MA542 Lecture

Timothy Kohl

Boston University

March 26, 2025

Corollary

Let E be an extension field of F then the set of all elements of E which are algebraic over F is a subfield of E which we call the algebraic closure of F in E.

Of particular interest in number theory is the case where $F = \mathbb{Q}$ and $E = \mathbb{C}$ and we have

$$\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$$

which contains the roots of all polynomials in $\mathbb{Q}[x]$ due to the following fact.

The Fundamental Theorem of Algebra
Every polynomial $p(x) \in \mathbb{C}[x]$ has roots in $\mathbb{C}$.

That is, all polynomials in $\mathbb{C}[x]$ are reducible.

i.e. $\mathbb{C}$ is its own algebraic closure

What's kind of ironic about this theorem is that it is not proved using algebra!

i.e. Most proofs are analytic/topological in nature.

(If you've had some complex analysis, this is a consequence of Liouville's Theorem.)

Galois Theory

The key point of Galois theory is to understand the theory of field extensions via group theory, in particular via groups of **field automorphisms**.

We shall give the definition of these presently, but the power of this analysis is that can address questions of the solvability of equations in terms of a group which can, basically, be assigned to the equation, and whose properties correlate with the solvability of the equation.

Moreover, these groups reveal fundamental properties of the field extensions in and of themselves.

Before considering fields, let's observe some basic facts about homomorphisms and isomorphisms.

Proposition

If R, S, T are rings and $\phi : R \to S$ is a ring homomorphism, and $\psi : S \to T$ is a ring homomorphism, then $\psi \circ \phi : R \to T$ given $\psi \circ \phi(r) = \psi(\phi(r))$ is a ring homomorphism.
Moreover, if ϕ and ψ are isomorphisms, then so is $\psi \circ \phi$.

PROOF (sketch) We note that
$\psi(\phi(r_1 + r_2)) = \psi(\phi(r_1) + \phi(r_2)) = \psi(\phi(r_1)) + \psi(\phi(r_2))$ since ϕ and ψ are (individually) homomorphisms.
The same argument works for $\psi(\phi(r_1 \cdot r_2))$.

Lastly, we recall the (basic) fact that the composition of two bijections is a bijection. □

Also, if $\phi : R \to R$ is an isomorphism of R with itself, we call ϕ an automorphism.

The lead-in to this analysis is the contrast between extensions like

$$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$$

where the adjunction of one of the roots $\sqrt{2}$ yields a field which contains both (i.e. all) roots of $x^2 - 2 \in \mathbb{Q}[x]$, whereas in contrast, the field

$$\mathbb{Q}(\sqrt[3]{2})$$

contains only one of the roots of $x^3 - 2 \in \mathbb{Q}[x]$, i.e. one is the splitting field, the other is not.

If $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ is an isomorphism (of rings/fields) then one must have that $\phi(1) = 1$ since ϕ is one-to-one and onto its image, which is $\mathbb{Q}(\sqrt{2})$.

But this also means that $\phi(n) = n$ for any $n \in \mathbb{Z}$ and therefore, for any $r = \frac{m}{n} \in \mathbb{Q}$, $\phi(r) = r$.

So that this implies is that if $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ is an isomorphism, then

$$\phi(a + b\sqrt{2}) = \phi(a) + \phi(b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b\phi(\sqrt{2})$$

and so ϕ is determined by $\phi(\sqrt{2})$.

The possibilities for $\phi(\sqrt{2})$ are keyed to the equation $\sqrt{2}$ satisfies, in particular $\phi((\sqrt{2})^2) = (\phi(\sqrt{2}))^2$ which means $(\phi(\sqrt{2}))^2 = 2$ so $\phi(\sqrt{2}) = \pm\sqrt{2}$ are the only possibilities.

As such we write $Aut(\mathbb{Q}(\sqrt{2})) = \{\sigma, I\}$ namely a set with two functions (i.e. automorphisms of $\mathbb{Q}(\sqrt{2})$), σ, and I which is determined by $I(\sqrt{2}) = \sqrt{2}$ and so $I(a + b\sqrt{2}) = a + b\sqrt{2}$, that is the literal identity function.

