FINAL
MATH 220C

Name: Jiajie (Jerry) Luo

Viewing the Galois group of Polynomials as a Permutation Group on its Roots

One of the more important results from group theory is Caley's theorem, which tells us that any finite group can be embedded into S_n, for some n. As Galois groups are indeed groups, we can say the same about Galois groups of polynomials. This itself is a rather dull fact. The more interesting thing about this is exactly what n needs to be. Let F be a field and let $f \in F[x]$. Let M be the splitting field of f. If f is a degree n polynomial, then we in fact have that the Galois group of f (ie. $Gal(M/F)$) can be viewed as a subgroup of S_n. More specifically, the Galois group permutes the roots of f.

In order for this to happen, we must describe how the Galois group acts on the roots of f. In particular, we need to show that given $\sigma \in Gal(M/F)$, σ maps roots of f to other roots of f. To see how this happens, let $f(x) = \sum_{i=0}^{n} a_i x^i$, and let α be a root. Since σ is a field automorphism (which means addition and multiplication is preserved) fixing elements in F, we see that $0 = \sigma(f(\alpha)) = \sum_{i=0}^{n} \sigma(a_i \alpha^i) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i = f(\sigma(\alpha))$, which tell that $\sigma(\alpha)$ is also a root of f. So, we see that indeed, elements of $Gal(M/F)$ maps roots of f to other roots of f.

Since we have $Gal(M/F)$ acting of the roots of f, let us now discuss the orbits of this action. To begin, let us show when this action is transitive. Suppose f was irreducible in F. Then we know that given any root α of f, $F(\alpha) \cong F[x]/(f(x))$ (sending $\bar{x} \mapsto \alpha$). In this case, we see that given roots α, α', we can define an isomorphism $\phi : F(\alpha) \to F(\alpha')$ where $\phi(a) = a$ for every $a \in F$ and $\alpha \mapsto \alpha'$. From here, we can extend f to an automorphism $\bar{f} : \bar{F} \to \bar{F}$, and since M is normal (ie. stable. This is because roots map to roots), we can restrict $\bar{f}$ to M, thus creating an automorphism of M that fixes F and maps $\alpha \mapsto \alpha'$ (this is by definition, an element of $Gal(M/F)$). Thus, we see that $Gal(M/F)$ acts transitively on the roots of f.

But what if f wasn't irreducible in F? Let $f = f_1 f_2 \cdots f_n$, where each f_i is irreducible with degree at least 1 and $n > 1$. Let us take any of the f_i's. We notice that as before, $Gal(M/F)$ maps roots of f_i to other roots of f_i (the argument from above still works). Here, we see that the action cannot be transitive, because each root α can only map to another root another root of f_i, where f_i it the polynomial that has α as a root. We notice that there's no 'funny business' happening, because if f_i and f_j has α as a shared root, we see that the $f_i = f_j$, because $irr_F(\alpha)$ must divide f_i and f_j, but f_i and f_j are irreducible themselves. This tells us that $Gal(M/F)$ acts transitively on the roots of f if and only if f is irreducible. That is, the orbit of a root α of f is all the roots that are roots of the irreducible polynomial of α.

It now makes sense to look at fields between M and F, and how they relate to subgroups of $Gal(M/F)$. Let L be an intermediate field between F and M (ie. $F \subset L \subset M$). Here, it is clear that $Gal(M/L) \subset Gal(M/F)$, as automorphisms of M fixing L also fix F. In fact, we see that as the intermediate field gets bigger, the Galois group of the extension gets smaller.

That is, if we have $F \subset K \subset L \subset M$, we have that $Gal(M/L) \subset Gal(M/K)$. From here, we see a relationship between how subfields L relate with their corresponding Galois group $Gal(M/L)$.

Let us now talk about how $Gal(M/L)$, which is a subgroup of $Gal(M/F)$, acts on the roots of f. To do this, we look at $f = f_1 \cdots f_n$, where the f_i's are irreducible factors of f as a polynomial of M. As before, we have that given any of the f_i's, elements of $Gal(M/L)$ map roots of f_i to other roots of f_i. We can similarly show that the $Gal(M/L)$ acts transitively on the roots of f_i. From this, we see that some of the $Gal(M/F)$-orbits in the will break up, according to how the corresponding irreducible factors of f over F factor as polynomials in L.

But is there any way we can talk about the 'other' Galois group - that is, given an intermediate field L, what can we say about $Gal(L/F)$ in respect to $Gal(M/F)$? Turns out there is. In fact, if L is a normal subgroup, we have that $Gal(M/L) \triangleleft Gal(M/F)$. Since we have normality in the group setting, it makes sense to look at the quotient group. We can actually show that $Gal(M/F)/Gal(M/L) \cong Gal(L/F)$. This tells us that given normality of an intermediate field L between F and M, we can find $Gal(L/F)$ as a quotient group.

But when exactly do we get a normal intermediate fields between F and M? Let us look at the case where $f = f_1 \cdots f_n$, where each f_i is irreducible (ie. when f is reducible). Clearly, the splitting field L_i of any of the f_i's gives us an intermediate field. We notice that L_i is in fact normal, because elements of $Gal(M/F)$ map roots of f_i to other roots of f_i, which is all contained in L_i. It is easy to see from here that taking product of the L_i's also give us normal intermediate fields.

