GALOIS THEORY: LECTURE 21

LEO GOLDMAKHER

1. Simple groups and the Jordan-Hölder theorem

Recall that at the end of last class we stated the Jordan-Hölder Theorem. Here's the setup. Given any finite nontrivial group G, we have a normal series $G \rhd \{e\}$. We refine this normal series by inserting proper normal subgroups in between G and $\{e\}$ one at a time. Eventually we obtain a maximally refined normal series of the form

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\},$$

where no more intermediate normal subgroups can be inserted. Any such maximally refined normal series is called a *composition series* of G; the adjacent quotients G_i/G_{i+1} are called the *composition factors* of G.

Jordan-Hölder Theorem (Jordan 1869-70, Hölder 1889)**.** Fix any finite group G. Then every composition series of G has the same length, and the list of composition factors is unique up to order and isomorphism.

What can we say about the composition factors of a given group? Writing a given composition factor in the form G_i/G_{i+1}, we know by definition that there are no intermediate normal subgroups between G_i and G_{i+1}. This implies that the quotient group G_i/G_{i+1} has no normal subgroups. A group with this property has a special name:

Definition. A group is called *simple* if and only if its only normal subgroups are itself and the trivial group.

Thus all the composition factors of G are simple. According to our analogy between groups and whole numbers from last time, we see that simple groups are the natural analogues of prime numbers, since their only proper 'divisor' is the trivial group $\{e\}$. Thus, Jordan-Hölder is completely parallel to unique factorization in the whole numbers: just as every whole number can be decomposed into a unique list of prime factors, every finite group can be decomposed into a unique list of simple composition factors. In fact, Jordan-Hölder is literally a generalization of uniqueness of factorization in $\mathbb{N}$; see problem **11.2**.

There are some familiar examples of simple groups, e.g. the alternating groups A_n for all $n \geq 5$, and all cyclic groups of prime order. Remarkably, finite simple groups have been completely classified: every simple group lies in one of 18 infinite families (two of which we listed above) or one of 26 exceptional ("sporadic") groups. This classification is the main advantage of Jordan-Hölder over Krull-Schmidt: rather than breaking down G into some equally mysterious indecomposables, we decompose G into finite simple groups, which we understand very well.

Unfortunately, unlike the case of factorization in $\mathbb{Z}$, one cannot in general recover the group G from its composition factors. In other words, given two groups N and H there sometimes exist non-isomorphic groups G and G' such that N is isomorphic to a normal subgroup of both G and G', and $G/N \simeq H \simeq G'/N$. See problem **11.2**.

2. Radical extensions

Early on this semester, we learned that the original motivation for Galois' work was to prove the insolvability of the quintic. The goal for the rest of today's class is to sketch this proof. The main idea is transparent and lovely, but there are a few technical complications that arise. We'll postpone dealing with these details to next class. Throughout, we'll assume all fields have characteristic 0.

Date: May 3, 2018.

Based on notes by Qiana Yang.

Question 1. *What does it mean for a number to be expressible in radicals? i.e. how do we formally define it?*

What Galois realized is that any number expressible in radicals must live in a particularly nice type of field extension of $\mathbb{Q}$ called a *radical extension*. For example, in which field does $\alpha := \sqrt{-7 + \sqrt[3]{2}} - \sqrt[5]{10}$ live? Of course it lives in $K := \mathbb{Q}(\alpha)$, but this doesn't tell us anything new. Galois' insight was that we can construct the field K in simple stages by building a tower of simple extensions:

$$\begin{tikzcd}
K := K_2(\sqrt[5]{10}) \arrow[d, dash] \\
K_2 := K_1(\sqrt{-7 + \sqrt[3]{2}}) \arrow[d, dash] \\
K_1 := K_0(\sqrt[3]{2}) \arrow[d, dash] \\
K_0 := \mathbb{Q}
\end{tikzcd}$$

Note that each intermediate field is a simple extension of the one right below it, and that a primitive element of each extension is just a single radical applied to a single field element. This motivates the following concepts:

Definition. Any extension $K(\alpha^{1/n})/K$ where $n \in \mathbb{N}$ and $\alpha \in K$ is called a *simple radical extension*.

Definition. An extension L/K is a *radical extension* if and only if it can be broken down into a finite tower of simple radical extensions.

Trevin noted that any simple radical extension must be algebraic. Indeed, any simple radical extension is finite, hence (by Tower Law) so is any radical extension. But we know that every finite extension is algebraic.

Galois' main insight was:

$$\text{\textit{If a simple radical extension is Galois, then its Galois group is abelian.}} \tag{1}$$

A secondary (but also important) insight was that if a polynomial has a root expressible in radicals, then *all* its roots must live in some radical extension of $\mathbb{Q}$. Taking these two insights on faith for now, we describe Galois' proof of the insolvability of the quintic.

Suppose we have some polynomial $f \in \mathbb{Q}[x]$ with one root expressible in radicals. By Galois' second insight, all its roots live in some radical extension $L/\mathbb{Q}$. Decomposing the radical extension into a tower of simple radical extensions and applying the Galois correspondence yields the following picture:

$$\begin{tikzcd}
L = K_n \arrow[d, dash, "\text{simple radical extn}\to"'] & & G_0 = \text{Gal}(L/K_0) \arrow[d, dash] \\
K_{n-1} \arrow[d, dash, "\text{simple radical extn}\to"'] & & G_1 = \text{Gal}(L/K_1) \arrow[d, dash] \\
\vdots \arrow[d, dash, "\text{simple radical extn}\to"'] & \longleftrightarrow & \vdots \arrow[d, dash] \\
K_1 \arrow[d, dash, "\text{simple radical extn}\to"'] & & G_{n-1} = \text{Gal}(L/K_{n-1}) \arrow[d, dash] \\
K_0 = \mathbb{Q} & & G_n = \{e\}
\end{tikzcd}$$

Suppose all the simple extensions making up our tower are Galois. The Fundamental Theorem of Galois Theory implies that

$$G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{e\},$$

and that

$$\mathrm{Gal}(K_{j+1}/K_j) \simeq G_j/G_{j+1}$$

for each j. Moreover, Galois' first insight (1) tells us that all the $\mathrm{Gal}(K_{j+1}/K_j)$ are abelian. In other words, we deduce the existence of a normal series

$$\mathrm{Gal}(f) = G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{e\}$$

such that G_j/G_{j+1} is abelian for all j. In particular, if we can find some $f \in \mathbb{Q}[x]$ with Galois group which doesn't satisfy this property, the above argument shows that f cannot be solved in radicals!

