GALOIS THEORY: LECTURE 22

LEO GOLDMAKHER

1. Recap of previous lecture

Recall that last class we sketched a proof for the insolvability of the quintic. We argued that any quintic polynomial $f \in \mathbb{Q}[x]$ with $\mathrm{Gal}(f) \simeq S_5$ cannot be solved in radicals. (We considered the specific example $f(x) = x^5 - 4x - 2$, but the argument works for any f with $\mathrm{Gal}(f) = S_5$.) At the heart of the argument is the following result due to Galois:

Galois' solvability criterion. Given a separable polynomial $f \in \mathbb{Q}[x]$. Then f is solvable in radicals if and only if all composition factors of $\mathrm{Gal}(f)$ are abelian.

With this in hand, the rest of the argument isn't hard. Indeed, the composition series for S_5 is $S_5 \rhd A_5 \rhd \{e\}$, because A_5 is simple and has index 2 in S_5. Thus, the composition factors of S_5 are A_5 and $\mathbb{Z}/2\mathbb{Z}$. Since A_5 isn't abelian, Galois' solvability criterion implies that the roots of f do not live in any radical extension of $\mathbb{Q}$. (Note that we only used the forward implication of Galois' criterion in this argument.)

Although we sketched an argument for the (forward direction of the) Galois solvability criterion in Lecture 21 (see Theorem 2.1 there), it was not a rigorous proof. Our goal for today is to prove the theorem. The first order of business is to revise the definition of a simple radical extension that we gave last time; although the adjustment seems minor, it is a crucial move.

Definition. Any extension of the form $K(\beta)/K$ with $\beta^m \in K$ for some positive integer m is called a *simple radical extension*.

Remark. Last class, for L/K to be a simple radical extension we required that $L = K(\alpha^{1/n})$ for $n \in \mathbb{N}$ and $\alpha \in K$. Our updated definition is less restrictive, because we no longer distinguish any of the roots of $x^n - \alpha$. For example, denoting the principal n^{th} root of unity by ζ_n, we now consider $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ to be a simple radical extension (our more restricted definition from last class wouldn't permit this).

Our definition of radical extension remains unchanged:

Definition. L/K is a *radical extension* if it can be decomposed into a finite tower of simple radical extensions.

Recall the *raison d'être* of this concept: we wish to say that a number $\alpha \in \mathbb{C}$ is expressible in terms of radicals iff α lives inside of some radical extension of $\mathbb{Q}$. The main effect of changing our definition of simple radical extension is that, under the new definition, we allow arbitrary roots of unity to be used in a radical expression. (Under the earlier definition, $i = \sqrt{-1}$ was allowed, but the cube root of unity ω wasn't.)

2. Ingredients

Before rigorously proving Galois' solvability criterion, we need to assemble a few ingredients. The first is a basic result from group theory.

Third Isomorphism Theorem. Given $G \trianglerighteq H$, and suppose $G \geq N \geq H$. Then
(1) $N \trianglerighteq H$ and $G/H \geq N/H$.
If, moreover, $G \trianglerighteq N \trianglerighteq H$, then
(2) $G/H \trianglerighteq N/H$, and $G/N \simeq (G/H)/(N/H)$.

Date: May 7, 2018.
Based on notes by Trevin Corsiglia.

Note that this is reminiscent of field extensions: the first assertion is parallel to the result that inserting any intermediate field into a Galois extension makes the top extension Galois, and the second assertion is parallel to part (4) of the FTGT.

A second important ingredient is a result we proved at the end of Lecture 21:

Lemma 2.1. *Given K a finite extension of $\mathbb{Q}$. If $\alpha^m, \zeta_m \in K$ then* $\mathrm{Gal}(K(\alpha)/K)$ *is cyclic.*

Recall from our sketch of Galois' solvability criterion that, given a radical extension $L/\mathbb{Q}$, we'd like to build a tower of abelian extensions between $\mathbb{Q}$ and L. The above lemma allows us to accomplish this under the assumption that the intermediate fields all contain an appropriate root of unity. How do we enforce this condition? Simple: we start our tower by adjoining some large root of unity to $\mathbb{Q}$, thereby ensuring its existence thenceforth. But now we need to check that we haven't ruined our argument in the process. More precisely, we must verify that

(1) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a simple radical extension, and
(2) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is abelian.

