GALOIS THEORY: LECTURE 14

LEO GOLDMAKHER

1. Exploring Galois Conjugates

We returned to a motivating question we asked previously:

Question 1. *Given $f \in K[t]$ and one of its roots $\alpha \in L/K$, can we find other roots of f in L? If so, how?*

Jonah noted that one approach to finding the remaining roots is to consider $\frac{f(t)}{t-\alpha}$ from which we may be able to "see" remaining roots more easily. While this approach works sometimes, $\frac{f(t)}{t-\alpha}$ can be messy and there is no guarantee that the roots of $\frac{f(t)}{t-\alpha}$ will be any more apparent than the roots of $f(t)$. Instead, we considered two examples of the type we considered in the first lecture of the course:

Example 1. If $2 + 17\sqrt{3}$ is a root of $f \in \mathbb{Q}[t]$, then its conjugate, $2 - 17\sqrt{3}$, is also a root.

Example 2. If $3 - 5i$ is a root of $f \in \mathbb{R}[t]$, then its complex conjugate, $3 + 5i$ is also a root.

Michael pointed out that to determine this new root, we exchanged i with $-i$, which is the same change made by the non-identity field automorphisms of the complex numbers. This observation prompted the following conjecture:

Conjecture 1.1 (Alex and Michael)**.** *Given $f \in K[t]$ and $\alpha \in L/K$ such that $f(\alpha) = 0$, let M/K be the splitting field of f. Then for all $\sigma \in \text{Aut}(M)$, $f(\sigma(\alpha)) = 0$.*

However, when we tried to prove this conjecture, we saw that it was not necessary for M to be a splitting field. Moreover, it was necessary for $\sigma(\alpha)$ to fix all elements of K. This realization led us to the following definition and updated proposition:

Definition. We define $\text{Aut}(L/K)$ to be the group of automorphisms of L that fix all elements of the field K:

$$\text{Aut}(L/K) := \{\sigma \in \text{Aut}(L) : \sigma(x) = x \text{ for all } x \in K\}$$

Proposition 1.2. *Given $f \in K[t]$ and $\alpha \in L/K$ a root of f. Then $\sigma(\alpha)$ is a root of f for all $\sigma \in \text{Aut}(L/K)$.*

Proof (Isaac). Let $f(t) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then, since $a_i \in K$ for all i, we have

$$\begin{aligned} f(\sigma(\alpha)) &= a_n\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(a_n)\sigma(\alpha^n) + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = \sigma(f(\alpha)) = \sigma(0) = 0. \end{aligned}$$

Therefore, $\sigma(\alpha)$ is a root of f. □

Remark. Note that this proposition implies something remarkable: that given α we can find other roots of f, *even if we don't know what f is*.

Remark. We noted that $\text{Aut}(K/\mathbb{Q}) = \text{Aut}(K)$ because we have shown previously that automorphisms of K always fix elements of $\mathbb{Q}$. Therefore, when the ground field is $\mathbb{Q}$, no automorphisms are "excluded" when considering the group $\text{Aut}(K/\mathbb{Q})$ rather than the group $\text{Aut}(K)$.

Since we are most familiar with Proposition 1.2 in the special cases of conjugates and complex conjugates, we call $\sigma(\alpha)$ a conjugate as well:

Date: April 9, 2018.

Based on notes by Emily Sundquist.

Definition. Given $\alpha \in L/K$, the *Galois conjugates* of α are $\{\sigma(\alpha) : \sigma \in \text{Aut}(L/K)\}$.

To build intuition, we considered two examples of $\text{Aut}(L/K)$.

Example 3. Determine $\text{Aut}(\mathbb{C}/\mathbb{R})$.

Note that $\mathbb{C} = \mathbb{R}[i]$, whence $\{1, i\}$ forms a basis for $\mathbb{C}$ over $\mathbb{R}$. Now pick any $\sigma \in \text{Aut}(\mathbb{C}/\mathbb{R})$. By definition $\sigma(r) = r$ for all $r \in \mathbb{R}$, so it suffices to determine the value of $\sigma(i)$. We know that the following must hold:

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1.$$

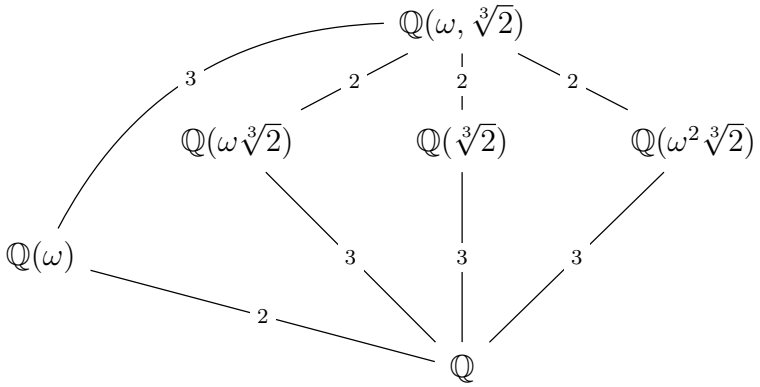
Therefore, $\sigma(i) = \pm i$. Each choice determines a unique automorphism: $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{e, \tau\}$ where e is the identity map and $\tau(\alpha) := \overline{\alpha}$ (the complex conjugate of α).

Example 4. Determine $\text{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$.

The given group is simply $\text{Aut}(\mathbb{Q}(\sqrt{3}))$. With a bit of work we see that $\text{Aut}(\mathbb{Q}(\sqrt{3})) = \{e, \sigma\}$, where e is the identity and $\sigma(a + b\sqrt{3}) := a - b\sqrt{3}$ for any $a, b \in \mathbb{Q}$. Therefore, $\text{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{e, \sigma\}$.

