Chapter 7

Galois theory

We finished Chapter 6 by computing automorphism groups of field extensions. We also began to connect the subfields of an extension field L of F to subgroups of $\mathrm{Aut}(L/F)$. We now narrow our focus on which types of extension fields we consider, and in doing so, we significantly sharpen what we can say about this connection. It will be lynchpin of our argument showing that not all polynomials over $\mathbb{Q}$ are solvable by radicals over $\mathbb{Q}$.

Also, from here on, we will exclusively focus on subfields of $\mathbb{C}$. This will streamline (and simplify) our work, but it will also slightly obscure the general theory. Which is to say, this is more the beginning of the story than the end.

7.1 Galois extensions and Galois groups

Definition 7.1. Let F be a subfield of $\mathbb{C}$, and let $p(x) \in F[x]$. Define $F^{p(x)}$ to be the subfield of $\mathbb{C}$ generated by F and all roots of $p(x)$; thus, $F^{p(x)} = F(r_1, \ldots, r_n)$ where $r_1, \ldots, r_n$ are all of the roots of $p(x)$ in $\mathbb{C}$.

For example, if $p(x) = x^5 - 1$, then by Theorem 3.24, the roots of $p(x)$ are $1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$, so $\mathbb{Q}^{p(x)} = \mathbb{Q}(1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4)$.

Problem 7.2. Let $p(x) = x^5 - 1$. Use Theorem 3.68 to explain why $\mathbb{Q}^{p(x)} = \mathbb{Q}(\zeta_5)$.

Problem 7.3. Let $p(x) = x^3 - 2$. Explain why $\mathbb{Q}^{p(x)} \neq \mathbb{Q}(\sqrt[3]{2})$.

Problem 7.4. For each field F below, find a polynomial $p(x) \in \mathbb{Q}[x]$ such that $F = \mathbb{Q}^{p(x)}$.

(1) $F = \mathbb{Q}(\sqrt{2})$

(2) $F = \mathbb{Q}(\sqrt{2}, i)$

(3) $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

(4) $F = \mathbb{Q}(\zeta_{12})$

Definition 7.5. Let $F \subseteq K$ be subfields of $\mathbb{C}$.

(1) We say that K is a **Galois extension** of F if $K = F^{p(x)}$ for some $p(x) \in F[x]$.

(2) If K is a Galois extension of F, then $\mathrm{Aut}(K/F)$ is called the **Galois group** of K over F.

Revisiting Problem 7.4 with this new terminology, we see that each of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, and $\mathbb{Q}(\zeta_{12})$ are Galois extensions of $\mathbb{Q}$. Also, Problem 7.3 hints at the fact that $\mathbb{Q}(\sqrt[3]{2})$ might not be a Galois extension of $\mathbb{Q}$ (but there is more to prove to establish that).

Let's generalize parts of Problem 7.4 and record some types of extensions that are always Galois.

Theorem 7.6. Let $a \in \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{a})$ is a Galois extension of $\mathbb{Q}$.

Theorem 7.7. Let n be a positive integer. Then $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$.

As mentioned above, $\mathbb{Q}(\sqrt[3]{2})$ might not be a Galois extension of $\mathbb{Q}$, but it is true that $F(\sqrt[3]{2})$ a Galois extension of F provided F contains ζ_3. The next theorem addresses this.

Theorem 7.8. Let F be a subfield of $\mathbb{C}$. Suppose that $r \in \mathbb{C}$ and $r^n \in F$ for some positive integer n. If $\zeta_n \in F$, then $F(r)$ is a Galois extension of F.

7.1.1 Size of Galois groups

The next fact highlights the importance of Galois extensions. The point is roughly that the automorphism group of a Galois extension has the "expected" number of automorphisms; whereas, automorphism groups of non-Galois extension will necessarily have fewer.

Fact 7.9. Let $F \subseteq K$ be subfields of $\mathbb{C}$. If K is a Galois extension of F, $|\mathrm{Aut}(K/F)| = [K : F]$.

Fact 7.9 is extremely powerful. Let's start by seeing how it can help streamline the computation of certain automorphism groups.

Problem 7.10. Let $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Let's determine $\mathrm{Aut}(L/\mathbb{Q})$. Recall from Problem 7.4 that L is a Galois extension of $\mathbb{Q}$.

(1) What is minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}$? Why?

(2) What is minimal polynomial for ζ_3 over $\mathbb{Q}(\sqrt[3]{2})$? Why?

