Algebraic elements and algebraic extensions:

- We say that $z = i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ since it is the root of a nonzero polynomial, namely $x^2 + 1$, in $\mathbb{R}[x]$.
- We say that $z = \sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since it is the root of a nonzero polynomial, namely $x^2 - 2$, in $\mathbb{Q}[x]$.
- Any n^{th} root of unity is algebraic over $\mathbb{Q}$ since is is a root of $x^n - 1$, which is nonzero in $\mathbb{Q}[x]$.
- The extension $\mathbb{C}/\mathbb{R}$ is algebraic, since every element of $\mathbb{C}$ is the root of a nonzero polynomial in $\mathbb{R}[x]$. (If $a + bi$ is a complex number, then it is a root of the polynomial $x^2 - 2a + (a^2 + b^2)$ which has real coefficients; check this!)
- The extension $\mathbb{R}/\mathbb{Q}$ is not algebraic, since there are elements in $\mathbb{R}$ that are not roots of any nonzero polynomial in $\mathbb{Q}[x]$. (This is not obvious, but it is true. Examples of real numbers that are not roots of any polynomials in $\mathbb{Q}[x]$ are $z = e$ and $z = \pi$.)
- We can consider $\mathbb{F}_4$ as a field extension of $\mathbb{F}_2$ if we identify $[0]$ in $\mathbb{F}_2$ with $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ in $\mathbb{F}_4$ and $[1]$ in $\mathbb{F}_2$ with $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathbb{F}_4$. The extension $\mathbb{F}_4/\mathbb{F}_2$ is algebraic because every element in $\mathbb{F}_4$ is the root of a nonzero polynomial in $\mathbb{F}_2$. (Recall Exercise 6.35.)

Adjoining an element to a base field:

Note. Given a base field k, an extension field K/k, and an element $z \in K$, the field $k(z)$ is defined as the intersection of all subfields of K containing k and z. This definition, while precise, is not very explicit. How does one find the intersection of all subfields of K containing z? In practice, we use Theorem 7.25 and Proposition 7.20 to provide an explicit description of $k(z)$.

- We can adjoin the element $z = i \in \mathbb{C}$ to $\mathbb{R}$ to create the field $\mathbb{R}(i)$. This is defined to be the intersection of all subfields of $\mathbb{C}$ that contain all the real numbers as well as i. Theorem 7.25 says that $\mathbb{R}(i) \cong \mathbb{R}[x]/(x^2 + 1)$. We know from Theorem 7.11 that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$; in fact $\mathbb{R}(i) = \mathbb{C}$.
- We can adjoin the element $z = \sqrt{2} \in \mathbb{R}$ to $\mathbb{Q}$ to create the field $\mathbb{Q}(\sqrt{2})$. By definition, this is the intersection of all subfields of $\mathbb{R}$ that contain the rational numbers as well as $\sqrt{2}$. Theorem 7.25 says that $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$, since $x^2 - 2$ is the unique monic irreducible polynomial in $\mathbb{Q}[x]$ that has $\sqrt{2}$ as a root. Thus, by Proposition 7.20, $\mathbb{Q}(\sqrt{2})$ is a two-dimensional vector space over $\mathbb{Q}$; in particular $\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2} : r, s \in \mathbb{Q}\}$.
- A similar discussion shows that $\mathbb{Q}(i) = \{r + si : r, s \in \mathbb{Q}\}$ and $\mathbb{Q}(\omega) = \{r + s\omega : r, s \in \mathbb{Q}\}$.
- The field $\mathbb{Q}(\sqrt[3]{5})$ is a 3-dimensional vector space over $\mathbb{Q}$ since the unique monic irreducible polynomial in $\mathbb{Q}[x]$ having $\sqrt[3]{5}$ as a root is $x^3 - 5$. Explicitly $\mathbb{Q}(\sqrt[3]{5}) = \{r + s\sqrt[3]{5} + t(\sqrt[3]{5})^2 : r, s, t \in \mathbb{Q}\}$.

Minimal polynomial

Let K/k be a field extension and $z \in K$ be algebraic over k. The unique monic irreducible polynomial in $k[x]$ having z as a root is called the minimal polynomial of z. (We know that such a polynomial exists, because it is the unique monic generator of the kernel of the homomorphism $k[x] \to K$ given by $f \mapsto f(z)$.)

- The minimal polynomial of i over $\mathbb{R}$ is $x^2 + 1$, since it is the unique monic irreducible polynomial in $\mathbb{R}[x]$ having i as a root.
- The polynomial $x^3 - 3x^2 + x - 3$ has i as a root. (Check it!) By Proposition 7.20(iii) and the definition of minimal polynomial, $x^2 + 1$ must divide $x^3 - 3x^2 + x - 3$. Polynomial long division yields $x^3 - 3x^2 + x - 3 = (x - 3)(x^2 + 1)$.

- The minimal polynomial of i over $\mathbb{C}$ is $x - i$. Note that $x^2 + 1$ is not irreducible in $\mathbb{C}[x]$; it factors as $x^2 + 1 = (x - i)(x + i)$.
- The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.
- The minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$ is $x - \sqrt{2}$.

It is worth restating Proposition 7.20(iii)(v) and Corollary 7.21 using the term minimal polynomial. Let K/k be a field extension and let $z \in K$ be algebraic over k.

- The minimal polynomial of z over k is a divisor of every polynomial in $k[x]$ that has z as a root. (Proposition 7.20(iii))
- The degree of the field extension K/k is the degree of the minimal polynomial of z over k. (Proposition 7.20(v) and Corollary 7.21.)

Adjoining an element to a base field, revisited

It is worth stating how Proposition 7.20(v) and Theorem 7.25 work together to give an explicit description of $k(z)$. Let K/k be an extension field and $z \in K$ be algebraic over k. Let $p(x)$ be the minimal polynomial of z over k and d be the degree of $p(x)$. Then $k(z)$ is a d-dimensional vector space over k; explicitly:

$$k(z) \quad = \quad \{a_0 + a_1 z + \cdots + a_{d-1} z^{d-1} : a_i \in k \text{ for } 0 \leq i \leq d-1\}$$

This generalizes the examples discussed above:

$$\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}$$

$$\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2} : r, s \in \mathbb{Q}\}$$
$$\mathbb{Q}(i) = \{r + si : r, s \in \mathbb{Q}\}$$
$$\mathbb{Q}(\omega) = \{r + s\omega : r, s \in \mathbb{Q}\}$$
$$\mathbb{Q}(\sqrt[3]{5}) = \{r + s\sqrt[3]{5} + t(\sqrt[3]{5})^2 : r, s, t \in \mathbb{Q}\}$$