# GALOIS THEORY: LECTURE 23

LEO GOLDMAKHER

## 1. Are splitting fields of solvable polynomials radical?

Recall the first step in the proof of Theorem 3.1 from Lecture 22: given a solvable, separable polynomial $f \in \mathbb{Q}[x]$, we enlarge its splitting field $K/\mathbb{Q}$ to a radical Galois extension of $\mathbb{Q}$. It's tempting to argue (as Ben did) that this step is unnecessary. After all, we know that $K/\mathbb{Q}$ must be Galois, and by adjoining all the roots of $f$ to $\mathbb{Q}$ one at a time, we create a sequence of radical extensions connecting $\mathbb{Q}$ to $K$... which is to say, $K/\mathbb{Q}$ is radical. But something must be wrong with this argument, or else we wouldn't have gone through all the trouble we did in Lecture 22 to generate a Galois radical extension $L/\mathbb{Q}$! Formally:

**Question 1** (Ben)**.** *Must splitting fields of solvable polynomials radical? More precisely, given a separable $f \in \mathbb{Q}[x]$ whose roots are all expressible in radicals, is it possible for its splitting field $K$ to* not *be a radical extension of $\mathbb{Q}$?*

To sort out this puzzling issue, we begin with the following observation.

**Proposition 1.1.** *If $K/\mathbb{Q}$ is normal and of degree 3, then it is not radical.*

*Proof.* Suppose $K/\mathbb{Q}$ were radical. Then Tower Law implies $K/\mathbb{Q}$ must be a *simple* radical extension. This is equivalent to writing $K = \mathbb{Q}(\alpha)$ with $\alpha^3 \in \mathbb{Q}$. Moreover, the minimal polynomial of $\alpha$ has degree 3, whence the minimal polynomial of $\alpha$ must be $x^3 - \alpha^3$. Since $K/\mathbb{Q}$ is normal and contains a root of the irreducible polynomial $x^3 - \alpha^3$, the field extension $K/\mathbb{Q}$ contains *all* the roots of $x^3 - \alpha^3$. It follows that $\omega$ (the cube root of unity) lives in $K$. But this contradicts Tower Law, since $K/\mathbb{Q}(\omega)/\mathbb{Q}$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Thus, $K/\mathbb{Q}$ cannot be a radical extension. □

*Remark.* Emily noted that this proposition can be generalized to normal extensions of arbitrary (odd) prime degree.

**Corollary 1.2.** *The polynomial $f(x) = x^3 - 3x - 1$ has all radical roots and its splitting field $K$ is not a radical extension of $\mathbb{Q}$.*

*Proof.* First recall that the cubic formula expresses all three roots of $f$ as a combination of the coefficients of $f$, the four field operations, square roots, cube roots, and roots of unity. Since the coefficients of $f$ are rational, it follows that all its roots are expressible in radicals. It remains to show that $K/\mathbb{Q}$ isn't radical.

To do this, we'll employ Proposition 1.1. We have to show that $K/\mathbb{Q}$ satisfies the hypotheses of the proposition. First off, note that $f$ is irreducible over $\mathbb{Q}$ (for example by reduction in $\mathbb{F}_2$), which implies that $f$ is separable. We deduce that $K/\mathbb{Q}$ is Galois, whence

$$[K : \mathbb{Q}] = |\mathrm{Gal}(f)| \qquad \text{and} \qquad K/\mathbb{Q} \text{ is normal.}$$

Finally, it's a good exercise to prove that

$$\mathrm{Gal}(f) \simeq \mathbb{Z}_3.$$

Putting all this together, we see that $K/\mathbb{Q}$ satisfies the hypotheses of Proposition 1.1, hence cannot be a radical extension. □

*Exercise* 1. In the first paragraph of this section we gave an argument that $K/\mathbb{Q}$ should be radical. In view of Corollary 1.2, that argument cannot be correct. What's wrong with it?

*Date*: May 10, 2018.
Based on notes by Jonah Greenberg.

## 2. Computing Gal($f$) without explicitly knowing its roots

Before Galois' work, mathematicians expected a solvability criterion (if not an outright formula) in terms of the *coefficients* of a polynomial $f \in \mathbb{Q}[x]$. Instead, Galois gave a criterion for solvability in terms of $\mathrm{Gal}(f)$. At first glance this seems to be begging the question, since $\mathrm{Gal}(f)$ is itself measuring the symmetries among the roots, which implies that we already need to know something about the roots! What Galois realized is that one can determine a good deal about $\mathrm{Gal}(f)$ without knowing the roots – it suffices to figure out a bunch of relations *among* the roots. The more relations we know, the more information we can glean about $\mathrm{Gal}(f)$. The goal of this section is to illustrate how we can determine the Galois group of a given polynomial without already knowing its roots.

Let

$$f(x) := x^4 + 4x^2 + 2$$

and set $G := \mathrm{Gal}(f)$. Recall that any element of $G$ permutes the roots of $f$, whence

$$G \leq S_4.$$

The game we're going to play is to determine as many relations among the roots as possible; each relation will eliminate some subgroups of $S_4$. If we eliminate all but one subgroup, $G$ must be whatever's left!

Let $K$ be a splitting field of $f$ over $\mathbb{Q}$.

(i) *The roots come in pairs.*

Observe that all powers of $x$ appearing in $f$ are even. Right away this imposes a symmetry on the roots of $f$: if $\alpha$ is a root of $f$, then so is $-\alpha$. Thus, we can write the roots of $f$ as $\{\pm\alpha, \pm\beta\}$. For ease of notation, let's make the following associations:

$$1 \leftrightarrow \alpha \qquad 2 \leftrightarrow -\alpha \qquad 3 \leftrightarrow \beta \qquad 4 \leftrightarrow -\beta$$

Thus, for example, we can notate the transposition exchanging $\alpha$ and $-\beta$ as $(1\ 4)$.

