Chapter 6

Algebraic extension fields

Our goal remains: to show that there exist polynomials that are *not* solvable by radicals over $\mathbb{Q}$. In Chapter 4, we finally succeeded in properly formulating the notion of solvability by radicals, which we did in the language of field extensions. Additionally, we were able to catalog many polynomials that we are certain are solvable by radicals. Then, in Chapter 5, we took a much closer look a polynomials, ultimately building a significant amount of language and theory to analyze polynomial rings over fields. The conclusion of the chapter hinted at the tight connection between polynomial rings and field extensions where we saw that $\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}(i)$. In this chapter, we will clarify this connection and exploit it to significantly deepen our understanding of extension fields of the form $\mathbb{Q}(\alpha)$ where α is a root of some polynomial in $\mathbb{Q}[x]$.

6.1 Algebraic elements

Recall that a polynomial in $F[x]$ is solvable by radicals over F if all of the roots of the polynomial lie in some radical extension of F. Our focus is on roots of polynomials, and the next definition gives us some language to highlight this.

Definition 6.1. Let F be a subfield of E. An element $\alpha \in E$ is **algebraic** over F if $p(\alpha) = 0$ for some nonzero $p(x) \in F[x]$. If α is not algebraic over F, then it is said to be **transendental** over F.

To show an element α is algebraic over F, we need only produce a polynomial *with coefficients in F* for which α is a root. For example, the complex number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because $\sqrt{2}$ is a root of $p(x) = x^2 - 2$ and $p(x) \in \mathbb{Q}[x]$. Also, π is algebraic over $\mathbb{R}$ because π is a root of $q(x) = x - \pi$ and $q(x) \in \mathbb{R}[x]$. However, it is *much* harder to show that π is *not* algebraic over $\mathbb{Q}$ (so π is transcendental over $\mathbb{Q}$). Incidentally, a set-theoretic argument shows that almost all elements of $\mathbb{C}$ are transcendental over $\mathbb{Q}$; nevertheless, we will focus on algebraic elements.

Problem 6.2. Show that each of the following are algebraic over $\mathbb{Q}$: 11, $\sqrt[3]{11}$, ζ_{11}, and i.

Problem 6.3. Suppose that $\gamma \in \mathbb{C}$ and $\gamma^5 = 2\gamma^2 - 7$. Explain why γ is algebraic over $\mathbb{Q}$.

Problem 6.4. Let $\alpha = \sqrt{2} + i$. Show that α is algebraic over $\mathbb{Q}$.

Now, an algebraic element over F is a root of *some* nonzero polynomial over F, but such an element will be a root of lots of polynomials. For example, since $\sqrt{2}$ is a root of $p(x) = x^2 - 2$, we find that for *every* $q(x) \in \mathbb{Q}[x]$, $\sqrt{2}$ is a root of $q(x)p(x)$ because $q(\sqrt{2})p(\sqrt{2}) = q(\sqrt{2})p(0) = 0$. The polynomial $x^2 - 2$ is special because it is a polynomial *of smallest degree* for which $\sqrt{2}$ is a root. In order to formalize this observation, we need to weave together several results from the last chapter.

Let F be a subfield of E, and suppose that $\alpha \in E$ is algebraic over F. Then α is the root of *some* nonzero $p(x) \in F[x]$. Let's look at the set of *all* polynomials for which α is a root: $I = \{p(x) \in F[x] \mid p(\alpha) = 0\}$. By Theorem 5.109, "evaluation at α" gives rise to a homomorphism $\mathcal{E}_\alpha : F[x] \to E[x]$, and notice that I is precisely the kernel of $\mathcal{E}_\alpha$. Thus, by Theorem 5.116, I is an ideal of $F[x]$, and since $F[x]$ is a PID, it must be that $I = (m(x))$ for some $m(x) \in F[x]$.