2. The Galois Correspondence

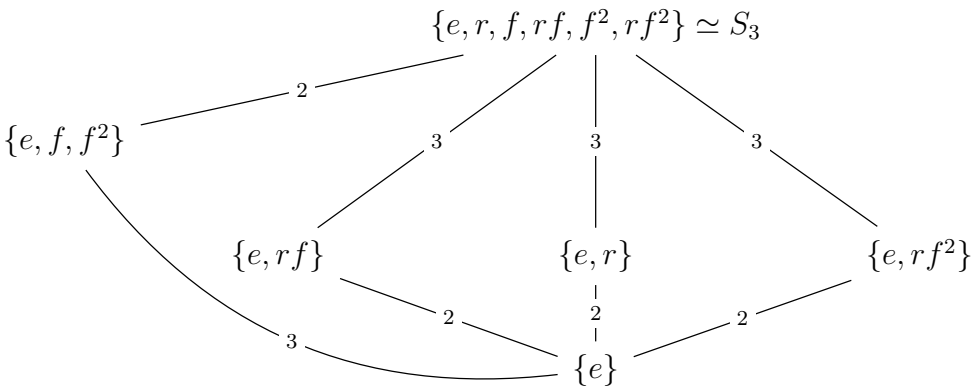
We now return to an example we explored in Lecture 13. We considered the smallest field containing all the cube roots of 2, which we determined to be $\mathbb{Q}(\omega, \sqrt[3]{2})$. We then built a lattice of all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\omega, \sqrt[3]{2})$:



Next, we considered $\text{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2}))$, which we determined to be $\{e, r, f, rf, f^2, rf^2\}$ where e is the identity and r, f are defined

$$r(\sqrt[3]{2}) = \sqrt[3]{2} \qquad r(\omega) = \omega^2$$
$$f(\sqrt[3]{2}) = \omega\sqrt[3]{2} \qquad f(\omega) = \omega$$

We then described a corresponding lattice of subgroups of $\text{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2}))$:



and noticed these two lattices "match up" when one is flipped upside down. This inspired the following question:

Question 2. *We know that the extreme (the topmost and bottom-most) groups in the latter diagram are the automorphism groups of the extreme fields in the former diagram. What about the intermediate groups? Are they automorphism groups of the intermediate fields?*

We began exploring this by considering the group $\text{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2}))$; some thought showed that

$$\text{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})) = \{e, r\}$$

We can also prove that

$$\begin{aligned}\text{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega\sqrt[3]{2})) &= \{e, rf\}\\ \text{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega^2\sqrt[3]{2})) &= \{e, rf^2\}\\ \text{Aut}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega)) &= \{e, f, f^2\}.\end{aligned}$$

Thus, the earlier correspondence that we observed between the extreme ends of our diagrams seems to hold in the middle of the diagram, as well.

Note that, even though we began our exploration with a polynomial, we've now moved away from that and are examining correspondences between field extensions and subgroups. We try to formalize this correspondence as follows:

Conjecture 2.1 (Fundamental Theorem of Galois Theory v1.0)**.** *Given L/K, let $G := \text{Aut}(L/K)$. Then there exists a bijective correspondence between the set of all intermediate fields lying between L and K and the set of all subgroups of G, given by $F \longmapsto \text{Aut}(L/F)$.*

As a first check that this is a reasonable conjecture, Trevin proposed to verify the degenerate case $L = K$. In this case, the field lattice consists of a single level, while $\text{Aut}(K/K) = \{e\}$ which has no subgroups. It follows that there is indeed a bijective correspondence between K and the trivial group.

However, Will noted that our conjecture fails for $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$: $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{e\}$, whereas $\mathbb{Q}(\sqrt[3]{2})$ has a subfield, namely $\mathbb{Q}$. In other words, there's no bijection in this case! In order to fix our conjecture, we consider the following question:

Question 3. *What extra conditions might we impose on L/K to make our conjecture hold?*

Idea 1. (Michael) Perhaps we lost too much information when we started focusing on the field extensions without keeping track of which polynomial we used. Thus, we might need to require that there exists some $f \in K[t]$ such that L is a splitting field of f.

Idea 2. (Daishiro) For there to even be a chance of a correspondence among the degrees of the extensions between the field diagram and the subgroup diagram, we need the overall degree from top to bottom to match. Thus, we need to require $|\text{Aut}(L/K)| = [L : K]$.

Idea 3. Note that $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ fixed more than just $\mathbb{Q}$: it fixed all of $\mathbb{Q}(\sqrt[3]{2})$. Thus, we might wish to require that the set of all elements of L that are fixed by every automorphism in $\text{Aut}(L/K)$ is *precisely* the field K.

Remarkably, these three potential fixes turn out to be (essentially) equivalent!

Proposition 2.2. *Given L/K a finite extension, the following are equivalent:*

(A) $|\text{Aut}(L/K)| = [L : K]$

(B) There exists a separable *polynomial $f \in K[t]$ such that L is the splitting field of f.*

(C) $K = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in \text{Aut}(L/K)\}$

Definition. L/K is a *Galois extension* if and only if it satisfies any one of the above equivalent conditions.

In light of these new ideas, we return to our guess of the Fundamental Theorem:

Conjecture 2.3 (Fundamental Theorem of Galois Theory, Version 2.0)**.** *Given L/K a finite* Galois extension*, let $G := \text{Aut}(L/K)$. Then there exists a bijective correspondence between the set of all intermediate fields lying between L and K and the set of all subgroups of G, given by $F \longmapsto \text{Aut}(L/F)$.*