Chapter 8

End game

Chapter 7 finished with a criterion, given as Fact 7.38, that can be used to show that a polynomial $p(x)$ is not solvable by radicals over $\mathbb{Q}$. It says that if $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ is *not* a solvable group, then $p(x)$ is not solvable by radicals over $\mathbb{Q}$. We are extremely close to our goal. Here begins the end game.

8.1 Solvable groups

To better understand how we might apply Fact 7.38, let's try to collect some examples of solvable groups as well as some examples of groups that are not solvable.

We'll initially focus on groups that have arisen as we studied $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ for various polynomials $p(x)$; here are the groups that we encountered.

- If $p(x) = (x^2 - 2)(x^2 + 1)$, then $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q}) \cong V_4$. See Problems 6.79 and 7.17.
- If $p(x) = x^4 + x^3 + x^2 + x + 1$, then $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q}) \cong \mathbb{Z}_4$. See Examples 6.73 and 7.16 and Problem 6.74.
- If $p(x) = x^3 - 2$, then $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q}) \cong S_3$. See Problems 7.10 and 7.18.

We know that each of the polynomials listed above are solvable by radicals, so by Fact 7.38, each of the associated automorphism groups must be solvable. However, let's see this directly from the definition of a solvable group (Definition 7.35). Since V_4 and $\mathbb{Z}_4$ are both abelian groups, the next theorem confirms that both groups are solvable.

Theorem 8.1. Every abelian group is a solvable group.

Let's address S_3 next. In showing S_3 is solvable, there are various theorems from group theory that are helpful. The next fact highlights one of them. Recall that $[G : H]$ denotes the *index* of H in G, which is the number of left cosets of H in G. In practice, $[G : H]$ is often computed using Lagrange's Theorem, which is also given below.

Fact 8.2. Suppose that G is a group, and $H \leq G$. If $[G : H] = 2$, then then $H \trianglelefteq G$.

Fact 8.3 (Lagrange's Theorem)**.** If G is a finite group and $H \leq G$, then $|G| = [G : H] \cdot |H|$.

Problem 8.4. Let's show that S_3 is a solvable group. Recall that $R = \{\mathrm{id}, (123), (132)\}$ is a subgroup of S_3. Consider the chain of subgroups

$$\{\mathrm{id}\} \leq R \leq S_3.$$

(1) Briefly explain why $\{\mathrm{id}\} \trianglelefteq R$.

(2) Use Fact 8.2 to explain why $R \trianglelefteq S_3$.

(3) Prove that R is abelian.

(4) Compute $|S_3/R|$. What familiar group is the S_3/R isomorphic to? Conclude that S_3/R is abelian.

(5) Use Definition 7.35 (and the previous parts) to show that S_3 is a solvable group.

Let's continue looking at the symmetric groups. Is S_4 solvable? What about S_5? Note that these questions are highly relevant to determining if a polynomial is solvable by radicals since Corollary 7.15 tells us that $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ is isomorphic to a subgroup of S_n where $n = \deg p(x)$.

Problem 8.5. Let's now show that S_4 is a solvable group. We'll focus on two special subgroups: the alternating group A_4, and the group $V = \{id, (12)(34), (13)(24), (14)(23)\}$. Recall that A_4 consists of those permutations that can be written as a product of an *even* number of transpositions. In particular, $V \leq A_4$. Also, exactly half of the elements of S_4 lie in A_4, so $|A_4| = 12$. Consider the chain of subgroups

$$\{\mathrm{id}\} \leq V \leq A_4 \leq S_4.$$

(1) Prove that $V \trianglelefteq A_4$. (In fact, something stronger holds: $V \trianglelefteq S_4$.)

(2) Use Fact 8.2 to explain why $A_4 \trianglelefteq S_4$.

(3) Prove that V is abelian.

(4) Compute $|A_4/V|$. What familiar group is A_4/V isomorphic to? Conclude that A_4/V is abelian.

(5) Compute $|S_4/A_4|$. What familiar group is S_4/A_4 isomorphic to? Conclude that S_4/A_4 is abelian.

(6) Use Definition 7.35 (and the previous parts) to show that S_4 is a solvable group.