Now, $m(x)$ is nonzero since I contains some nonzero polynomial, and this also implies that $m(x)$ is not a constant polynomial since the only constant polynomial that has roots is the zero polynomial. Moreover, if $m(x)$ is not monic, we can make it monic by multiplying by the inverse of the leading coefficient and the result will still generate I by Theorem 5.103. So, we may assume that $I = (m(x))$ with $m(x)$ nonconstant and monic.

Also, notice that by Theorem 5.91, $m(x)$ divides every polynomial in I. So if $I = (n(x))$ for some other monic polynomial $n(x)$, then $m(x)$ and $n(x)$ would divide each other. In other words, $m(x) = a(x)n(x) = a(x)b(x)m(x)$ for some polynomials $a(x), b(x) \in F[x]$. Considering the degree of both sides of $m(x) = a(x)b(x)m(x)$, we see that $a(x)$ and $b(x)$ must be constant polynomials. But since $m(x) = a(x)n(x)$ with $m(x)$ and $n(x)$ both monic, the only conclusion is that $a(x) = 1$, so $m(x) = n(x)$.

In summary, $I = \{p(x) \in F[x] \mid p(\alpha) = 0\}$ is an ideal, and there is a unique nonconstant monic polynomial $m(x)$ that generates I. In fact, more is true.

Lemma 6.5. Let F be a subfield of E, and suppose that $\alpha \in E$ is algebraic over F. Let $I = \{p(x) \in F[x] \mid p(\alpha) = 0\}$, and suppose that $I = (m(x))$ for some nonconstant $m(x) \in F[x]$. Then $m(x)$ is irreducible.

Combining Lemma 6.5 with our previous discussion, we arrive at the following fact.

Fact 6.6. Let F be a subfield of E, and suppose that $\alpha \in E$ is algebraic over F. Then there is a unique irreducible monic polynomial $m(x) \in F[x]$ such that $m(\alpha) = 0$. Moreover, if $p(x) \in F[x]$ and $p(\alpha) = 0$, then $m(x)$ divides $p(x)$.

The polynomial $m(x)$ from Fact 6.6 gets a special name.

Definition 6.7. Suppose that $\alpha \in E$ is algebraic over F. The unique irreducible monic polynomial $m(x) \in F[x]$ such that $m(\alpha) = 0$ is called the **minimal polynomial** of α over F. The **degree** of α over F is defined to be the degree of the minimal polynomial of α over F.

Theorem 6.8. Let F be a subfield of E. Suppose that $\alpha \in E$ is algebraic over F, and let $m(x)$ be the minimal polynomial of α over F. If $V = \{p(x) \in F[x] \mid p(\alpha) = 0\}$ (i.e the set of all polynomials that vanish at α), then $V = (m(x))$.

We will see shortly that the minimal polynomial of α over F is key to understanding the field extension $F(\alpha)$. But how do we find the minimal polynomial of α over F? The first step is to find *any* monic polynomial $p(x) \in F[x]$ for which $p(\alpha) = 0$ (which also verifies that α is algebraic over F). If we can show that $p(x)$ is irreducible, then $p(x)$ is the minimal polynomial, and we're done. Otherwise, we factor $p(x)$ into irreducible polynomials in $F[x]$, and by Fact 6.6, the minimal polynomial will be whichever one of the factors has α as a root. Let's test this out with some examples.

Problem 6.9. Explain why the minimal polynomial for ζ_3 over $\mathbb{Q}$ is *not* $x^3 - 1$. Find the minimal polynomial ζ_3 over $\mathbb{Q}$, and determine the degree of ζ_3 over $\mathbb{Q}$?

Problem 6.10. The polynomial $p(x) = x^3 - 11$ has three roots in $\mathbb{C}$.

(1) Find the degree over $\mathbb{Q}$ of each of the three roots.

(2) Find the degree over $\mathbb{R}$ of each of the three roots.