The former holds thanks to our new, more permissive definition of simple radical extension, and you will prove the latter in your assignment (see problem **11.3**). To be able to refer to it, we state the result formally here:

Lemma 2.2. *For any $n \in \mathbb{N}$, the Galois group* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is abelian.*

We now have all the tools we need to prove Galois' solvability criterion, which we carry out in the next section. But first, we discuss a bit of related history. Any group all of whose composition factors are abelian is called *solvable*; thus, Galois' criterion asserts that a separable $f \in \mathbb{Q}[x]$ is solvable in radicals if and only if $\mathrm{Gal}(f)$ is solvable. In other words, we've translated the problem of determining the solvability of polynomials into a problem about determining the solvability of groups. This inspires a natural question: is it possible to classify all solvable groups? Or at least to give an easy sufficient condition for a group to be solvable?

As a warm up, we prove the following:

Proposition 2.3. *If $|G| = p^m$ for some prime p, then G is solvable.*

Proof. By Sylow's theorem, there exist subgroups $G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_m = \{e\}$ with $|G_k| = p^{m-k}$. It follows that $|G_i/G_{i+1}| = p$ for all i. It turns out (see lemma below) that this forces $G_{i+1} \lhd G_i$, whence $G_i/G_{i+1} \simeq \mathbb{Z}_p$ for all i. This immediately implies that G is solvable. □

Lemma 2.4. *Suppose p is the* smallest *prime factor of a group G, and that $|G/H| = p$ for some $H \leq G$. Then $H \lhd G$.*

Remark. The hypothesis that p be the smallest prime factor can be weakened, but it cannot be removed entirely. For a proof of the lemma (as well as a nice generalization to subgroups of composite index), see the supplementary document 'Subgroups of Prime Index'.

Can Proposition 2.3 be strengthened? For example, what can we say about groups of order other than a prime power? The first serious work on this was completed by William Burnside, an applied mathematician who became one of the pioneers in the theory of group representations.

Theorem 2.5 (Burnside, 1904)**.** *If $|G| = p^m q^n$ for some primes p and q, then G is solvable.*

Seven years later, Burnside conjectured that every finite nonabelian simple group must have even order (the connection to solvability being that a solvable nonabelian group cannot be simple). This conjecture inspired a lot of research, including one of the greatest (and most difficult) accomplishments in abstract algebra:

Theorem 2.6 (Feit-Thompson, 1962)**.** *If $|G|$ is odd, then G is solvable.*

Note that this implies Burnside's conjecture.

3. Proof of Galois' solvability criterion

Our goal in this section will be to prove the forward direction of Galois' solvability criterion. In other words, we'll prove

Theorem 3.1. *If $f \in \mathbb{Q}[x]$ is separable and solvable in radicals, then* $\mathrm{Gal}(f)$ *is a solvable group.*

Remark. Although we won't prove it here, once you understand the proof of the forward direction of Galois' criterion you will have all the tools for handling the reverse direction.

Although the underlying idea isn't so complicated, the formal proof is clouded by technical details. To help the reader keep track of this, I split the proof into several broad steps.

Step 1. *Enlarge the splitting extension to one which is simultaneously Galois and radical.*

Recall from Lecture 21 that our proof hinges on two ideas: (i) all the roots of f live inside some extension $L/\mathbb{Q}$ which is Galois and radical, hence can be decomposed into a tower of simple radical extensions; and (ii) the Galois group of each simple radical extension is abelian. From here, one uses the Fundamental Theorem of Galois Theory to translate the problem into group theory, and then some more group theory produces the desired result.

But what is this field L? A first guess might be that L is the splitting field of f over $\mathbb{Q}$, but it turns out that this doesn't work. To see this, let K denote the splitting field of f over $\mathbb{Q}$. Since f is separable, $K/\mathbb{Q}$ is Galois – so far, so good. Moreover, we know (see problem **11.6**) that *all* roots of f are expressible in radicals. It therefore comes as a bit of a shock that $K/\mathbb{Q}$ might not be a radical extension! (We'll see an example of this strange behavior next lecture.)