(ii) *We have $G \leq D_8$, the dihedral group of order 8.*[1]

Pick any $\sigma \in G$. Since $\sigma(-\alpha) = -\sigma(\alpha)$, we see that $\sigma(\{\pm\alpha\}) = \{\pm\alpha\}$ or $\{\pm\beta\}$. In particular, this imposes some limitations on $\sigma$:

$$\begin{aligned}\sigma \notin \{&(1\ 3), (1\ 4), (2\ 3), (2\ 4),\\ &(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),\\ &(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 4\ 3\ 2)\}\end{aligned}$$

Since $\sigma \in G$ was arbitrary, we deduce that

$$\begin{aligned}G &\subseteq \{(\ ), (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}\\ &= \{e, \rho, \rho^2, \rho^3, \phi, \rho\phi, \rho^2\phi, \rho^3\phi\}\end{aligned}$$

where $e := (\ )$, $\rho := (1\ 3\ 2\ 4)$, and $\phi := (1\ 2)$. Note that $\rho^4 = e = \phi^2$ and $\phi\rho = \rho^3\phi$; it follows that $G \leq D_8$.

(iii) *We have $4 \mid |G|$.*

Eisenstein implies that $f$ is irreducible. It follows that $f$ is the minimal polynomial of $\alpha$, whence

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4.$$

Since $Q(\alpha)$ is an intermediate field of the extension $K/\mathbb{Q}$, Tower Law yields

$$4 \mid [K : \mathbb{Q}] = |G|.$$

(iv) *$G$ must be isomorphic to $D_8$, $\mathbb{Z}_4$, or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

[1] We're cheating a bit here: $G$ is a subgroup of an *isomorphic copy* of $D_8$ sitting inside $S_4$.

Combining the previous two steps we see that

$$|G| = 4 \text{ or } 8.$$

There are precisely four subgroups of $D_8$ of order 4 or 8:

$$\underbrace{\{e, \rho, \rho^2, \rho^3, \phi, \rho\phi, \rho^2\phi, \rho^3\phi\}}_{D_8} \qquad \underbrace{\{e, \rho, \rho^2, \rho^3\}}_{H_1} \qquad \underbrace{\{e, \rho^2, \phi, \rho^2\phi\}}_{H_2} \qquad \underbrace{\{e, \rho\phi, \phi\rho, \rho^2\}}_{H_3}.$$

Our hope is to rule out three of these.

(v) $G \neq H_3$

Since the roots are $\pm\alpha, \pm\beta$, we have

$$f(x) = x^4 + 4x^2 + 2 = (x^2 - \alpha^2)(x^2 - \beta^2).$$

This implies

$$\alpha^2 + \beta^2 = -4 \qquad \text{and} \qquad \alpha^2\beta^2 = 2.$$

From the second observation, we deduce that $\alpha\beta \notin \mathbb{Q}$. On the other hand we know $K^G = \mathbb{Q}$. It follows that $\alpha\beta$ cannot be fixed by all of $G$. Since $\alpha\beta$ is fixed by all of $H_3$ (a straightforward verification), we deduce that $G \neq H_3$.

(vi) $G \neq H_2$

From above we know that $\alpha^2 + \beta^2 = -4$ and $\alpha^2\beta^2 = 2$. It follows that

$$(\alpha^2 - \beta^2)^2 = (\alpha^2 + \beta^2)^2 - 4\alpha^2\beta^2 = 8.$$

Thus $\alpha^2 - \beta^2 = 2\sqrt{2}$, and we deduce that $\alpha^2 = -2 + \sqrt{2} \notin \mathbb{Q}$. As before, this means $\alpha^2$ isn't fixed by all of $G$. On the other hand, $\alpha^2$ is fixed by all of $H_2$ (a straightforward verification). This shows that $G \neq H_2$.

(vii) $G \neq D_8$

In our previous two arguments, we produced some combination of the roots which was irrational, hence couldn't be fixed by all of $G$. Now we take a different tack, producing a combination of the roots which is rational and therefore *must* be fixed by all of $G$.

Observe that

$$\sigma(\alpha^3\beta - \alpha\beta^3)^2 = \sigma(\alpha\beta)^2\sigma(\alpha^2 - \beta^2)^2 = 16$$

by our work above. It follows that

$$\sigma(\alpha^3\beta - \alpha\beta^3) = \pm 4.$$

Since $\sigma \in \text{Aut}(K/\mathbb{Q})$, we deduce

$$\alpha^3\beta - \alpha\beta^3 = \pm 4,$$

whence $\alpha^3\beta - \alpha\beta^3$ is fixed by all of $G$. However, it's straightforward to verify that $\alpha^3\beta - \alpha\beta^3$ is *not* fixed by $\rho\phi$. Thus $G$ cannot be $D_8$.

(viii) By process of elimination, we conclude that

$$\text{Gal}(f) = \{e, \rho, \rho^2, \rho^3\} \simeq \mathbb{Z}_4.$$

*Remark.* Since $\text{Gal}(f)$ is abelian, we deduce that $f$ is solvable. Of course for this particular $f$ we could have found the roots directly, but the point of the exercise is that we don't need to – with a bit of cleverness we can make deductions directly from the coefficients of $f$ about relations between the roots, which can be combined to pinpoint the Galois group of $f$.