(3) Use Fact 6.44 to explain why $[L : \mathbb{Q}] = 6$.

(4) Let $\phi \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$. Use Theorem 6.61 to explain why there are only 3 choices for $\phi(\sqrt[3]{2})$ and only two choices for ζ_3. What are they?

(5) Complete the table of possible elements of $\mathrm{Aut}(L/\mathbb{Q})$.

	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
$\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$					
$\zeta_3 \mapsto$	ζ_3					

(6) Use Fact 7.9 to explain why every function in the table above must be in $\mathrm{Aut}(L/\mathbb{Q})$.

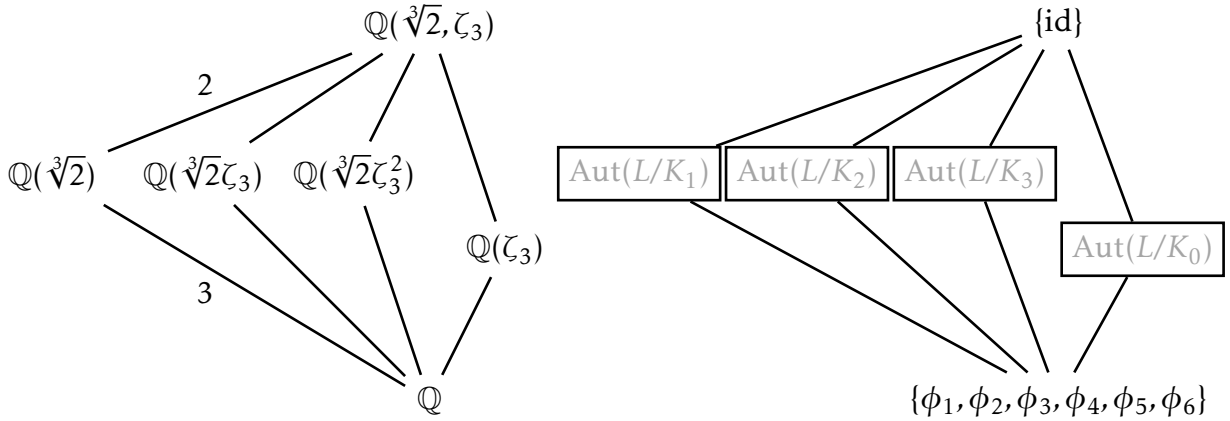
Problem 7.11. Let's revisit $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ from Problem 7.10 and connect subfields of L with subgroups of $\mathrm{Aut}(L/\mathbb{Q})$ using Theorem 6.72. The following are subfields of L.

$$K_0 = \mathbb{Q}(\zeta_3) \quad K_1 = \mathbb{Q}(\sqrt[3]{2}) \quad K_2 = \mathbb{Q}(\sqrt[3]{2}\zeta_3) \qquad K_3 = \mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$$

(1) Compute $\mathrm{Aut}(L/K_0)$, $\mathrm{Aut}(L/K_1)$, $\mathrm{Aut}(L/K_2)$, and $\mathrm{Aut}(L/K_3)$ by determining which of $\phi_1, \ldots, \phi_6$ are in each one.

(2) Use Theorem 6.72 to organize your findings by writing the appropriate elements in the boxes in the subgroup lattice of $\mathrm{Aut}(L/\mathbb{Q})$.

- Label the degree of each field extension on the lines of the lattice on the left. Fact 6.44 should help. A couple have been done for you.
- Label the order and index of each subgroup on the lines of the lattice on the right.



(3) What familiar group is $\mathrm{Aut}(L/\mathbb{Q})$ isomorphic to?

Problem 7.12. Use Fact 7.9 and Problem 6.77 to argue that $\mathbb{Q}(\sqrt[3]{2})$ is *not* a Galois extension of $\mathbb{Q}$

7.1.2 Galois groups as permutation groups

We now explore how to look at Galois groups as groups of permutations. The key, yet again, is Theorem 6.61. We begin by recalling a some definitions from group theory.

Definition 7.13. Let X be a set. A bijection from X to X is called a **permutation** of X. The set of all permutations of X is denoted $\mathrm{Sym}(X)$. The set of all permutations of $\{1, \ldots, n\}$ is usually denoted by S_n (instead of $\mathrm{Sym}(\{1, \ldots, n\})$).