Thus, we can't apply our argument to the splitting field $K/\mathbb{Q}$. That's OK, though, because we know that all the roots of f must live in some radical extension $F/\mathbb{Q}$. Moreover, since K is the splitting field of f, we deduce that we have a tower $F/K/\mathbb{Q}$. This looks promising, but there's a fly in the ointment: $K/\mathbb{Q}$ is Galois, but $F/\mathbb{Q}$ might not be! This is bad for us, because it prevents us from applying the FTGT as our argument requires.

Fortunately, we know (see problem **9.4**) that any finite extension of $\mathbb{Q}$ can be enlarged to a finite Galois extension. This allows us to find some finite Galois extension $L/\mathbb{Q}$ such that L/F. The problem is that it's not at all obvious that this larger field L is still a radical extension of $\mathbb{Q}$! Fortunately, it turns out that it is. In other words, $L/\mathbb{Q}$ is simultaneously radical and Galois, which puts us in the position to proceed with our argument. Without further ado, we state and prove the necessary result.

Lemma 3.2. *Any radical extension $F/\mathbb{Q}$ can be enlarged to an extension $L/\mathbb{Q}$ that is simultaneously radical and Galois.*

Proof. Given $F/\mathbb{Q}$ a radical extension, we know (by definition) that it can be decomposed into a finite tower of simple radical extensions. In other words, we have a sequence of field extensions

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_n = F$$

such that each extension F_k/F_{k-1} is a simple radical extension. In other words, for each k there exists some number α_k such that $F_k = F_{k-1}(\alpha_k)$ and some positive power of α_k lives in F_{k-1}.

Writing $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ we enlarge $F/\mathbb{Q}$ to a Galois extension in the usual way, by letting L be the splitting field of the least common multiple of the minimal polynomials $\{m_{\alpha_i} : 1 \leq i \leq n\}$. Note that this least common multiple must be separable, by the Fundamental Lemma and problem **9.3**. It follows that $L/\mathbb{Q}$ is Galois. We claim that $L/\mathbb{Q}$ is a radical extension.

To prove this, we'll show that adjoining Galois conjugates one at a time creates a sequence of simple radical extensions. To do this, it's helpful to introduce some notation. Set $G := \mathrm{Gal}(L/\mathbb{Q})$ and define a tower of fields recursively by

$$\widetilde{F}_0 := \mathbb{Q} \qquad \text{and} \qquad \widetilde{F}_k := \widetilde{F}_{k-1}(\{\sigma(\alpha_k) : \sigma \in G\}).$$

Note that $\widetilde{F}_0 = \mathbb{Q}$ and $\widetilde{F}_n = L$, so to prove that $L/\mathbb{Q}$ is radical it suffices to show that $\widetilde{F}_k/\widetilde{F}_{k-1}$ is a radical extension for all k. We'll require the following tool:

Lemma 3.3. *For all $\sigma \in G$, $\sigma(F_k) \subseteq \widetilde{F}_k$.*

With this in hand, we conclude the proof of Lemma 3.2. Then we'll go back and prove Lemma 3.3.

Pick $\sigma \in G$. There exists some $m \in \mathbb{N}$ such that $\alpha_i^m \in F_{i-1}$. It follows that

$$\sigma(\alpha_i)^m = \sigma(\alpha_i^m) \in \sigma(F_{i-1}) \subseteq \widetilde{F}_{i-1}.$$

In other words, $\widetilde{F}_{i-1}\Big(\sigma(\alpha_i)\Big)/\widetilde{F}_{i-1}$ is a simple radical extension for any $\sigma \in G$. Adjoining all the Galois conjugates of α_i one at a time therefore produces a sequence of simple radical extensions from $\widetilde{F}_{i-1}$ to $\widetilde{F}_i$. This shows that $\widetilde{F}_i/\widetilde{F}_{i-1}$ is radical for all i, whence $L/\mathbb{Q}$ must also be radical. □

One step in the proof above remains unresolved: we need to prove Lemma 3.3.

