Chapter 4

Solvability by Radicals

Our overarching goal, as laid out in Chapter 2, is to find a polynomial whose roots can **not** be expressed in terms of the coefficients of the polynomial using just the operations of addition, subtraction, multiplication, division, and the extraction of roots. Or, in other words, we are searching for a polynomial that is **not** solvable by radicals, a term that we have only defined informally so far. Laying out a formal definition of solvability by radicals (and trying to wrap our head around it) is the main goal of this chapter.

4.1 Radical extensions

The notion of "solvable by radicals" is about how we may express the roots of a polynomial. We start by formalizing the notion that "a number can be expressed in terms of other numbers using just the operations of addition, subtraction, multiplication, division, and the extraction of roots." In the next section, we apply this to roots of polynomials.

Now, when we define what it means for a number to be built using the various operations listed above, we need to capture the possibility that we may need "iterated roots" to express a number. For example, consider

$$\alpha = \sqrt{2} + \sqrt[3]{-1 + \sqrt{2}}.$$

To see that α can be expressed using addition, subtraction, multiplication, division, and the extraction of roots, we first note that the number $\beta = -1 + \sqrt{2}$ can be built using addition and a square root; we then arrive at α by taking a cube root of β and adding $\sqrt{2}$.

Let's begin to formalize this by introducing fields. Our observations above imply that α can be built using field operations from $\sqrt[3]{\beta}$ and $\sqrt{2}$, and β in turn can be built using field operations from $\sqrt{2}$. Thus, $\alpha \in \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{\beta}\right)$ and $\beta \in \mathbb{Q}\left(\sqrt{2}\right)$. The lattice looks like this.

$$\begin{array}{rc} \alpha \in & \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{\beta}\right) \\ & \Big| \\ \beta \in & \mathbb{Q}\left(\sqrt{2}\right) \\ & \Big| \\ & \mathbb{Q} \end{array}$$

Now, when we talk about extracting roots, we must be careful to avoid ambiguous (not well-defined) notation. For this reason, we usually adopt the point of view of Definition 3.19 where z being an n^{th} root of a means that $z^n = a$ (as opposed to $z = \sqrt[n]{a}$). That said, we do still occasionally use the root symbol when there is no ambiguity. For example, $\sqrt[3]{5}$ and $\sqrt{-1}$ are well-defined: the first is the one and only *real* solution to $x^3 = 5$, and the second is i (which we made a choice about long ago). However, $\sqrt[4]{-1 + i\sqrt{3}}$ is *not* well-defined, as there are 4 equally good choices.

Definition 4.1. We say K is a **radical extension** of a field F if there exist nonzero elements $r_1, r_2, \ldots, r_m \in K$ and positive integers $n_1, n_2 \ldots, n_m$ such that $K = F(r_1, r_2, \ldots, r_m)$, and

$$\begin{aligned} r_1^{n_1} &\in F, \\ r_2^{n_2} &\in F(r_1), \\ r_3^{n_3} &\in F(r_1, r_2), \\ &\vdots \\ r_k^{n_k} &\in F(r_1, \ldots, r_{k-1}). \end{aligned}$$

The definition expresses that each r_i is an n_i^{th}-root of some element in $F(r_1, \ldots, r_{i-1})$, so K may be thought of as being built by iteratively adding in n^{th}-roots of elements. The picture is something like this:

$$\begin{array}{rc} & K = F(r_1, r_2, \ldots, r_m) \\ & \Big| \\ r_m^{n_m} \in & F(r_1, r_2, \ldots, r_{m-1}) \\ & \Big| \\ & \vdots \\ & \Big| \\ r_3^{n_3} \in & F(r_1, r_2) \\ & \Big| \\ r_2^{n_2} \in & F(r_1) \\ & \Big| \\ r_1^{n_1} \in & F \end{array}$$

Example 4.2. Let's show that $K = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{-1+\sqrt{2}}\right)$ is a radical extension of $\mathbb{Q}$.