The other is $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ determined by $\sigma(\sqrt{2}) = -\sqrt{2}$ and thus $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$.

The set $Aut(\mathbb{Q}(\sqrt{2})) = \{I, \sigma\}$ is actually a group since bijections can be composed and one can show that the composition of two homomorphisms (isomorphisms) is a homomorphism (isomorphism), and indeed we note that

$$\begin{aligned}\sigma(\sigma(a + b\sqrt{2})) &= \sigma(a - b\sqrt{2}) \\ &= \sigma(a) - \sigma(b\sqrt{2}) \\ &= \sigma(a) - \sigma(b)\sigma(\sqrt{2}) \\ &= a - b(-\sqrt{2}) = a + b\sqrt{2}\end{aligned}$$

which implies that $\sigma \circ \sigma = I$, and one may check the obvious facts that $\sigma \circ I = \sigma$ and $I \circ \sigma = \sigma$.

This implies that $Aut(\mathbb{Q}(\sqrt{2}))$ is a group, of order 2.

Again, we emphasize that the number of 'choices' for $\phi(\sqrt{2})$ is precisely determined by the number of distinct root of $x^2 - 2$ *in* $\mathbb{Q}(\sqrt{2})$.

We also observe that $|Aut(\mathbb{Q}(\sqrt{2}))| = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. (More on this later.)

For a contrasting example, let's examine $Aut(\mathbb{Q}(\sqrt[3]{2}))$.

Again, if $\phi \in Aut(\mathbb{Q}(\sqrt[3]{2}))$ then $\phi(r) = r$ for any $r \in \mathbb{Q}$ and so for a typical element $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ we have

$$\phi(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + b\phi(\sqrt[3]{2}) + c\phi(\sqrt[3]{2}^2) = a + b\phi(\sqrt[3]{2}) + c\phi(\sqrt[3]{2})^2$$

where $\phi(\sqrt[3]{2})$ must be a(nother) root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$.

However, here we run into the key difference, there *are no other* roots of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$ and so $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$ only, and so ϕ must be the identity!

As such $Aut(\mathbb{Q}(\sqrt[3]{2})) = \{I\}$, namely it is a trivial group, and certainly $|Aut(\mathbb{Q}(\sqrt[3]{2}))| < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ which is not an accident.

Before going further, let's present some defintions:

Definition

Let E be an extension field of F. An automorphism of E is a ring isomorphism from E to itself.

The Galois Group of a E over F, denoted $Gal(E/F)$ is the set of automorphisms $\phi : E \to E$ such that for $c \in F$, one has $\phi(c) = c$.

Also, if $H \leq Gal(E/F)$ is a subgroup, the fixed field is the set $E_H = \{x \in E \mid \phi(x) = x \text{ for all } \phi \in H\}$.

So we've seen so far that $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma, I\}$ and $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{I\}$.

Important: When $F = \mathbb{Q}$, and E is an extension field of $F = \mathbb{Q}$ then *every* automorphism $\phi : E \to E$ will fix the elements of $F = \mathbb{Q}$ automatically. (as we saw in the $\mathbb{Q}(\sqrt{2})$ example earlier)

However, for general extensions E/F, one must restrict to those automorphisms which fix F.

Also, for some extensions E/F the group fixes *more* than just the elements of F, e.g. $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ fixes *all* of $\mathbb{Q}(\sqrt[3]{2})$.

We'll talk about the fixed field of a subgroup $H \leq Gal(E/F)$ next time, but there is one thing to point out.

We call $Gal(E/F)$ the Galois group, but we also use the adjective 'Galois' to describe a field extension E/F, but even though we can compute a Galois group $Gal(E/F)$, not all *extensions* are Galois extensions.

In particular, we will insist on having $|Gal(E/F)| = [E : F]$, as compared to those cases where $|Gal(E/F)| < [E : F]$, as we saw in the contrast between $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ as compared to $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

And the actual definition we are thinking of, which actually points to an extension being termed 'Galois', is one we saw already, namely

Definition

An extension E/F is a normal extension if E is a separable splitting field of some polynomial in $F[x]$.

And it is exactly this condition is which distinguishes $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ from $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, and in particular distinguishes $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ from $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.