The above argument is riddled with holes, unfortunately. Perhaps the most immediately glaring issue (pointed out by Andrew) is that simple radical extensions need not be Galois, as our favorite counterexample $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ demonstrates. This is consistent with Galois' insight (1), but it does mean we have to think carefully about when a simple radical extension is Galois.

A more serious flaw is that we cannot apply the Fundamental Theorem of Galois Theory unless we know that the extension $L/\mathbb{Q}$ is Galois. More precisely, we know that the splitting field of f is Galois over $\mathbb{Q}$ (assuming f is separable), but we *don't* know whether this holds for the radical extension L containing the roots of f. Note that even in the ideal case of a tower of simple radical extensions which are all Galois connecting $\mathbb{Q}$ to L, the overall extension $L/\mathbb{Q}$ might not be Galois![1] (See problem **8.5**.) Next class we'll get around this by showing that any radical extension of $\mathbb{Q}$ can be enlarged to a Galois radical extension. Combining this with a bit of elbow grease will ultimately lead us to the following result:

Theorem 2.1 (Galois). *Given a separable polynomial $f \in \mathbb{Q}[x]$. If f is solvable in radicals, then all composition factors of* $\mathrm{Gal}(f)$ *are abelian.*

Remark. Galois also proved that the converse holds. This boils down to proving the following: any finite Galois extension $K/\mathbb{Q}$ such that all composition factors of $\mathrm{Gal}(K/\mathbb{Q})$ are abelian can be enlarged to a radical extension of $\mathbb{Q}$. After next class you will have all the tools to prove this!

3. Insolvability of a specific quintic

We postpone the proof of Theorem 2.1 to next class. In the meantime, we illustrate the power of the theorem by using it to prove the insolvability of a specific polynomial in radicals. Consider the quintic

$$f(x) := x^5 - 4x - 2.$$

Note the following properties of f:

(1) it is irreducible (by Eisenstein),
(2) it is separable (since we're in characteristic 0 and it's irreducible), and
(3) it has precisely 3 real roots and 2 imaginary roots.

Claim. *The roots of f cannot be expressed using only radicals and field operations.*

Proof. We break the proof into three steps.

I. $\mathrm{Gal}(f) \simeq S_5$.

First, observe that $\mathrm{Gal}(f)$ must contain an element of order 5; see problem **11.4(a)**. Next, since f has precisely three real roots and two complex roots, $\mathrm{Gal}(f)$ must contain a transposition; see problem **11.4(b)**. It is important to note that if f has more than two complex roots, then $\mathrm{Gal}(f)$ might *not* contain a transposition!

II. Determine the composition factors of S_5.

First observe that the alternating group $A_5 \lhd S_5$. Furthermore, it turns out that A_5 is simple (see problem **11.1**). Combining this with the fact that $|S_5/A_5| = 2$, we deduce that

$$S_5 \rhd A_5 \rhd \{e\}$$

is a composition series for S_5, with composition factors $\mathbb{Z}/2\mathbb{Z}$ and A_5.

[1] This is essentially the error in Ruffini's work on the quintic.

III. Conclude by the Jordan-Hölder Theorem.

We see that the composition factors of Gal$(f) \simeq S_5$ aren't all abelian (since A_5 isn't). Theorem 2.1 implies that f isn't solvable in radicals. □

Remark. This proof works for any polynomial with Galois group isomorphic to S_n for any $n \geq 5$, since it can be shown that A_n is nonabelian and simple for all $n \geq 5$.

4. Proof of Galois' main insight

Our next result shows that if the ground field in a simple radical extension happens to contain an appropriate root of unity, then the extension is Galois and cyclic; note that an extension is called cyclic (or abelian or...) iff its Galois group is cyclic (or abelian or...). This justifies Galois' insight (1) under a suitable hypothesis.

Lemma 4.1. *Suppose α, $\zeta_n \in K$. Then $K(\alpha^{1/n})/K$ is Galois and cyclic.*

Proof. Note that $K(\alpha^{1/n})/K$ is a splitting field of $x^n - \alpha$ over K, which is a separable polynomial. (We can write down all its solutions explicitly.) It follows that $K(\alpha^{1/n})/K$ is Galois. Set $G :=$ Gal$(K(\alpha^{1/n})/K)$.

Now, pick any $\sigma \in G$. Since σ fixes K, we see that σ is completely determined by where it sends $\alpha^{1/n}$. We know that $\sigma(\alpha)$ is a root of $x^n - \alpha \in K[x]$, i.e. $\sigma(\alpha) = \zeta_n^k \alpha$ for some $k \in \mathbb{Z}/n\mathbb{Z}$. This gives us a natural map $G \to \mathbb{Z}/n\mathbb{Z}$ defined by $\sigma \mapsto k$. It's an exercise to check that this map is an injective homomorphism. Thus G embeds inside $\mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}/n\mathbb{Z}$ is cyclic, this implies that G must be cyclic. □