GALOIS THEORY: LECTURE 4

FEBRUARY 12, 2023

1. A Brief Review of S_n

Much of this course relies on familiarity with the symmetric group on n elements, denoted S_n (the group of all permutations of n elements). Here we collect some nice facts about S_n that will be particularly useful to us.

(1) Any element of the symmetric group S_n can be written in cycle notation. For example, in S_5, the permutation $(1\ 3\ 2\ 5)$ represents mapping $1 \mapsto 3$, $3 \mapsto 2$, $2 \mapsto 5$, $5 \mapsto 1$, and $4 \mapsto 4$. Products of cycles are evaluated right to left, so for example, $(1\ 3\ 2\ 5)(4\ 5)(1\ 4\ 3) = (2\ 5\ 4)$. Eli pointed out that it's right to left because it's function composition, with the right-most permutation serving as the inside function, the one that's evaluated first.

(2) Any $\sigma \in S_n$ can be expressed as a product of disjoint cycles (disjoint here means that the cycles do not permute the same elements). For example, the permutation $(1\,2)(2\,3)(4\,5)$ can be written as the following product of disjoint cycles: $(1\,2\,3)(4\,5)$.

(3) Any $\sigma \in S_n$ can be expressed as a product of transpositions (transpositions are 2-cycles).[1] For example, Zoe produced a factorization of the permutation $(1\,2\,3\,4)$:

$$(1\,2\,3\,4) = (1\,4)(1\,3)(1\,2).$$

This product is not unique, however—Jake and Felix proposed two other factorizations into transpositions:

$$(1\,2\,3\,4) = (1\ 2)(2\ 3)(3\ 4) = (2\ 3)(3\ 4)(1\ 4).$$

All of our factorizations thus far used three transpositions. It's tempting to conjecture that this is always the case, but Alex pointed out that this cannot be the case, since we can trivially modify any factorization to contain more transpositions, e.g.

$$(1\,2\,3\,4) = (1\,4)(1\,3)(1\,2)(1\,2)(1\,2)$$

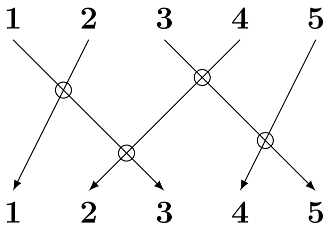
However, Jamie pointed out that the *parity* of the number of transpositions in the product remains the same, no matter which product of transpositions you choose to write σ as. This leads to the following definition:

Definition. $\sigma \in S_n$ is an *even* permutation iff σ can be expresssed as a product of an even number of transpositions; if not, we say σ is *odd.*

Here's a nice way to visualize the parity of a permutation (that Leo learned from John Conway). Suppose we wish to figure out the parity of $(1\ 3\ 5\ 4\ 2)$. We represent this permutation pictorially:

Summary of a lecture by Leo Goldmakher; typed by Jacob Lehmann Duke from notes by Shaurya Taxali.

[1] Here's a 'biological proof' of this that Leo learned from Brian Conrad: using two hands, we can rearrange a set of objects in whatever order we like!



There are four intersections of the arrows (circled in the picture). Conway's claim is that, since there is an even number of intersections, the permutation must be even! We can verify this using the definition:

$$(1\,3\,5\,4\,2) = (1\,2)(1\,4)(1\,5)(1\,3)$$

is a decomposition into an even number of transpositions.

(4) You might run across a different (but equivalent) way to express the parity of a permutation:

Definition. The *sign* (or *signature*) of $\sigma \in S_n$, denoted by $\operatorname{sgn}(\sigma)$, is the function $\operatorname{sgn} : S_n \to \{-1, 1\}$ given by

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

There are a few advantages to recasting the parity of a permutation in this language. For one thing, sgn is a group homomorphism (in fact, it's the *unique* nontrivial homomorphism $S_n \to \{\pm 1\}$; see this week's problem set). It is therefore an example of a *group character*, a concept that comes up in algebra, representation theory, number theory, and even chemistry. Thus, using the language of signature rather than parity allows us to apply the theory to other areas. Here's a nice example from number theory. Given a prime p and $a \in \mathbb{Z}_p$, let $m_a : \mathbb{Z}_p \to \mathbb{Z}_p$ denote multiplication by a; we can view m_a as a permutation living in S_p. In 1874, Zolotarev proved that $\operatorname{sgn}(m_a) = \left(\frac{a}{p}\right)$, the Legendre symbol (mod p). This leads to a beautiful proof of Quadratic Reciprocity; see Matt Baker's blog post on this, as well as a lovely generalization by Williams Duke and Kimberly Hopkins in the American Math Monthly.

(5) The set of all even permutations is a subgroup of S_n of index 2; hence, it is the largest proper subgroup of S_n. It has a fancy name:

Definition. The set of all even permutations in S_n is called A_n, the **alternating group.**

Observe that $A_n \trianglelefteq S_n$, since it is the kernel of the sgn map. (Here and throughout, $\trianglelefteq$ means "is a normal subgroup of".)