Problem 6.11. The polynomial $p(x) = x^5 - 2x^3 - 3x$ has five roots in $\mathbb{C}$. Find the minimal polynomial over $\mathbb{Q}$ of each of the five roots.

Problem 6.12. Let $z = a + bi$ with $a, b \in \mathbb{Q}$, and define $p(x) = (x - z)(x - \overline{z})$. Prove that $p(x) \in \mathbb{Q}[x]$, and then use this to find the minimal polynomial of $2 + i$ over $\mathbb{Q}$.

Problem 6.13. Find the minimal polynomial of $3 - \sqrt{5}$ over $\mathbb{Q}$.

6.1.1 Describing elements of $F(\alpha)$

In Chapter 3, we explored extension fields of the form $F(\alpha)$ where α was chosen from some larger field E. However, the definition of $F(\alpha)$ was abstract and often hard to work with. For example, $\mathbb{Q}(i)$ is defined to be the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and i, but this doesn't tell us much about what the elements of $\mathbb{Q}(i)$ actually look like. Nevertheless, in Problem 3.64, we were able show that $\mathbb{Q}(i)$ is precisely the set of elements of the form $a + bi$ with $a, b \in \mathbb{Q}$, and we also succeeded in showing that $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.

However, we noticed that describing $\mathbb{Q}(\alpha)$ is not always so easy since, for example, if $\alpha = \sqrt{2} + i$, then $\mathbb{Q}(\alpha) \neq \{a + b\alpha \mid a, b \in \mathbb{Q}\}$. That said, we've learned a lot since Chapter 3, so let's take another go at trying to describe fields like $\mathbb{Q}(\alpha)$.

Remember that (for $\alpha = \sqrt{2} + i$) we were able to show that $\{a + b\alpha \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}(\alpha)$, but the reverse containment did not hold. And, the reason the reverse containment didn't hold was because $\{a + b\alpha \mid a, b \in \mathbb{Q}\}$ is not a field, which can be seen fairly easily since $\alpha^2 \notin \{a + b\alpha \mid a, b \in \mathbb{Q}\}$ (so it's not closed under multiplication).

So why not add in α^2 and consider something like $\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$? Remembering that $\mathbb{Q}(\alpha)$ is a field containg $\mathbb{Q}$ and α (and is closed under addition and multiplication), we see again that $\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\} \subseteq \mathbb{Q}(\alpha)$. So maybe $\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\} = \mathbb{Q}(\alpha)$. Or, maybe we need to look at $\{a + b\alpha + c\alpha^2 + d\alpha^3 \mid a, b, c, d \in \mathbb{Q}\}$. These are all good ideas since $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \cdots + a_n\alpha^n \in \mathbb{Q}(\alpha)$ whenever $a_0, a_1, a_2, a_3, \ldots, a_n \in \mathbb{Q}$. Let's formalize this.

Theorem 6.14. Let F be a subfield of E, and let $\alpha \in E$. If $p(x) \in F[x]$, then $p(\alpha) \in F(\alpha)$.

Problem 6.15. Let $p(x) = 2x^3 + 7x^2 - \frac{1}{2}$. We know that $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ by Problem 3.66. Verify directly that $p(\sqrt{5}) \in \mathbb{Q}(\sqrt{5})$ by writing $p(\sqrt{5})$ in the form $a + b\sqrt{5}$ for some $a, b \in \mathbb{Q}$.

We are studying the elements we get when we plug α into polynomials. Let's frame this in terms of the evaluation homomorphism introduced in Theorem 5.109, like we did at the beginning of this chapter. The next theorem generalizes Problem 5.118.

Theorem 6.16. Let F be a subfield of E. Suppose that $\alpha \in E$ is algebraic over F, and let $m(x)$ be the minimal polynomial of α over F. If $\mathcal{E}_\alpha : F[x] \to E$ is the homomorphism defined by $\mathcal{E}_\alpha(p(x)) = p(\alpha)$, then

(1) $\ker(\mathcal{E}_\alpha) = (m(x))$, and

(2) $\operatorname{im}(\mathcal{E}_\alpha) \subseteq F(\alpha)$ and $F \cup \{\alpha\} \subset \operatorname{im}(\mathcal{E}_\alpha)$.