If we let $r_1 = \sqrt{2}$ and $r_2 = \sqrt[3]{-1+\sqrt{2}}$, then we see that

- $K = \mathbb{Q}(r_1, r_2)$;
- $r_1^2 = 2 \in \mathbb{Q}$;
- $r_2^3 = -1 + \sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}(r_1)$.

This shows that K is a radical extension of $\mathbb{Q}$ using $r_1 = \sqrt{2}$, $n_1 = 2$, $r_2 = \sqrt[3]{-1+\sqrt{2}}$, and $n_2 = 3$ in the definition of a radical extension. The picture is like this:

$$\begin{array}{ccc} K = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{-1+\sqrt{2}}\right) & & \\ & | & \\ \left(\sqrt[3]{-1+\sqrt{2}}\right)^3 \in & \mathbb{Q}\left(\sqrt{2}\right) & \\ & | & \\ \left(\sqrt{2}\right)^2 \in & \mathbb{Q} & \end{array}$$

Problem 4.3. Show that $\mathbb{Q}\left(\sqrt{3}, \zeta_5, \sqrt[4]{1-\sqrt{3}}\right)$ is a radical extension of $\mathbb{Q}$. What are you using for r_1, n_1, r_2, n_2, and r_3, n_3 when applying the definition?

Problem 4.4. Show that $\mathbb{C}$ is a radical extension of $\mathbb{R}$.

4.2 Solvability by radicals: the definition

Making precise what it means to express a number using addition, subtraction, multiplication, division, and the extraction of roots was the crux of defining solvability by radicals. However, we are aiming to define what it means to express the roots of a polynomial *in terms of the coefficients* using these operations. Let's establish some notation that allows us to highlight where the coefficients of a polynomial live.

Definition 4.5. Let F be a field. Then $F[x]$ is the set of all polynomials whose coefficients lie in F. This is read "F adjoin x."

For example, consider $a(x) = x^3 - ix^2 - 0.5$. Then $a(x) \notin \mathbb{Q}[x]$, because $i \notin \mathbb{Q}$; however, $a(x) \in \mathbb{C}[x]$ (and, in fact, $a(x) \in \mathbb{Q}(i)[x]$).

Problem 4.6. Give examples of polynomials $a(x)$, $b(x)$, and $c(x)$ such that

(1) $a(x) \in \mathbb{Q}[x]$,

(2) $b(x) \in \mathbb{R}[x]$ but $b(x) \notin \mathbb{Q}[x]$, and

(3) $c(x) \in \mathbb{C}[x]$ but $c(x) \notin \mathbb{R}[x]$.

We now, finally, write down one of our main definitions.

Definition 4.7. Let F be a field, and let $p(x) \in F[x]$. We say that $p(x)$ is **solvable by radicals** over F if all of the roots of $p(x)$ are contained in some radical extension of F.

Problem 4.8. Let $p(x) = x^2 + 3x + 1$. Show that all roots of $p(x)$ lie in $\mathbb{Q}\left(\sqrt{5}\right)$. Use this to explain why $p(x)$ is solvable by radicals over $\mathbb{Q}$.

Problem 4.9. Let $p(x) = x^4 + 2x^2 + 5$. Show that all four roots of $p(x)$ lie in $\mathbb{Q}(i, r, s)$ for some r and s such that $r^2 = -1 - 2i$ and $s^2 = -1 + 2i$. Use this to explain why $p(x)$ is solvable by radicals over $\mathbb{Q}$.

Problem 4.10. Let $p(x) = x^3 - 2$. Use Theorem 3.26 to write out all complex roots of $p(x)$, and then show that $p(x)$ is solvable by radicals over $\mathbb{Q}$.

Theorem 4.11. For each positive $n \in \mathbb{Z}$, $x^n - 1$ is solvable by radicals over $\mathbb{Q}$.

Theorem 4.12. For each positive $n \in \mathbb{Z}$, $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$ is solvable by radicals over $\mathbb{Q}$.

Theorem 4.13. Every quadratic polynomial $p(x) \in \mathbb{Q}[x]$ is solvable by radicals over $\mathbb{Q}$.

Problem 4.14. Let $p(x) = x^6 - 3x^3 - 1$. Show that $p(x)$ is solvable by radicals over $\mathbb{Q}$.