Recall that, for any set X, $\mathrm{Sym}(X)$ is a group with respect to function composition. The identity is the identity function, denoted id.

Theorem 7.14. Let F be a subfield of $\mathbb{C}$. Let $p(x) \in F(x)$ be a polynomial of degree n, and let $R = \{r_1, \ldots, r_n\}$ be the set of all of roots of $p(x)$ in $\mathbb{C}$. Then

(1) for all $\phi \in \mathrm{Aut}(F^{p(x)}/F)$, restricting the domain of ϕ to R yields a permutation of R;

(2) the map $\mathrm{Aut}(F^{p(x)}/F) \to \mathrm{Sym}(R)$ that restricts the domain of each automorphism to R is an injective homomorphism.

Consequently, $\mathrm{Aut}(F^{p(x)}/F)$ is isomorphic to a subgroup of $\mathrm{Sym}(R)$.

Corollary 7.15. Let F be a subfield of $\mathbb{C}$. Let $p(x) \in F(x)$ be a polynomial of degree n. Then $\mathrm{Aut}(F^{p(x)}/F)$ is isomorphic to a subgroup of S_n.

To view $\mathrm{Aut}(F^{p(x)}/F)$ as a subgroup of S_n, we just need to label the roots of $p(x)$ by $1,\ldots,n$ in some way and then record how each element of $\mathrm{Aut}(F^{p(x)}/F)$ permutes the roots. Let's take a look at an example of this.

Example 7.16. Similar to Problem 7.2, we can see that $\mathbb{Q}(\zeta_5) = \mathbb{Q}^{p(x)}$ for $p(x) = x^4 + x^3 + x^2 + x + 1$. We know that the set of roots of $p(x)$ is $R = \{\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$.

By Corollary 7.15, $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is isomorphic to a subgroup of S_4 because $p(x)$ has degree 4 (hence 4 roots to permute). Let's find an explicit isomorphism. Recall from Example 6.73 that the elements of $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ are defined by the following table.

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
$\zeta_5 \mapsto$	ζ_5	ζ_5^2	ζ_5^3	ζ_5^4

Now let's expand the table to see how the automorphisms operate on all roots of $p(x)$.

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
$\zeta_5 \mapsto$	ζ_5	ζ_5^2	ζ_5^3	ζ_5^4
$\zeta_5^2 \mapsto$	ζ_5^2	ζ_5^4	ζ_5	ζ_5^3
$\zeta_5^3 \mapsto$	ζ_5^3	ζ_5	ζ_5^4	ζ_5^2
$\zeta_5^4 \mapsto$	ζ_5^4	ζ_5^3	ζ_5^2	ζ_5

Next, let's identify the roots with the numbers 1 up to 4 as follows.

$$\zeta_5 \leftrightarrow 1 \quad \zeta_5^2 \leftrightarrow 2 \quad \zeta_5^3 \leftrightarrow 3 \quad \zeta_5^4 \leftrightarrow 4.$$

Then the previous table becomes as follows.

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
$1 \mapsto$	1	2	3	4
$2 \mapsto$	2	4	1	3
$3 \mapsto$	3	1	4	2
$4 \mapsto$	4	3	2	1

So, using our labeling of the four roots, we can view $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ as a subgroup of S_4. If we write the permutation using cycle notation, we have

$$\phi_1 = \mathrm{id} \quad \phi_2 = (1243) \quad \phi_2 = (1342) \quad \phi_4 = (14)(23).$$

Problem 7.17. Let's look at Problem 6.79 again. Notice that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}^{p(x)}$ for $p(x) = (x^2-2)(x^2+1)$, and the set of roots of $p(x)$ are $R = \{\sqrt{2}, -\sqrt{2}, i, -i\}$.

(1) Fill in the extended table below to list how the elements of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ operate on the elements of R. Two of the lines were completed for you.

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
$\sqrt{2} \mapsto$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$-\sqrt{2} \mapsto$				
$i \mapsto$	i	$-i$	i	$-i$
$-i \mapsto$				

(2) Label the roots of $p(x)$ via: $\sqrt{2} \leftrightarrow 1$, $-\sqrt{2} \leftrightarrow 2$, $i \leftrightarrow 3$, and $-i \leftrightarrow 4$. Write each element of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ as a permutation in S_4 using cycle notation as in Example 7.16.

Problem 7.18. Let's revisit Problem 7.10. Set $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. We've seen that $L = \mathbb{Q}^{p(x)}$ for $p(x) = x^3 - 2$, and the set of roots of $p(x)$ are $R = \{\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\}$.