Using Theorems 5.105 and 5.124 (and the First Isomorphism Theorem for Rings), we can deduce that the image of $\mathcal{E}_\alpha$ is a field. But then, if we can verify that the image of $\mathcal{E}_\alpha$ contains F and α, we can conclude that the image of $\mathcal{E}_\alpha$ is actually *equal* to $F(\alpha)$ (by the definition of $F(\alpha)$). Let's put this together.

Theorem 6.17. Let F be a subfield of E. Suppose that $\alpha \in E$ is algebraic over F, and let $m(x)$ be the minimal polynomial of α over F. Then $F(\alpha) \cong F[x]/(m(x))$.

Notice that we still haven't succeeded in providing a nice description $F(\alpha)$, but we will if we can find a nice description of $F[x]/(m(x))$.

Lemma 6.18. Let F be a subfield of E, and suppose that $\alpha \in E$ is algebraic over F. Let $m(x)$ be the minimal polynomial of α over F, and let n be the degree of α over F. If $a(x) + (m(x)) \in F[x]/(m(x))$, then $a(x) + (m(x)) = r(x) + (m(x))$ where $r(x)$ is the remainder obtained when dividing $a(x)$ by $m(x)$. Consequently,

$$F[x]/(m(x)) = \{r(x) + (m(x)) \mid \deg r(x) < n \text{ or } r(x) = 0\}.$$

Tying together all of our work, we finally arrive at our desired description of $F(\alpha)$.

Theorem 6.19. Let F be a subfield of E. Suppose that $\alpha \in E$ is algebraic over F, and let n be the degree of α over F. Then

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}.$$

We had to work hard for Theorem 6.19, but using it is fairly easy. For example, suppose we want to describe $\mathbb{Q}(\sqrt[3]{2})$. We first need to know the degree of $\sqrt[3]{2}$ over $\mathbb{Q}$. Of course, $\sqrt[3]{2}$ is a root of $m(x) = x^3 - 2$, and $m(x)$ is irreducible by Theorems 3.26 and 5.64. Thus, $m(x) = x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$, so $\sqrt[3]{2}$ has degree 3 over $\mathbb{Q}$. Now we apply Theorem 6.19 to find that $\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$.

Problem 6.20. Use Theorem 6.19 to describe $\mathbb{Q}(\zeta_3)$.

Problem 6.21. Let $p(x) = x^3 - x + 1 \in \mathbb{Z}_3[x]$, and let r be a root of $p(x)$.

(1) Prove that $p(x)$ is irreducible in $\mathbb{Z}_3[x]$.

(2) Use Theorem 6.19 to describe $\mathbb{Z}_3(r)$.

(3) How many elements are in the field $\mathbb{Z}_3(r)$?

Problem 6.22. Let $\alpha = \sqrt{2} + i$. In Problem 6.4, we saw that α is algebraic over $\mathbb{Q}$ since α is a root of $x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$. Let $m(x)$ denote the minimal polynomial for α over $\mathbb{Q}$.

(1) Use Theorem 6.19 (and Problem 3.64) to explain why the degree of $m(x)$ isn't 1 or 2.

(2) Use Fact 6.6 to explain why $m(x)$ is a factor of $x^4 - 2x^2 + 9$.

(3) Explain why the degree of $m(x)$ isn't 3.

(4) Explain why $m(x) = x^4 - 2x^2 + 9$.

(5) Use Theorem 6.19 to describe $\mathbb{Q}(\sqrt{2} + i)$.

The next problem highlights how we use the minimal polynomial for α to compute (or rather, simplify) in $F(\alpha)$.