(6) The following result shows that symmetric groups are, in a sense, the most general type of group. Though this is not always the most useful way to think about a given group, it demonstrates that we can 'reduce' any question about abstract groups to a question about permutations.

Theorem 1 (Cayley's Theorem)**.** *For any finite group G, there exists some $n \in \mathbb{N}$ such that G can be embedded in S_n.*

By "embedded" we mean that there exists an injective homomorphism $G \hookrightarrow S_n$. Equivalently, this means G is isomorphic to a subgroup of S_n. A natural question is: given G, what's the smallest symmetric group one can embed it in? Although some upper bounds are known, this seems to be open!

2. Galois Theory in 30 Minutes

The following result will be a consequence of our work over the course of the semester:

Theorem 2 (Consequence of Galois theory)**.** *Given any polynomial $f(x)$, pick one of its roots r_f, and express it using only the coefficients of f, the four field operations, and radicals. There exists an algorithm which, given f, predicts the level of nesting of radicals in the expression.*

The goal of the rest of the lecture is to provide a sketch of this algorithm and run it on a couple examples. *Many* details and crucial insights will be missing, of course, but the point is to get a feel for how Galois theory works and what we are building towards. In brief, the algorithm is as follows:

(1) To each polynomial $f(x) \in \mathbb{Q}[x]$ we associate a certain group, called the "Galois group" of f and denoted by $\text{Gal}(f)$. It turns out that $\text{Gal}(f) \leq S_n$ where n is the degree of f. (Here and throughout, $\leq$ means "is a subgroup of").

   Remark. In general, finding the Galois group of a polynomial of f is hard and requires the use of a bunch of *ad hoc* tricks.

(2) Set $G_0 := \text{Gal}(f)$, and recursively define
$$G_n := [G_{n-1}, G_{n-1}]$$
for all integers $n > 0$.

(3) Let $\ell(f) := \min\{n \in \mathbb{N} : G_n \text{ is trivial}\}$.

What this algorithm tells us is: f has a root that can be expressed in terms of the coefficients of f, $+$, $-$, $\times$, $\div$, and $\ell(f)$ nesting of radicals. For example, if $\text{Gal}(f)$ is trivial, then $\ell(f) = 0$, which means that f has a root that can be expressed without using radicals at all. If $\text{Gal}(f)$ is not trivial but G_1 is, then $\ell(f) = 1$, which means that f has a root which can be expressed with just one radical. We will now fill in some of the missing details of this algorithm by actually running it on a couple of examples.

Example 1. Let $f(x) = x^4 - 5x^2 + 6$. To begin with, it is important to note that this is sort of a silly example, because we can actually find the roots of f quite simply by factoring. If we let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ denote the roots of f, we see that:
$$f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) = 0 \implies \alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}$$
The fact that we know the roots of f in advance makes running the algorithm simpler and easier to understand. In the next example, however, we will see an example of how to run the algorithm on a polynomial whose roots we do not know in advance.

Step 1 of the Galois Algorithm

The first step of the algorithm is to "produce the Galois group of f." Here's a heuristic explanation of how to do this. First, we need the notion of a "rational relation":

Definition. A *rational relation* among the roots of f is an equation involving only α_1, α_2, α_3, α_4, rational numbers, and the field operations: $+$, $-$, $\times$, $\div$.

So the first step to finding the Galois group of f is to write down all (non-redundant!) rational relations amongst its roots. For example, the following four equations are all rational relations of the roots of f:
$$(\alpha_1)^2 = 2 \qquad \alpha_1\alpha_2 = -2 \qquad (\alpha_3)^2 = 3 \qquad \alpha_1\alpha_2\alpha_3\alpha_4 = 6$$
There are other rational relations in addition to these, but they are redundant—they can be derived from the above four rational relations. For example, all of the following rational relations are true but redundant:
$$(\alpha_1)^4 = 4 \qquad (\alpha_2)^2 = 2 \qquad \frac{1}{2}(\alpha_3)^2 = \frac{3}{2} \qquad \alpha_1 + \alpha_2 = 0$$
We will not prove that the above four rational relations suffice (but see the extra credit on the problem set!). But it should seem at least vaguely intuitive that four equations could be enough to uniquely determine four unknowns, and hence any other rational relations we generate would be redundant.

Taking on faith that the four rational relations are a complete set, we can now construct the Galois group of f:

$$\boxed{\text{Gal}(f) \text{ is the set of permutations from } S_4 \text{ that leave all of our rational relations true.}}$$

For example, the permutation $(1\,2) \in S_4$ is an element of Gal(f) since if we replace α_1 with α_2 and α_2 with α_1 in all of the above rational relations, they remain true:

$$(\alpha_1)^2 = 2 \text{ becomes } (\alpha_2)^2 = 2 \text{ which is still true}$$
$$\alpha_1\alpha_2 = -2 \text{ becomes } \alpha_2\alpha_1 = -2 \text{ which is still true}$$
$$(\alpha_3)^2 = 3 \text{ stays the same, so it is trivially still true}$$
$$\alpha_1\alpha_2\alpha_3\alpha_4 = 6 \text{ becomes } \alpha_2\alpha_1\alpha_3\alpha_4 = 6 \text{ which is still true}$$

As a non-example, the permutation $(1\,3)$ is *not* an elemenet of Gal(f) since it transforms the first rational relation, $(\alpha_1)^2 = 4$, into $(\alpha_3)^2 = 4$, which is false. Going through and checking which of the $4! = 24$ permutations of S_4 are in Gal(f), we find

$$\text{Gal}(f) = \{(), (1\,2), (3\,4), (1\,2)(3\,4)\}.$$

On to Step 2!