(1) Fill in the extended table below to list how the elements of $\mathrm{Aut}(L/\mathbb{Q})$ operate on the elements of R. For the first two lines, use what you wrote in Problem 7.10.

	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
$\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$					
$\zeta_3 \mapsto$	ζ_3					
$\sqrt[3]{2}\zeta_3 \mapsto$						
$\sqrt[3]{2}\zeta_3^2 \mapsto$						

(2) Label the elements of R as follows: $\sqrt[3]{2} \leftrightarrow 1$, $\sqrt[3]{2}\zeta_3 \leftrightarrow 2$, and $\sqrt[3]{2}\zeta_3^2 \leftrightarrow 3$. Write each element of $\mathrm{Aut}(L/\mathbb{Q})$ as a permutation in S_3 using cycle notation as in Example 7.16.

Let's apply the many things that we've learned to a very specific map: complex conjugation (which sends $z \mapsto \overline{z}$). Remember that we know a lot about this map. In Chapter 5, we noted that complex conjugation yields an isomorphism from $\mathbb{C}$ to $\mathbb{C}$, and in Problem 6.60, we saw that it fixes every real number.

We'll investigate complex conjugation when we restrict the domain to a subfield K of $\mathbb{C}$. Let γ denote complex conjugation. As γ is a homomorphism and is injective (so $\ker\gamma = \{0\}$), the First Isomorphism Theorem tells us that γ gives an isomorphism of K with its image under γ (i.e. $K \cong \gamma(K)$). Additionally, if $K = \gamma(K)$, then γ will be an *automorphism* of K, and the next theorem identifies one situation where this always happens.

Theorem 7.19. Let $p(x) \in \mathbb{Q}[x]$, and let $R = \{r_1, \ldots, r_n\}$ be the set of all of roots of $p(x)$ in $\mathbb{C}$. If γ is the complex conjugation map defined via $\gamma(z) = \overline{z}$, then

(1) restricting the domain of γ to R yields a permutation of R, and

(2) $\gamma \in \mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$.

Problem 7.20. Let $p(x) = (x^2-2)(x^2+1)$. Theorem 7.19 says that the complex conjugation map is in $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$. Look back at Problem 7.17 and determine which element of $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ corresponds to complex conjugation. Write your answer in cycle notation as in Problem 7.17.

Problem 7.21. Repeat Problem 7.20 for $p(x) = x^3 - 2$. Use Problem 7.18 to determine which element of $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ corresponds to complex conjugation. Write your answer in cycle notation as in Problem 7.18.

Problem 7.22. Repeat Problem 7.20 for $p(x) = x^4 + x^3 + x^2 + x + 1$. Use Example 7.16 to determine which element of $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ corresponds to complex conjugation. Write your answer in cycle notation as in Example 7.16.

The similarities and difference between our answers to Problems 7.20–7.22 hint at the following theorem.

Theorem 7.23. Let $p(x) \in \mathbb{Q}[x]$, and suppose that $p(x)$ has exactly two roots in $\mathbb{C}$ that are not in $\mathbb{R}$. Then when viewing $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ as permutations of the roots of $p(x)$, $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ contains a transposition.

Problem 7.24. Consider $p(x) = x^5 + 5x^4 - 5 \in \mathbb{Q}[x]$. Graph $p(x)$ or use calculus to show that $p(x)$ has exactly 3 roots in $\mathbb{R}$, and use Theorem 7.23 to conclude that when $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ is viewed as permutations of the 5 roots of $p(x)$, $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ contains a transposition.

7.2 Fundamental theorem of Galois theory

We finally arrive at the main course. Looking back at Problems 6.80 and 7.11, we see that there is a tight connection between subfields of an extension field L of F to subgroups of $\mathrm{Aut}(L/F)$. However, the extensions we considered in those problems where not just any extensions of $\mathbb{Q}$, they were *Galois extensions*. And in fact, the connection broke down for $\mathbb{Q}(\sqrt[3]{2}$ in Problem 6.77 where we saw that $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$, but as noted in Problem 7.12, this is *not* a Galois extension of $\mathbb{Q}$.

As it turns out, the connection we observed between subfields and subgroups holds for all Galois extensions, and the Fundamental Theorem of Galois Theory makes this explicit. Let's quickly establish some notation.