Problem 6.23. The polynomial $p(x) = x^5 + 2x + 2$ is irreducible in $\mathbb{Q}[x]$ (you do not need to prove this). Let s be a root of $p(x)$. By Theorem 6.19, every element of $\mathbb{Q}(s)$ can be written in the form $a_0 + a_1 s + a_2 s^2 + a_3 s^3 + a_4 s^4$ for some $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}$.

(1) Use the fact that $p(s) = 0$ to write s^5 in the form $a_0 + a_1 s + a_2 s^2 + a_3 s^3 + a_4 s^4$.

(2) Rewrite each of the following elements of $\mathbb{Q}(\alpha)$ in the form $a_0 + a_1 s + a_2 s^2 + a_3 s^3 + a_4 s^4$.

(a) $(s^3 + 2)(s^3 + 3s)$

(b) $3s^4(2 + s^3)(5 - s + s^2)$

Problem 6.24. Let's try to describe $\mathbb{Q}(\sqrt{2}, i)$. Notice that $\mathbb{Q}(\sqrt{2}, i) = \left(\mathbb{Q}(\sqrt{2})\right)(i)$. In words, the field obtained by adjoining $\sqrt{2}$ and i at the same time is equal to the field obtained by first adjoining $\sqrt{2}$ and then adjoining i to the result.

(1) Use Theorem 6.19 to describe $\mathbb{Q}(\sqrt{2})$.

(2) Use Theorem 5.64 to explain why $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$.

(3) Use Theorem 6.19 to describe $\left(\mathbb{Q}(\sqrt{2})\right)(i)$, which is equal to $\mathbb{Q}(\sqrt{2}, i)$.

(4) How does your description of $\mathbb{Q}(\sqrt{2}, i)$ compare to that for $\mathbb{Q}(\sqrt{2}+i)$ in Problem 6.22?

6.1.2 Eisenstein's irreducibility criterion

Theorem 6.19 provides a nice description of $F(\alpha)$ when α is algebraic over F. However, the description rests on us knowing the minimal polynomial of α over F (or at least its degree), which in turn rests on us being able to determine when polynomials are irreducible. We now introduce a useful irreducibility criterion for polynomials in $\mathbb{Q}[x]$.

Fact 6.25 (Eisenstein's Irreducibility Criterion (EIC))**.** Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ with all $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. Suppose that there is some *prime* number $p \in \mathbb{Z}$ such that all of the following conditions are met:

(1) p does *not* divide a_n,

(2) p does divide a_i for all $i < n$, and

(3) p^2 does *not* divide a_0.

Then $p(x)$ is irreducible in $\mathbb{Q}[x]$.

The proof of the EIC is interesting and not too difficult, but as it is more number-theoretic than algebraic, we will leave it for another time. The idea is to take the polynomial $p(x)$ whose coefficients are all integers and consider it as a polynomial in $\mathbb{Z}_p[x]$ by reducing all of the coefficients modulo p. Details can be found in other books or on Wikipedia.

Problem 6.26. Use the EIC to show that each of the following polynomials are irreducible in $\mathbb{Q}[x]$. What did you choose as your prime p? Were there other choices?

(1) $f(x) = 7x^4 + 6x^3 + 12x - 30$

(2) $g(x) = x^8 - 6x^5 - 30x^3 + 12$

Problem 6.27. Let α be a root of $p(x) = x^5 + 5x^4 - 5$. (You don't need to compute α!)

(1) Prove that $p(x)$ is irreducible over $\mathbb{Q}$.

(2) Use Theorem 6.19 to describe $\mathbb{Q}(\alpha)$.

Problem 6.28. Consider the polynomial $f(x) = x^7 - \frac{5}{2}$.

(1) Explain why the EIC does *not* apply to $f(x)$.

(2) Prove that if $f(x)$ is reducible in $\mathbb{Q}[x]$, then so is $g(x) = 2x^7 - 5$.

(3) Use the EIC to show that $g(x)$ is irreducible, and conclude that $f(x)$ is irreducible.

