Lecture 6.4: Galois groups

Matthew Macauley

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

Math 4120, Modern Algebra
The Galois group of a polynomial

**Definition**

Let $f \in \mathbb{Z}[x]$ be a polynomial, with roots $r_1, \ldots, r_n$. The **splitting field** of $f$ is the field $\mathbb{Q}(r_1, \ldots, r_n)$.

The splitting field $F$ of $f(x)$ has several equivalent characterizations:

- the smallest field that contains all of the roots of $f(x)$;
- the smallest field in which $f(x)$ **splits** into linear factors:

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n) \in F[x].$$

Recall that the **Galois group** of an extension $F \supseteq \mathbb{Q}$ is the group of automorphisms of $F$, denoted $\text{Gal}(F)$.

**Definition**

The **Galois group** of a polynomial $f(x)$ is the Galois group of its splitting field, denoted $\text{Gal}(f(x))$. 

M. Macauley (Clemson) Lecture 6.4: Galois groups Math 4120, Modern Algebra 2 / 7
A few examples of Galois groups

- The polynomial $x^2 - 2$ splits in $\mathbb{Q}(\sqrt{2})$, so
  $$\text{Gal}(x^2 - 2) = \text{Gal}(\mathbb{Q}(\sqrt{2})) \cong C_2.$$ 

- The polynomial $x^2 + 1$ splits in $\mathbb{Q}(i)$, so
  $$\text{Gal}(x^2 + 1) = \text{Gal}(\mathbb{Q}(i)) \cong C_2.$$ 

- The polynomial $x^2 + x + 1$ splits in $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/3}$, so
  $$\text{Gal}(x^2 + x + 1) = \text{Gal}(\mathbb{Q}(\zeta)) \cong C_2.$$ 

- The polynomial $x^3 - 1 = (x - 1)(x^2 + x + 1)$ also splits in $\mathbb{Q}(\zeta)$, so
  $$\text{Gal}(x^3 - 1) = \text{Gal}(\mathbb{Q}(\zeta)) \cong C_2.$$ 

- The polynomial $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$ splits in $\mathbb{Q}(\sqrt{2}, i)$, so
  $$\text{Gal}(x^4 - x^2 - 2) = \text{Gal}(\mathbb{Q}(\sqrt{2}, i)) \cong V_4.$$ 

- The polynomial $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ splits in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so
  $$\text{Gal}(x^4 - 5x^2 + 6) = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong V_4.$$ 

- The polynomial $x^3 - 2$ splits in $\mathbb{Q}(\zeta, \sqrt[3]{2})$, so
  $$\text{Gal}(x^3 - 2) = \text{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2})) \cong D_3.$$ 

The tower law of field extensions

Recall that if we had a chain of subgroups $K \leq H \leq G$, then the index satisfies a tower law: $[G : K] = [G : H][H : K]$.

Not surprisingly, the degree of field extensions obeys a similar tower law:

**Theorem (Tower law)**

For any chain of field extensions, $F \subset E \subset K$,

$$[K : F] = [K : E][E : F].$$

We have already observed this in our subfield lattices:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]}_{\text{min. poly: } x^2 - 3} \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{\text{min. poly: } x^2 - 2} = 2 \cdot 2 = 4.$$

Here is another example:

$$[\mathbb{Q}(\zeta, \sqrt{3}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\zeta, \sqrt{2}) : \mathbb{Q}(\sqrt{2})]}_{\text{min. poly: } x^2 + x + 1} \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{\text{min. poly: } x^3 - 2} = 2 \cdot 3 = 6.$$
Primitive elements

Primitive element theorem

If $F$ is an extension of $\mathbb{Q}$ with $[F : \mathbb{Q}] < \infty$, then $F$ has a primitive element: some $\alpha \not\in \mathbb{Q}$ for which $F = \mathbb{Q}(\alpha)$.

How do we find a primitive element $\alpha$ of $F = \mathbb{Q}(\zeta, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$?

Let’s try $\alpha = i\sqrt{3}\sqrt[3]{2} \in F$. Clearly, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 6$. Observe that

$$\alpha^2 = -3\sqrt[3]{4}, \quad \alpha^3 = -6i\sqrt{3}, \quad \alpha^4 = -18\sqrt[3]{2}, \quad \alpha^5 = 18i\sqrt[3]{4}\sqrt{3}, \quad \alpha^6 = -108.$$  

Thus, $\alpha$ is a root of $x^6 + 108$. The following are equivalent (why?):

(i) $\alpha$ is a primitive element of $F$;
(ii) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$;
(iii) the minimal polynomial $m(x)$ of $\alpha$ has degree 6;
(iv) $x^6 + 108$ is irreducible (and hence must be $m(x)$).

In fact, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ holds because both 2 and 3 divide $[\mathbb{Q}(\alpha) : \mathbb{Q}]$:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(i\sqrt{3})][\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}], \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$
An example: The Galois group of $x^4 - 5x^2 + 6$

The polynomial $f(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$ has splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

We already know that its Galois group should be $V_4$. Let’s compute it explicitly; this will help us understand it better.

We need to determine all automorphisms $\phi$ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We know:

- $\phi$ is determined by where it sends the basis elements $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
- $\phi$ must fix 1.
- If we know where $\phi$ sends two of $\{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$, then we know where it sends the third, because
  \[
  \phi(\sqrt{6}) = \phi(\sqrt{2}\sqrt{3}) = \phi(\sqrt{2}) \phi(\sqrt{3}).
  \]

In addition to the identity automorphism $e$, we have

\[
\begin{align*}
\phi_2(\sqrt{2}) &= -\sqrt{2} & \phi_3(\sqrt{2}) &= \sqrt{2} & \phi_4(\sqrt{2}) &= -\sqrt{2} \\
\phi_2(\sqrt{3}) &= \sqrt{3} & \phi_3(\sqrt{3}) &= -\sqrt{3} & \phi_4(\sqrt{3}) &= -\sqrt{3}
\end{align*}
\]

Question

What goes wrong if we try to make $\phi(\sqrt{2}) = \sqrt{3}$?
An example: The Galois group of $x^4 - 5x^2 + 6$

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

- $e: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$
- $\phi_2: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$
- $\phi_3: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$
- $\phi_4: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$

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

Exercise

Show that $\alpha = \sqrt{2} + \sqrt{3}$ is a primitive element of $F$, i.e., $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. 

M. Macauley (Clemson)