Notation 7.25. Let F be a subfield of L, and let G be a group. Define

- $\textsc{Sub}(L/F)$ to be the set of all subfields K such that $F \subseteq K \subseteq L$, and
- $\textsc{Sub}(G)$ to be the set of all subgroups of G.

The set $\textsc{Sub}(L/F)$ can be concisely read as "the set of subfields of L containing F"; for example, $\mathbb{Q}(\zeta_3) \in \textsc{Sub}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$. Also, recall that we have drawn the lattices associated to $\textsc{Sub}(L/F)$ and $\textsc{Sub}(\mathrm{Aut}(L/F))$ (the latter upside down) in several problems before.

There is a lot it digest when reading the Fundamental Theorem of Galois Theory, but remember that we have observed almost all of it in previous problems. It may be valuable to look back at Problem 7.11 while reading the theorem. Anyway, here we go...

Fact 7.26 (Fundamental Theorem of Galois Theory (for $\mathbb{C}$))**.** Let $F \subseteq L$ be subfields of $\mathbb{C}$. Assume that L is a Galois extension of F.

(1) The following maps are bijections and inverses of each other.

- $\textsc{Sub}(L/F) \to \textsc{Sub}(\mathrm{Aut}(L/F))$ defined by $K \mapsto \mathrm{Aut}(L/K)$,
- $\textsc{Sub}(\mathrm{Aut}(L/F)) \to \textsc{Sub}(L/F)$ defined by $H \mapsto \mathrm{Fix}_L(H)$

(2) The map $K \mapsto \mathrm{Aut}(L/K)$

- reverses inclusions: $K_1 \subseteq K_2$ if and only if $\mathrm{Aut}(L/K_2) \subseteq \mathrm{Aut}(L/K_1)$ and
- sends Galois extensions to normal subgroups: K is a Galois extensions of F if and only if $\mathrm{Aut}(L/K) \trianglelefteq \mathrm{Aut}(L/F)$.

Moreover, if K is a Galois extension of F, then $\mathrm{Aut}(K/F) \cong \mathrm{Aut}(L/F)/\mathrm{Aut}(L/K)$.

(3) For all $K \in \textsc{Sub}(L/F)$,

- $[L : K] = |\mathrm{Aut}(L/K)|$,
- $[K : F] = |\mathrm{Aut}(L/F) : \mathrm{Aut}(L/K)|$, and

Note that since $H \mapsto \mathrm{Fix}_L(H)$ is the inverse of $K \mapsto \mathrm{Aut}(L/K)$, $H \mapsto \mathrm{Fix}_L(H)$ is also inclusion reversing and it sends normal subgroups to Galois extensions.

Let's revisit Problems 6.80 and 7.11 yet again and highlight the connection between Galois extensions and normal subgroups in part (2) of Fact 7.26.

Problem 7.27. Look back at Problem 6.80. Use what you learned in group theory to determine which subgroups of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ are normal subgroups. Then use Fact 7.26(2) to determine which subfields of $\mathbb{Q}(\sqrt{2}, i)$ are Galois extensions of $\mathbb{Q}$. You can check you answers by directly verifying which extensions are Galois using the definition.

Problem 7.28. Repeat Problem 7.27 for $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$. Look at Problem 7.11, and determine which subgroups of $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$ are normal subgroups. Then use Fact 7.26(2) to determine which subfields of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ are Galois extensions of $\mathbb{Q}$.

7.3 A criterion for solvability by radicals

Let's try to apply Galois theory to the problem of determining if a polynomial is solvable by radicals or not. Recall that $p(x) \in \mathbb{Q}[x]$ is *solvable by radicals* over $\mathbb{Q}$ if all of the roots of $p(x)$ are contained in some radical extension of $\mathbb{Q}$; notice that this is the same as requiring that $\mathbb{Q}^{p(x)}$ is contained in some radical extension of $\mathbb{Q}$.

We'll first take a closer look at radical extensions of $\mathbb{Q}$ and then we'll investigate the implications for $\mathbb{Q}^{p(x)}$. Of course, our goal is to find a criterion that we can use to show that some $p(x)$ is *not* solvable by radicals.