Step 2 of the Galois Algorithm

Step 2 of the algorithm says to start computing commutator groups. First, we are supposed to let $G_0 :=$ Gal(f) and $G_1 := [G_0, G_0]$. Some thought shows that $\{(), (1\,2), (3\,4), (1\,2)(3\,4)\}$ is isomorphic to the Klein four-group, $\mathbb{Z}_2 \times \mathbb{Z}_2$. In particular, G_0 is abelian, which immediately implies that G_1 is trivial.

Step 3 of the Galois Algorithm

Per the algorithm's instructions, we now set $\ell(f) := \min\{n \in \mathbb{N} : G_n \text{ is trivial}\}$. From the previous step, we see that $\ell(f) = 1$, which implies that f has a root that can be expressed using non-nested radicals. Recall that in this example, we knew all the roots in advance, and sure enough: they all consist of a single, non-nested radical. Galois theory works!

Example 2. Let $g(x) = x^3 - 6x + 2$. In this example, we tackle the question: how do we generate rational relations when we do not know the roots of g in advance? As before, we denote the roots of g by α_1, α_2, α_3.

Step 1 of the Galois Algorithm

Since α_1, α_2, α_3 are the roots of g, we know that

$$\begin{aligned} g(x) = x^3 - 6x + 2 &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \\ &= x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_2)x - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

Notice, this equality generates a few rational relations automatically, even though we do not know the specific values of α_1, α_2, or α_3 in advance:

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= -6 \\ \alpha_1\alpha_2\alpha_3 &= -2 \end{aligned}$$

These are the only "obvious" rational relations; without knowing any further information about $\alpha_1, \alpha_2, \alpha_3$, we would be hard pressed to conjure another, non-redundant rational relation. But, as in the first example, we will proceed under the (unproved) assumption that it actually is impossible to generate any other, non-redundant rational relations.

Since all of these equations are symmetric (i.e. the equations remain identical even after permuting the roles of α_1, α_2, α_3), it turns out that every permutation in S_3 is an element of Gal(g). Thus, Gal$(g) = S_3$.

Step 2 of the Galois Algorithm

We set $G_0 := \text{Gal}(g) = S_3$, whence $G_1 := [S_3, S_3]$. From last week's problem set we know that $G_1 \simeq \mathbb{Z}_3$. In particular, G_1 is abelian, whence $G_2 := [G_1, G_1]$ is trivial.

Step 3 of the Galois Algorithm

Set $\ell(g) = \min\{n \in \mathbb{N} : G_n \text{ is trivial}\}$. From the previous step, we see that $\ell(g) = 2$. This means that g has a root that can be expressed using a 2-nesting of radicals. Indeed, recall from the previous lecture that one of the roots of g is $\sqrt[3]{-1 + \sqrt{-7}} + \sqrt[3]{-1 - \sqrt{-7}}$. Galois theory works again!

3. Revisiting the Insolvability of the Quintic

Now that we have a better understanding of how the Galois theory algorithm works, we can start to glean how it would demonstrate the insolvability of the quintic. Given a generic quintic polynomial, say $h(x)$, we would expect our rational relations to all be symmetric, as in the second example. If this were the case, it would imply that $\text{Gal}(h) = S_5$. It can be easily verified (with a short computer program) that $[S_5, S_5] = A_5$ and that $[A_5, A_5] = A_5$; the latter implies that $G_n = A_5$ for all $n \geq 1$. In particular, would expect $\ell(h)$ to "equal" infinity, meaning that there is no way to write down a root of h in terms of its coefficients, the field operations, and a finite nesting of radicals. Later on in the course, we will actually demonstrate this for a specific quintic polynomial: we'll show that $\text{Gal}(x^5 - x - 1) = S_5$.

Remark. In our second example and in our discussion of the insolvability of the quintic, we saw polynomials whose Galois group was in fact the entire symmetric group. It turns out that in general, 100% of degree n polynomials have their Galois group equal to S_n. *However, 100% does not mean "all"!* 100%, here, is a measure of density. That is to say, if we consider the set of all degree n polynomials, we can imagine listing out increasingly larger subsets of it. For each subset, we can calculate the percentage of polynomials whose Galois group equals S_n. If we calculate what these percentages tends towards in the limit, we see that they approach 100%. However, we'll see that there are infinitely many polynomials whose Galois group is not the full symmetric group.