Proof of Lemma 3.3. We proceed by induction. Pick $\sigma \in G$. The base case is purely notational:

$$\sigma(F_0) = \sigma(\mathbb{Q}) = \mathbb{Q} = \widetilde{F}_0.$$

Now we consider the inductive step:

$$\begin{aligned}
\sigma(F_k) &= \sigma\Big(F_{k-1}(\alpha_k)\Big) = \sigma\Big(F_{k-1}[\alpha_k]\Big) \\
&= \sigma\Big(\big\{f(\alpha_k) : f \in F_{k-1}[x]\big\}\Big) \\
&\subseteq \sigma(F_{k-1})\Big(\sigma(\alpha_k)\Big) \\
&\subseteq \widetilde{F}_{k-1}\Big(\sigma(\alpha_k)\Big) \\
&\subseteq \widetilde{F}_k.
\end{aligned}$$

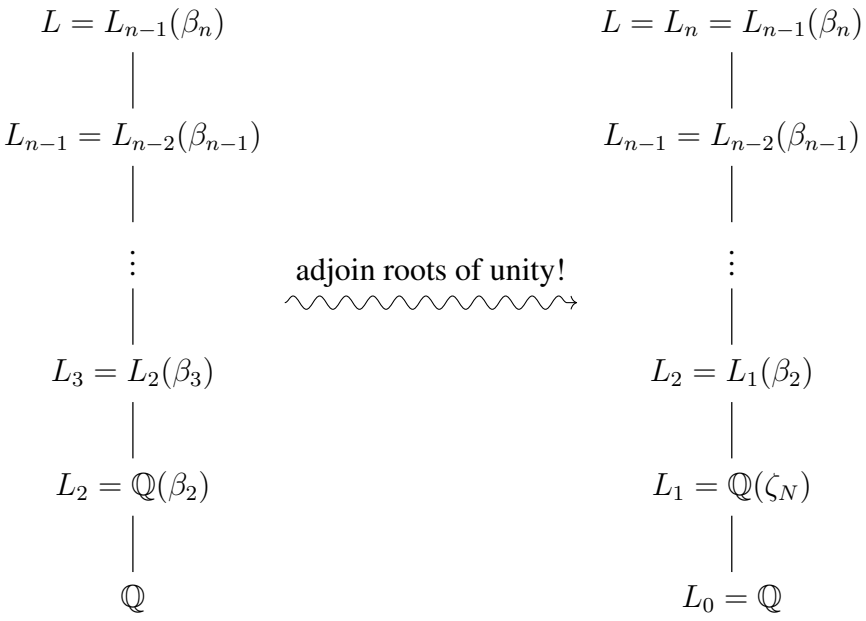
□

Step 2. *The composition factors of* $\mathrm{Gal}(L/\mathbb{Q})$ *are all abelian.*

Since L is radical, we can decompose it into a sequence of simple radical extensions

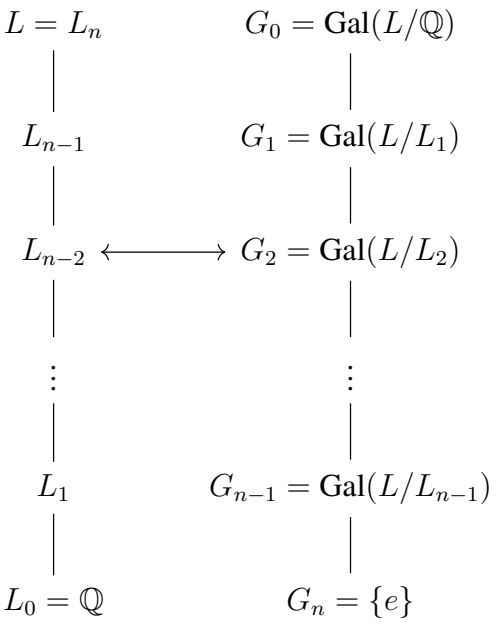
$$L = L_n \supsetneq L_{n-1} \supsetneq \cdots \supsetneq L_1 \supsetneq L_0 = \mathbb{Q}$$

where for each k there exists $\beta_k \in \mathbb{C}$ and $d_k \in \mathbb{N}$ such that $L_k = L_{k-1}(\beta_k)$ and $\beta_k^{d_k} \in L_{k-1}$. We now wish to apply Lemma 2.1 to the intermediate extensions L_k/L_{k-1}, but we can't because these might not contain the appropriate roots of unity! So, we employ a trick. Set $N := \mathrm{LCM}(d_2, d_3, \ldots, d_n)$.