7.3.1 Radical extensions, take 2

Let K be any radical extension of $\mathbb{Q}$. Thus, there exist nonzero elements $r_1, r_2, \ldots, r_m \in \mathbb{C}$ and positive integers $n_1, n_2 \ldots, n_m$ such that $K = \mathbb{Q}(r_1, r_2, \ldots, r_m)$, and

$$r_1^{n_1} \in \mathbb{Q}, r_2^{n_2} \in \mathbb{Q}(r_1), r_3^{n_3} \in \mathbb{Q}(r_1, r_2), \ldots, r_m^{n_m} \in \mathbb{Q}(r_1, \ldots, r_{m-1}).$$

Now, K might not be a Galois extension of $\mathbb{Q}$, so we'll try to expand K to a possibly larger radical extension L in such a way that L is a Galois extension of $\mathbb{Q}$ *and* that, as we iteratively add in elements, each field in the sequence is a Galois extension of the one that comes before it. Let's consider

$$L = \mathbb{Q}(\zeta_{n_1}, r_1, \zeta_{n_2}, r_2, \ldots, \zeta_{n_m}, r_m).$$

Lemma 7.29. The field L is a radical extension of $\mathbb{Q}$ and $K \subseteq L$.

Let's now look at L as a series of extensions. Note that our definitions of L_i and F_i below imply that $L_i = F_i(r_i)$ and $F_i = L_{i-1}(\zeta_{n_i})$.

$$\begin{array}{c}
L = L_m = \mathbb{Q}(\zeta_{n_1}, r_1, \zeta_{n_2}, r_2, \ldots, \zeta_{n_{m-1}}, r_{m-1}, \zeta_{n_m}, r_m) \\
\cup\!| \\
F_m = \mathbb{Q}(\zeta_{n_1}, r_1, \zeta_{n_2}, r_2, \ldots, \zeta_{n_{m-1}}, r_{m-1}, \zeta_{n_m}) \\
\cup\!| \\
\vdots \\
\cup\!| \\
L_2 = \mathbb{Q}(\zeta_{n_1}, r_1, \zeta_{n_2}, r_2) \\
\cup\!| \\
F_2 = \mathbb{Q}(\zeta_{n_1}, r_1, \zeta_{n_2}) \\
\cup\!| \\
L_1 = \mathbb{Q}(\zeta_{n_1}, r_1) \\
\cup\!| \\
F_1 = \mathbb{Q}(\zeta_{n_1}) \\
\cup\!| \\
L_0 = \mathbb{Q}
\end{array}$$

The next task to to show that each field in the sequence is a Galois extension of the one below it—Theorems 7.7 and 7.8 do most of the work.

Lemma 7.30. Each L_i is a Galois extension of F_i, and each F_i is a Galois extension of L_{i-1}.

We now apply the Fundamental Theorem of Galois Theory to our chain of extensions. Importantly, Fact 7.26(2), implies that $\mathrm{Aut}(L/L_i) \trianglelefteq \mathrm{Aut}(L/F_i)$ and $\mathrm{Aut}(L/L_i)/\mathrm{Aut}(L/F_i) \cong \mathrm{Aut}(L_i/F_i)$. A similar statement holds for each extension F_i over L_{i-1}, and we get the following picture.

$$
\begin{array}{ll}
L = L_m & \{\mathrm{id}\} \\
\cup\mathrel{|} & \mathrel{|}\triangle \quad \Big\} \cong \mathrm{Aut}(L/F_m) \\
F_m & \mathrm{Aut}(L/F_m) \\
\cup\mathrel{|} & \mathrel{|}\triangle \\
\vdots & \vdots \qquad\qquad \vdots \\
\cup\mathrel{|} & \mathrel{|}\triangle \\
L_2 & \mathrm{Aut}(L/L_2) \\
\cup\mathrel{|} & \mathrel{|}\triangle \quad \Big\} \cong \mathrm{Aut}(L_2/F_2) \\
F_2 & \mathrm{Aut}(L/F_2) \\
\cup\mathrel{|} & \mathrel{|}\triangle \quad \Big\} \cong \mathrm{Aut}(F_2/L_1) \\
L_1 & \mathrm{Aut}(L/L_1) \\
\cup\mathrel{|} & \mathrel{|}\triangle \quad \Big\} \cong \mathrm{Aut}(L_1/F_1) \\
F_1 & \mathrm{Aut}(L/F_1) \\
\cup\mathrel{|} & \mathrel{|}\triangle \quad \Big\} \cong \mathrm{Aut}(F_1/\mathbb{Q}) \\
L_0 = \mathbb{Q} & \mathrm{Aut}(L/\mathbb{Q})
\end{array}
$$

We'll now investigate the structure of each of the corresponding Galois groups, starting with $\mathrm{Aut}(L_i/F_i)$.