Okay, so what about S_5? As we'll see, S_n is not solvable when $n \geq 5$, and this is *precisely* why there are degree 5 polynomials that are not solvable by radicals. Whoa. Let's start with a couple of lemmas.

Lemma 8.6. Let H be a group, and let $N \trianglelefteq H$. Suppose that H/N is abelian. Then for all $x, y \in H$, we have that $x^{-1}y^{-1}xy \in N$.

Lemma 8.7. Let $n \geq 5$. Let $(a,b,c) \in S_n$ be any 3-cycle. If d and e are such that $1 \leq d,e \leq n$ and a,b,c,d,e are all distinct, then $(a,b,c) = x^{-1}y^{-1}xy$ for $x = (a,d,b)$ and $y = (a,e,c)$.

We're now ready to show that S_n is not solvable when $n \geq 5$. The strategy is to argue by contradiction. If S_n is solvable, then there is a chain of subgroups $\{\mathrm{id}\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{k-1} \trianglelefteq H_k = S_n$ with each successive quotient an abelian group.

Working with the group $S_n/H_{k-1} = H_k/H_{k-1}$ and using Lemmas 8.6 and 8.7, we can try to show that all of the 3-cycles must be contained in H_{k-1}. Then, if H_{k-1} contains all of the 3-cycles, we can repeat the argument in the group H_{k-1}/H_{k-2} to show that all of the 3-cycles must be contained in H_{k-2}. Continuing on, we'll eventually arrive at a contradiction.

Theorem 8.8. If $n \geq 5$, then S_n is not a solvable group.

8.2 Checkmate

Let's take another look at a polynomial that's come up several times before:

$$s(x) = x^5 + 5x^4 - 5.$$

We know a little about $\mathrm{Aut}(\mathbb{Q}^{s(x)}/\mathbb{Q})$, but seemingly not so much. Let's set $A = \mathrm{Aut}(\mathbb{Q}^{s(x)}/\mathbb{Q})$, and review what we know about A.

I. By Corollary 7.15, A can be viewed as a subgroup of S_5.

II. By Problem 7.24 (which relied on Theorem 7.23), A contains a transposition.

But in fact, we know a bit more.

Problem 8.9. Let α be a root of $s(x)$. Recall that $s(x)$ is irreducible by EIC, so $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$ by Theorem 6.40.

(1) Use Fact 6.44 to explain why $[\mathbb{Q}^{s(x)}:\mathbb{Q}]$ is divisible by 5.

(2) Use Fact 7.9 to explain why $|A|$ is divisible by 5.

We'll now invoke an important result from group theory: Cauchy's Theorem. Note that Lagrange's Theorem (Fact 8.3) implies that the order of any element of a finite group divides the order of the group—Cauchy's Theorem can be viewed as a partial converse.

Fact 8.10 (Cauchy's Theorem)**.** Let p be a prime. If G is any finite group such that $|G|$ is divisible by p, then G contains an element of order p.

Applying Cauchy's Theorem to A (in light of Problem 8.9), we see that A has an element of order 5. Let's add this our list of observations from above.

III. A has an element of order 5.

It turns out that our list is quite restrictive. We know that A contains a transposition and an element of order 5, but then A also contains everything that those two elements generate. To explore what these elements generate, let's start by recalling a basic fact from group theory.

Fact 8.11. The set of transpositions is a generating set for S_n.

Fact 8.11 is a launching point for finding other generating sets for S_n. Here's another.

Fact 8.12. If $(a_1, a_2, \ldots, a_n)$ is any n-cycle in S_n, then $(a_1, a_2, \ldots, a_n)$ together with the transposition (a_1, a_2) generate S_n.

Fact 8.12 has an extremely important implication for us.

Theorem 8.13. The group S_5 is generated by any element of order 5 together with any transposition. Consequently, if a subgroup of S_5 contains both an element of order 5 and a transposition, then the subgroup is all of S_5.

So here we are. It's time to tie everything together to prove the Main Theorem. Combining our three observations above with Theorem 8.13, we see that A is isomorphic to S_5. Then Theorem 8.8 applies, and we find that A is *not* a solvable group. Finally, we invoke Fact 7.38.

Theorem 8.14. The polynomial $s(x) = x^5 + 5x^4 - 5$ is *not* solvable by radicals over $\mathbb{Q}$.

The End