Let's try to use the EIC to determine the minimal polynomial of some special elements, namely the ζ_n. We know that ζ_n is algebraic over $\mathbb{Q}$ because it is a root of $x^n - 1$. However, $x^n - 1$ can not be the minimal polynomial since it has $x - 1$ as a factor. But, we've observed a few times now that

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1).$$

Set $\Psi_n(x) = x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$. Since $(\zeta_n)^n - 1 = 0$, it must be $\zeta_n - 1 = 0$ or $\Psi_n(\zeta_n) = 0$. Of course, $\zeta_n - 1 \neq 0$, so ζ_n is a root of $\Psi_n(x)$. Could $\Psi_n(x)$ be the minimal polynomial?

Problem 6.29. Show that $\Psi_4(x) = x^3 + x^2 + x + 1$ is *not* the minimal polynomial for ζ_4 over $\mathbb{Q}$. What is the minimal polynomial?

So, we see that $\Psi_n(x)$ is not always the minimal polynomial for ζ_n, as it fails for $n = 4$. But what about for $n = 5$? Could $\Psi_5(x) = x^4 + x^3 + x^2 + x + 1$ be the minimal polynomial for ζ_5? We need to determine if $\Psi_5(x)$ is irreducible, but the EIC does not apply because there is no prime that divides the non-leading coefficients. Let's see if we can transform $\Psi_5(x)$ into a related polynomial for which the EIC will apply.

Theorem 6.30. Let F be a field, and let $p(x) \in F[x]$. If $p(x)$ is reducible in $F[x]$, then $p(x+1)$ is also reducible in $F[x]$.

Problem 6.31. Consider the polynomial $\Psi_5(x) = x^4 + x^3 + x^2 + x + 1$.

(1) Compute $\Psi_5(x+1)$, and write it in the form $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Consider using the fact that $x^5 - 1 = (x-1)\Psi_5(x)$ to help with the computation.

(2) Use the EIC to show that $\Psi_5(x+1)$ is irreducible.

(3) Explain why $\Psi_5(x)$ is the minimal polynomial for ζ_5 over $\mathbb{Q}$.

(4) Use Theorem 6.19 to describe $\mathbb{Q}(\zeta_5)$.

So, why was $\Psi_5(x)$ irreducible while $\Psi_4(x)$ was not? To address the general case, we could use a similar approach as in Problem 6.31 to analyze $\Psi_n(x+1)$ (using the Binomial Theorem to simplify the expression).

Problem 6.32. Make a conjecture as to when $\Psi_n(x) = x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$ is the minimal polynomial for ζ_n over $\mathbb{Q}$. That is, try to fill in the blank: "$\Psi_n(x)$ is the minimal polynomial for ζ_n over $\mathbb{Q}$ if and only if __(something about n)__." If you have the time, try to prove your conjecture.

To learn more about the minimal polynomial for ζ_n (for any n), try looking up "cyclotomic polynomials" on Wikipedia.

6.2 Extension fields as vector spaces

When we work with complex numbers, we often write them in the form $a + bi$ for $a, b \in \mathbb{R}$. So, every complex number can be described using two real numbers: a and b. Moreover, each complex number is described by a *unique* choice of a and b. This allows us to associate a complex number $a + bi$ with a vector in $\mathbb{R}^2$ via

$$a + bi \mapsto \begin{bmatrix} a \\ b \end{bmatrix}.$$

Additionally, adding two complex numbers $a+bi$ and $c+di$ corresponds to adding the two associated vectors $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right]$, and multiplying $a + bi$ by a *real* number r corresponds to multiplying the vector $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ by the scalar r. But, we should be careful with multiplication because multiplying $a+bi$ and $c+di$ does not correspond to multiplying the entries in the corresponding vectors—do you see why? Nevertheless, we find that $\mathbb{C}$ is a vector space over $\mathbb{R}$, and the fact that every complex number can be described by a unique pair of real numbers is expressing that $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$.

