Polynomials IV - Abel's Theorem and Applications

Yan Tao

March 2022

1 Solvable Groups

Recall that a subgroup H of a group G is called *normal* if $ghg^{-1} = h$ for all $h \in H$ and all $g \in G$. We write $H \triangleleft G$ when H is a normal subgroup of G.

Definition 1 *A group G is called **solvable** (or **soluble**) if there exist subgroups*

$$\{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_{n-1} \triangleleft G$$

such that the quotients G/G_{n-1}, G_{n-1}/G_{n-2}, ..., G_2/G_1, and $G_1/\{e\}$ are all abelian. (Usually, the trivial group is denoted G_0 and G itself is denoted G_n.)

Problem 1

- *Show that every abelian group is solvable.*

- *Show that the permutation group S_3 is solvable.*

- *(Challenge) Show that S_4 is solvable.*

- *Show that any subgroup of a solvable group is solvable.*

As Problem 1 shows, most groups that we could possibly think of are solvable. The most important example of a non-solvable group, and also the smallest, is the following group with 60 elements (think about why it has 60 elements!)

Definition 2 *To every permutation $\sigma \in S_n$, written in cycle notation, associate with it a number as follows:*

- *To a k-cycle, associate the number $k-1$.*
- *To the product of two permutations, associate the sum of their numbers.*

*σ is called **even** if this number is even, and **odd** if this number is odd.*

Let A_n be the subset of S_n containing all the even permutations.

Problem 2 *Show that A_n is a subgroup of S_n.*

A_n is called the *alternating group* on n elements (recall that S_n is called the *symmetric group*).

Theorem 1 *For $n \geq 5$, A_n is **simple** - that is, it has no normal subgroups besides the trivial subgroup and itself.*

Problem 3 *Show that A_5 is not solvable. Then show that S_5 is not solvable.*

2 The Abel-Ruffini Theorem

Last week we showed how to extend $\mathbb{Q}$ to larger number systems. The same process can be used to extend an extension of $\mathbb{Q}$, and so on.

Problem 4 *Suppose that L is an extension of K and M is an extension of L (and therefore also an extension of K). Show that $Gal(M/L) \triangleleft Gal(M/K)$.*

Problem 5 *Let K, L, M be as in the previous problem. Show that $Gal(M/K)/Gal(M/L) = Gal(L/K)$.*

Problem 6 *Show that for any number system K, $Gal(K/K)$ is the trivial group.*

We also state the following useful theorem (try to think about how you would prove this!)

Theorem 2 *If $L = K(\sqrt[n]{\alpha})$, where $\alpha \in K$ and this is any n^{th} root of α (i.e. using any n^{th} root of unity), then $Gal(L/K)$ is cyclic.*

Definition 3 *A polynomial is said to be* ***solvable in radicals*** *if there is a formula for each of its roots in terms of rational numbers and addition, subtraction, multiplication, division, and taking n^{th} roots.*

Problem 7 *Suppose that p is a polynomial which is irreducible over $\mathbb{Q}$ and solvable in radicals. Let x be a root of p.*

- *Let K be a splitting field for p. Show that there is a sequence*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_{n-1} \subseteq K_n = K$$

  where each K_j is an extension of K_{j-1} by the n^{th} root of an element of K_{j-1}. (Hint: Since p is solvable in radicals, x can be written in radicals, so construct $K_1, K_2, ...$ in a way that undoes all the radicals in the formula for x.)

- *Use this sequence and Problem 4 to obtain a sequence of normal subgroups of $Gal(K/\mathbb{Q})$.*

- *Conclude that $Gal(K/\mathbb{Q})$ is solvable.*

Problem 7 proves one direction of the famous Abel-Ruffini Theorem. The converse is also true, but is much trickier to prove so we shall not do so this week. To summarize, we have

Theorem 3 *(Abel-Ruffini) A polynomial p is solvable in radicals if and only if its Galois group is solvable.*

Problem 8 • *Using the fact that the cubic formula exists, prove that S_3 is solvable.*

• *Using the fact that S_4 is solvable (see Problem 1), prove that there exists a quartic formula.*

• *Can we immediately rule out the existence of a quintic formula? Why or why not?*

3 Transitive Subgroups and Quintics

So far we have restricted attention to irreducible polynomials, and it wasn't entirely clear why. There are a few proofs on this and the previous worksheet which require irreducibility (go back and see how), but the most important application is that it forces a certain property on the Galois group - the Galois group can't just be any subgroup of S_n.

Definition 4 *A subgroup G of S_n is* ***transitive*** *if any for two different numbers $1 \leq j, k \leq n$ there exists a permutation $\sigma \in G$ such that $\sigma(j) = k$.*

Problem 9 *Let p be an irreducible degree n polynomial. Prove that its Galois group is a transitive subgroup of S_n. (Hint: If it weren't transitive, there would be roots r_j and r_k which cannot be mapped to each other by the Galois group. Consider the set of roots which are mapped to from r_j, which is now missing some r_k, and use this set of roots to create a nontrivial factor of p.)*

Problem 10 *Consider the polynomial* $p(x) = x^5 - 13x - 13$*, and let* G *be its Galois group.*

- *Using Eisenstein's Criterion (recall from last quarter), show that* p *is irreducible over* $\mathbb{Q}$*.*

- *Show that* G *contains a transposition (a 2-cycle). (Hint: You may use the fact that* p *has exactly three real roots - this can be seen by graphing it.)*

- *Show that* G *contains all ten transpositions in* S_5*. (Hint: Say you have the transposition* $g = (12)$*. By transitivity there exists some* h *such that* $h(2) = 3$*, so what can* hgh^{-1} *possibly be? Repeat this process until you've shown that* $(13) \in G$*. Then do this again for* $(14), (15) \in G$*. Now can you get the other six transpositions in* G*?)*

- *Show that the transpositions generate* S_5*; that is, every permutation in* S_5 *can be written as a product of transpositions. (Hint: Every permutation can be written in cycle notation. Can you write a cycle as a product of transpositions?)*

- *Conclude that* p *is not solvable in radicals, and therefore that there is no quintic formula.*