Lemma 7.31. Consider the field $L_i = F_i(r_i)$. The minimal polynomial of r_i over F_i is a factor of $x^{n_i} - r^{n_i}$, so the possible elements of $\mathrm{Aut}(L_i/F_i)$ are described by the following table.

	id	ϕ_1	ϕ_2	ϕ_3	$\cdots$	ϕ_{m-1}
$r_i \mapsto$	r_i	$r_i\zeta_{n_i}$	$r_i\zeta_{n_i}^2$	$r_i\zeta_{n_i}^3$	$\cdots$	$r_i\zeta_{n_i}^{m-1}$

Corollary 7.32. The group $\mathrm{Aut}(L_i/F_i)$ is abelian.

We now investigate $\mathrm{Aut}(F_i/L_{i-1})$ and obtain a similar result.

Lemma 7.33. Consider the field $F_i = L_{i-1}(\zeta_{n_i})$. The minimal polynomial of ζ_{n_i} over L_{i-1} is a factor of $x^{n_i} - 1$, and the possible elements of $\mathrm{Aut}(F_i/L_{i-1})$ are described by the following table.

	id	ϕ_2	ϕ_3	$\cdots$	ϕ_{n_i-1}
$\zeta_{n_i} \mapsto$	ζ_{n_i}	$\zeta_{n_i}^2$	$\zeta_{n_i}^3$	$\cdots$	$\zeta_{n_i}^{n_i-1}$

Corollary 7.34. The group $\mathrm{Aut}(F_i/L_{i-1})$ is abelian.

We've learned a lot about L, or, more specifically, about $\mathrm{Aut}(L\mathbb{Q})$. We see now that $\mathrm{Aut}(L/\mathbb{Q})$ has a chain of subgroups, each normal in the next, such that the corresponding quotient groups are abelian. Let's name this property.

Definition 7.35. Let G be a group with identity 1. We say that G is a **solvable** group if there exists a chain of subgroups

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_k = G$$

such that for all $1 \leq i \leq k$, the quotient group H_i/H_{i-1} is abelian.

Using this new language, we can summarize our findings above as follows.

Fact 7.36. If $p(x) \in \mathbb{Q}[x]$ is solvable by radicals over $\mathbb{Q}$, then $\mathbb{Q}^{p(x)}$ is contained in a subfield L of $\mathbb{C}$ for which

(1) L is a Galois extension of $\mathbb{Q}$, and

(2) $\mathrm{Aut}(L/\mathbb{Q})$ a solvable group.

7.3.2 The criterion

Notice that Fact 7.36 tells us a lot about L, but on the surface, it doesn't seem to address $\mathbb{Q}^{p(x)}$. However, by the definition of $\mathbb{Q}^{p(x)}$, we know that $\mathbb{Q}^{p(x)}$ is a Galois extension of $\mathbb{Q}$.

Applying the Fundamental Theorem of Galois Theory (specifically Fact 7.26(2)) to the sequence $\mathbb{Q} \subseteq \mathbb{Q}^{p(x)} \subseteq L$, we find that $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q}) \cong \mathrm{Aut}(L/\mathbb{Q})/\mathrm{Aut}(L/\mathbb{Q}^{p(x)})$. Thus, $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ is isomorphic to a quotient group of $\mathrm{Aut}(L/\mathbb{Q})$. The following fact from group theory now applies.

Fact 7.37. Suppose that G is a solvable. Then every subgroup of G and every quotient group of G is also a solvable group.

The implication is that if $\mathrm{Aut}(L/\mathbb{Q})$ is a solvable group, then $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ is also a solvable group. Putting everything together, we get the following lovely (and quite useful) test to determine if a polynomial is solvable by radicals.

Fact 7.38 (Solvability by Radicals Criterion)**.** If $p(x) \in \mathbb{Q}[x]$ is solvable by radicals over $\mathbb{Q}$, then $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ a solvable group.

So, if we can find some $p(x) \in \mathbb{Q}[x]$ for which $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ is *not* a solvable group, then we will be able to conclude that $p(x)$ is *not* solvable by radicals over $\mathbb{Q}$.

Incidentally, the converse of Fact 7.38 is also true! This means that $p(x) \in \mathbb{Q}[x]$ is solvable by radicals over $\mathbb{Q}$ *if and only if* $\mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$ a solvable group.