Can we do this for other fields? In Problem 6.27, we saw that if α is a root of x^5+5x^4-5, then each element $y \in \mathbb{Q}(\alpha)$ is of the form $y = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4$ for $a, b, c, d, e \in \mathbb{Q}$. If we knew that there was a *unique* choice of a, b, c, d, e for each y, then like before we could associate each element of $\mathbb{Q}(\alpha)$ with a vector in $\mathbb{Q}^5$ via

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 \mapsto \begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix}.$$

We'll see that these observations generalize to every extension field E of a field F. Let's start by properly defining vector spaces. Note that, in the formal definition below, scalar multiplication by a number c is being written as $\lambda_c v$, instead of just cv, but as we continue on, we will return to writing simply cv.

Definition 6.33. Let F be a field. A **vector space over** F is a structure $(V, +, \{\lambda_c \mid c \in F\})$ consisting of a set V together with a binary operation $+$ and a unary operation λ_c for each $c \in F$ (which we call *addition* and *scalar multiplication by* c) such that for some element $0 \in V$ the following axioms hold.

- **Addition Axioms:** Addition is associative and commutative; the element 0 is an additive identity; every $x \in F$ has an additive inverse with respect to 0, denoted $-x$.
- **Distributivity Axioms:** For all $u, v \in V$ and all $c \in F$, $\lambda_c(u+v) = \lambda_c u + \lambda_c v$.
- **Compatibility Axioms:** For all $v \in V$ and all $c, d \in F$,
  (1) $\lambda_{c+d} v = \lambda_c v + \lambda_d v$,
  (2) $\lambda_c(\lambda_d v) = \lambda_{cd} v$, and
  (3) $\lambda_1 v = v$.

Notice that the distributivity axiom can also be expressed by saying that each λ_c is a homomorphism from $(V, +)$ to $(V, +)$. The compatibility axioms can also be framed in terms of a homomorphism, but we will not explore that here.

As mentioned above, we tend to omit writing the λ, so for example, the distributivity axiom will be often written as $c(u+v) = cu + cv$.

Theorem 6.34. Let E be an extension field of F. Then E is a vector space over F where vector addition for E is just the usual field addition for E and scalar multiplication by an element $c \in F$ is just the usual field multiplication by c.

6.2.1 Degree of a field extension

We can now explore core concepts of linear algebra like linear independence, spanning sets, bases, dimension, and linear transformations. Basic results from a first course on linear algebra (over $\mathbb{R}$) transfer to our more general setting, and you should feel free to use them here.

Definition 6.35. Let V be a vector space over a field F, and let $v_1, \dots, v_n \in V$. Then

- $v_1, \dots, v_n$ are **linearly independent** if for all $c_1, \dots, c_n \in F$, $c_1 v_1 + \cdots + c_n v_n = 0$ implies that $c_1 = \cdots = c_n = 0$;
- $v_1, \dots, v_n$ **span** V if for all $w \in V$, there exist $c_1, \dots, c_n \in F$ such that $c_1 v_1 + \cdots + c_n v_n = w$;
- $v_1, \dots, v_n$ form a **basis** for V if they are linearly independent and span V.

Notice that we have defined linear independence and span only for finite sets of vectors, but the concepts can also be defined for infinite sets of vectors in a similar way. The importance of bases is more-or-less summarized in the following fact.

Fact 6.36. If V is a vector space, then all bases have the same cardinality ("size"). If $\mathcal{B}$ is any basis for V, then every element of V can be expressed as a linear combination of vectors in $\mathcal{B}$ in one and only one way.

This leads to the notion of dimension, which when considering field extensions (as in Theorem 6.34) we will refer to as the degree of the extension.

Definition 6.37. The **dimension** of a vector space V over a field F, denoted $\dim V$, is the cardinality of any basis for V.

