By the normal extension theorem, the order of the Galois group of $f(x)$ is the degree of the extension of its splitting field:

$$|\,\text{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))| = [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 6\,.$$

Since the Galois group acts on the roots of $x^3 - 2$, it must be a subgroup of $S_3 \cong D_3$.

There is only one subgroup of $S_3$ of order 6, so $\text{Gal}(x^3 - 2) \cong S_3$. Here is the action diagram of $\text{Gal}(x^3 - 2)$ acting on the set $S = \{r_1, r_2, r_3\}$ of roots of $x^3 - 2$:

$$\begin{cases} r\colon \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2} \\ r\colon \zeta \longmapsto \zeta \end{cases}$$

$$\begin{cases} f\colon \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ f\colon \zeta \longmapsto \zeta^2 \end{cases}$$