By adjoining ζ_N to $\mathbb{Q}$ as our bottom-most extension, we guarantee that all each field L_i will contain the root of unity ζ_{d_i}, which puts us in the position to apply Lemma 2.1. We thus deduce that L_i/L_{i-1} is Galois and abelian for all $i \geq 2$. And Lemma 2.2 asserts that L_1/L_0 is also Galois and abelian. (Note: our restriction that a radical extension consists of *finitely* many simple radical extensions is crucial in this step – otherwise, we might not have been able to construct the appropriate root of unity ζ_N!)

Now since $L/\mathbb{Q}$ is Galois, we can employ the FTGT:



Note that the Galois groups represented are *not* coming from the extensions L_i/L_{i-1} discussed above – instead, they are all of the form $\text{Gal}(L/L_i)$.

However, we also know that L_i/L_{i-1} is Galois for each i. The FTGT then implies that corresponding group extension is normal:

$$\text{Gal}(L/L_i) \lhd \text{Gal}(L/L_{i-1}).$$

Actually, the FTGT says more:

$$\text{Gal}(L_i/L_{i-1}) \simeq G_{i-1}/G_i.$$

In summary, we've created a normal chain

$$\text{Gal}(L/\mathbb{Q}) \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd \{e\} \tag{1}$$

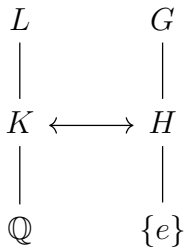
where each adjacent quotient is abelian. Now (1) is not necessarily a composition series – there may be intermediate groups. However, as Franny observed, any refinement of this series preserves abelianness. Indeed, suppose $G \rhd H$ with G/H abelian, and that N is some intermediate normal subgroup: $G \rhd N \rhd H$. Then the third isomorphism theorem produces two conclusions: that $N/H \lhd G/H$, and that $G/N \simeq (G/H)/(N/H)$. The former implies that N/H must be abelian; the latter implies that G/N must be as well.

Thus, we see that in any refinement of our normal series (1) all adjacent quotients must be abelian. It follows that all the composition factors of $\text{Gal}(L/\mathbb{Q})$ must be abelian, as claimed.

Step 3. *The composition factors of* $\text{Gal}(f)$ *are all abelian.*

Recall that the splitting field of f over $\mathbb{Q}$ is K, not L. Thus we still have a bit more work to do: we've proved that all the composition factors of $\text{Gal}(L/\mathbb{Q})$ are abelian, and now we wish to do the same for the group $\text{Gal}(K/\mathbb{Q})$.

Since K is an intermediate field of the extension $L/\mathbb{Q}$, the FTGT produces the following picture:



Here $G := \text{Gal}(L/\mathbb{Q})$ and $H := \text{Gal}(L/K)$.

Moreover, we know that $K/\mathbb{Q}$ is Galois, so the FTGT tells us that $H \lhd G$ and that

$$\text{Gal}(f) = \text{Gal}(K/\mathbb{Q}) \simeq G/H.$$

This allows us to remove all vestiges of field theory from the problem and rephrase it purely in terms of group theory:

What we know	**What we claim**
All composition factors of G are abelian $G \rhd H \rhd \{e\}$	All composition factors of G/H are abelian

Consider a complete refinement of the normal series $G \rhd H \rhd \{e\}$; it takes the form

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = H \rhd \cdots$$

By Jordan-Hölder, we obtain precisely the same list of composition factors from this composition series as we did in Step 2. In particular, we deduce that H_{i-1}/H_i is simple and abelian for all $i \leq m$. The third isomorphism theorem implies that for any $i \leq m$ we have

$$H_{i-1} \rhd H_i \rhd H,$$

and moreover that $(H_{i-1}/H) \rhd (H_i/H)$ and

$$(H_{i-1}/H)/(H_i/H) \simeq H_{i-1}/H_i,$$

which we know from above is simple and abelian. We've therefore produced a composition series

$$(G/H) = (H_0/H) \rhd (H_1/H) \rhd \cdots \rhd (H_m/H) = \{e\}$$

whose composition factors are all abelian. This completes the proof! Q.E.F.D.

I invite the reader to think about how to prove the converse direction of Galois' solvability criterion. You have all the necessary tools!