Lecture 6.2: Field automorphisms

Matthew Macauley

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

Math 4120, Modern Algebra

Field automorphisms

Recall that an automorphism of a group G was an isomorphism $\phi\colon G \to G$.

Definition

Let F be a field. A field automorphism of F is a bijection $\phi\colon F \to F$ such that for all $a, b \in F$,

$$\phi(a+b) = \phi(a) + \phi(b) \qquad \text{and} \qquad \phi(ab) = \phi(a)\,\phi(b)\,.$$

In other words, ϕ must preserve the structure of the field.

For example, let $F = \mathbb{Q}(\sqrt{2})$. Verify (HW) that the function

$$\phi\colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})\,, \qquad \phi\colon a + b\sqrt{2} \longmapsto a - b\sqrt{2}\,.$$

is an automorphism. That is, show that

- $\phi((a+b\sqrt{2}) + (c+d\sqrt{2})) = \cdots = \phi(a+b\sqrt{2}) + \phi(c+d\sqrt{2})$
- $\phi((a+b\sqrt{2})(c+d\sqrt{2})) = \cdots = \phi(a+b\sqrt{2})\,\phi(c+d\sqrt{2})$.

What other field automorphisms of $\mathbb{Q}(\sqrt{2})$ are there?

A defining property of field automorphisms

Field automorphisms are central to Galois theory! We'll see why shortly.

Proposition

If ϕ is an automorphism of an extension field F of $\mathbb{Q}$, then

$$\phi(q) = q \qquad \text{for all } q \in \mathbb{Q}.$$

Proof

Suppose that $\phi(1) = q$. Clearly, $q \neq 0$. (Why?) Observe that

$$q = \phi(1) = \phi(1 \cdot 1) = \phi(1)\,\phi(1) = q^2\,.$$

Similarly,

$$q = \phi(1) = \phi(1 \cdot 1 \cdot 1) = \phi(1)\,\phi(1)\,\phi(1) = q^3\,.$$

And so on. It follows that $q^n = q$ for every $n \geq 1$. Thus, $q = 1$. □

Corollary

$\sqrt{2}$ is irrational. □

The Galois group of a field extension

The set of all automorphisms of a field forms a group under composition.

Definition

Let F be an extension field of $\mathbb{Q}$. The Galois group of F is the group of automorphisms of F, denoted $\mathrm{Gal}(F)$.

Here are some examples (without proof):

- The Galois group of $\mathbb{Q}(\sqrt{2})$ is C_2:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})) = \langle f \rangle \cong C_2\,, \qquad \text{where } f\colon \sqrt{2} \longmapsto -\sqrt{2}$$

- An automorphism of $F = \mathbb{Q}(\sqrt{2}, i)$ is completely determined by where it sends $\sqrt{2}$ and i. There are four possibilities: the identity map e, and

$$\begin{cases} h(\sqrt{2}) = -\sqrt{2} \\ h(i) = i \end{cases} \qquad \begin{cases} v(\sqrt{2}) = \sqrt{2} \\ v(i) = -i \end{cases} \qquad \begin{cases} r(\sqrt{2}) = -\sqrt{2} \\ r(i) = -i \end{cases}$$

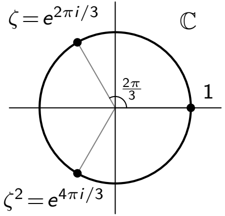
Thus, the Galois group of F is $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)) = \langle h, v \rangle \cong V_4$.

$\mathbb{Q}(\zeta, \sqrt[3]{2})$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains all roots of $g(x) = x^3 - 2$?

Let $\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. This is a 3rd root of unity; the roots of $x^3 - 1 = (x-1)(x^2+x+1)$ are $1, \zeta, \zeta^2$.



Note that the roots of $g(x)$ are

$$z_1 = \sqrt[3]{2}\,, \qquad z_2 = \zeta\sqrt[3]{2}\,, \qquad z_3 = \zeta^2\sqrt[3]{2}\,.$$

Thus, the field we seek is $F = \mathbb{Q}(z_1, z_2, z_3)$.

I claim that $F = \mathbb{Q}(\zeta, \sqrt[3]{2})$. Note that this field contains z_1, z_2, and z_3. Conversely, we can construct ζ and $\sqrt[3]{2}$ from z_1 and z_2, using arithmetic.

A little algebra can show that

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} : a, b, c, d, e, f \in \mathbb{Q}\}\,.$$

Since $\zeta = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ lies in $\mathbb{Q}(\zeta, \sqrt[3]{2})$, so does $2(\zeta - \frac{1}{2}) = \sqrt{3}i = \sqrt{-3}$. Thus,

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{3}i, \sqrt[3]{2})\,.$$

Subfields of $\mathbb{Q}(\zeta, \sqrt[3]{2})$

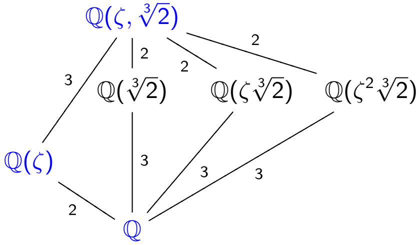
What are the subfields of

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} : a, b, c, d, e, f \in \mathbb{Q}\}\,?$$

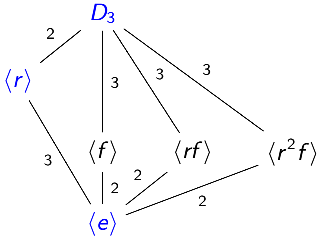
Note that $(\zeta^2)^2 = \zeta^4 = \zeta$, and so $\mathbb{Q}(\zeta^2) = \mathbb{Q}(\zeta) = \{a + b\zeta : a, b \in \mathbb{Q}\}$.

Similarly, $(\sqrt[3]{4})^2 = 2\sqrt[3]{2}$, and so $\mathbb{Q}(\sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.

There are two more subfields. As we did before, we can arrange them in a lattice:



Look familiar?



Compare this to the subgroup lattice of D_3.

Summary so far

Roughly speaking, a field is a group under both addition and multiplication (if we exclude 0), with the distributive law connecting these two operations.

We are mostly interested in the field $\mathbb{Q}$, and certain extension fields: $F \supseteq \mathbb{Q}$. Some of the extension fields we've encountered:

$$\mathbb{Q}(\sqrt{2}), \qquad \mathbb{Q}(i), \qquad \mathbb{Q}(\sqrt{2}, i), \qquad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \qquad \mathbb{Q}(\zeta, \sqrt[3]{2}).$$

An automorphism of a field $F \supset \mathbb{Q}$ is a structure-preserving map that fixes $\mathbb{Q}$.

The set of all automorphisms of $F \supseteq \mathbb{Q}$ forms a group, called the Galois group of F, denoted $\mathrm{Gal}(F)$.

There is an intriguing but mysterious connection between subfields of F and subgroups of $\mathrm{Gal}(F)$. This is at the heart of Galois theory!

Something to ponder

How does this all relate to solving polynomials with radicals?