Galois Correspondence in the Finite Separable Case

One of the intricacies of Galois theory is that it ties together group theory and field theory. In particular, given a field F, when we have a Galois field extension L, we have a inclusion reversing one-to-one correspondence between subfields of L containing F and subgroups of $Gal(L/F)$. This motivates the usage of the priming operation between intermediate fields of L and F, and subgroups of $Gal(L/F)$. That is, given $F \subset K \subset L$, we define K' as the subgroup of $Gal(L/F)$ fixing K. Similarly, given $H \subset Gal(L/F)$, we define H' to be the subfield of L fixed by H.

We know that when L is Galois, $G' = F$. In this case, we have some nice results, such as the following:

- Given intermediate fields $F \subset M \subset N \subset L$, we have that $[N : M] = [N' : M']$
- Given subgroups $\{e\} \subset J \subset H \subset Gal(L/F)$, we have that $[H : J] = [J' : H']$.

However, when L is not Galois, this need not be true. In particular, we have that $G' \neq F$ (by definition of Galois). An example of this is when we look at $\mathbb{Q}(\sqrt[3]{2})$. We see that $\sqrt[3]{2}$ is a root of the irreducible $x^3 - 2$, which means $\mathbb{Q}(\sqrt[3]{2})$ is a degree 3 extension of $\mathbb{Q}$. However, we see that in this case, the other roots of $x^3 - 2$ are $\zeta_3\sqrt[3]{2}$ and $\zeta_3^2\sqrt[3]{2}$, neither of which are real. Since roots of $x^3 - 2$ must map to other roots by $Gal(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q}))$, and $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of $\mathbb{R}$, while neither $\zeta_3\sqrt[3]{2}$ nor $\zeta_3^2\sqrt[3]{2}$ are contained in $\mathbb{R}$, we see that any element of $Gal(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q}))$ must map $\sqrt[3]{2}$ to itself, which means $Gal(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q}))$ is trivial. In this case, we see clearly that we do not have the one-to-one inclusion reversing corresponding lattice structure as we do in the Galois case, as $\mathbb{Q}(\sqrt[3]{2})$ is a nontrivial extension of $\mathbb{Q}$, while $Gal(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q}))$ is trivial.

The example above illustrates the following in the general (non-Galois) case:

- Given intermediate fields $F \subset M \subset N \subset L$, we have that $[N : M] \geq [N' : M']$
- Given subgroups $\{e\} \subset J \subset H \subset Gal(L/F)$, we have that $[H : J] \geq [J' : H']$.

One of the ways we can study Galois correspondence in the non-Galois separable case is to look at the Galois closure of our given field. That is, given L a finite extension of F, we can look at $F \subset L \subset M$, where M is the Galois closure of L. In this case, we have that M, which is Galois over F, is also Galois over L. One of the things we can do here is to look at how many ways we can embed L into M. The number of ways we can look at how L embeds into M gives us the $\sigma(L)$'s, for $\sigma \in Gal(M/L)$. Here, we see that given σ, we have that the subgroup of $Gal(M/F)$ fixing $\sigma(L)$ is $\sigma Gal(M/L)\sigma^{-1}$. In fact, we can show the converse of this too. One of the corollaries of this is that L is a normal (stable) extension if and only if $Gal(M/L)$, the fixed field of L in M, is normal in $Gal(M/F)$. In fact, when we have L being a normal extension of F, living inside the Galois closure M, then we have that $Gal(M/F)/L'$ is isomorphic to the automorphism in $Gal(L/F)$ that extend to M. From this, we are able to see that $Gal(M/F)/Gal(M/L) \cong Gal(L/F)$. However, the case that L is normal is unnecessary for the case that L is not a Galois extension, because if L is stable, then we can actually show that L is Galois over F.

By looking at the Galois closure of L, we're able to see "how much stuff is missing" in

the Galois group. For example, in our case of $\mathbb{Q}(\sqrt[3]{2})$, we're able to observe how missing roots of an irreducible polynomial can cause the Galois group to "collapse." In particular, given L and its Galois closure M, when we view L as a subfield of M, we can look at the fixed field of $Gal(L/F)$ in relation with $Gal(M/F)$ and $Gal(L/F)$. It makes sense to look at this, because towards the end of the last paragraph, we see that in the normal setting, we have $Gal(M/F)/Gal(M/L) \cong Gal(L/F)$. In the example of $\mathbb{Q}(\sqrt[3]{2})$, we see that the missing roots "takes away" from the structure of the Galois group $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, in that it ends up fixing everything in $\mathbb{Q}(\sqrt[3]{2})$. So, we see that the number of isomorphic fields L has in M (which corresponds to the conjugate subgroups of $Gal(M/L)$ in $Gal(M/F)$), in respect to the roots of the irreducible polynomial of the elements adjoined to obtain L, give us an idea "how many things are missing," with more isomorphic fields corresponding to more things "missing" in the Galois group. More specifically, the things "missing" are the roots of irreducible polynomials of elements in L, that are absent from L, and in extension, the automorphisms that would arise if they were present. This is consistent with fact that normal extensions in the separable setting is give us Galois fields, in a bigger Galois extension, there is only one conjugate subfield. Indeed, this also gives us intuition in the fact that the traditional definition of Galois (fixed field is the base field) is equivalent to being normal and separable, as well as being the splitting field of a separable polynomial.