Definition 6.38. If E is an extension field of F, then the dimension of E as a vector space over F is called the **degree of** E **over** F, denoted $[E : F]$. If $[E : F]$ is finite, we say that E is **finite dimensional** over F.

Problem 6.39. Let α be a root of $p(x) = x^5 + 5x^4 - 5$. In Problem 6.27, we saw that $p(x)$ is the minimal polynomial for α over $\mathbb{Q}$ and that $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 \mid a, b, c, d, e \in \mathbb{Q}\}$. By Theorem 6.34, $\mathbb{Q}(\alpha)$ is a vector space over $\mathbb{Q}$.

(1) Explain why the elements $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ span $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$.

(2) Assume that $c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_4\alpha^4 = 0$ for some $c_0, \dots, c_4 \in \mathbb{Q}$. Show that if at least one of $c_0, \dots, c_4$ is nonzero, then α is a root of some *nonzero* polynomial that has degree at most 4.

(3) Explain why the elements $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ are linearly independent over $\mathbb{Q}$.

(4) What is the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$? That is, find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Generalizing our work in Problem 6.39, we obtain a crucial theorem.

Theorem 6.40. Let F be a subfield of E. Suppose that $\alpha \in E$ is algebraic over F, and let n be the degree of α over F. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F, and $[F(\alpha) : F] = n$.

Problem 6.41. Use Theorem 6.40 and the results of Problem 6.10 to find a basis for $\mathbb{Q}(\sqrt[3]{11})$ over $\mathbb{Q}$ and compute $[\mathbb{Q}(\sqrt[3]{11}) : \mathbb{Q}]$.

Problem 6.42. Use Theorem 6.40 and the results of Problem 6.21 to find a basis for $\mathbb{Z}_3(r)$ over $\mathbb{Z}_3$ and compute $[\mathbb{Z}_3(r) : \mathbb{Z}_3]$ where r is a root of $p(x) = x^3 - x + 1 \in \mathbb{Z}_3[x]$.

Problem 6.43. Use Theorem 6.40 and the results of Problem 6.31 to find a basis for $\mathbb{Q}(\zeta_5)$ over $\mathbb{Q}$ and compute $[\mathbb{Q}(\zeta_5) : \mathbb{Q}]$.

Theorem 6.40 (which built off of Theorem 6.19) completes our goal of describing $F(\alpha)$, but we may want to adjoin more than one element to a field. For example, when we defined solvability by radicals in Chapter 4, we needed to ensure that all roots of the polynomial lived in some radical extension, often built by adjoining several elements.

Our approach to this will be as in Problem 6.24. Suppose we want a basis for $F(\alpha, \beta)$ over F. We can first find a basis for $F(\alpha)$ over F, and then find a basis for $F(\alpha, \beta)$ over $F(\alpha)$. If $1, \alpha, \ldots, \alpha^{m-1}$ is a basis for $F(\alpha)$ over F and $1, \beta, \ldots, \beta^{n-1}$ is a basis for $F(\alpha, \beta)$ over $F(\alpha)$, then we have that

$$\begin{aligned} F(\alpha) &= \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_0, \ldots, a_{m-1} \in F\}; \text{ and} \\ F(\alpha, \beta) &= \{b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} \mid b_0, \ldots, b_{n-1} \in F(\alpha)\}. \end{aligned}$$

But what we want is a basis for $F(\alpha, \beta)$ over F, so we want to express elements of $F(\alpha, \beta)$ using coefficients from F (not $F(\alpha)$). However, notice that since each b_i is in $F(\alpha)$, we can write each b_i in terms of $1, \alpha, \ldots, \alpha^{m-1}$, using only coefficients from F. Doing this for each b_i and simplifying, we see that every element of $F(\alpha, \beta)$ can be written as a linear combination of the elements

$$\begin{aligned} &1, \alpha, \ldots, \alpha^{m-1}, \\ &\beta, \alpha\beta, \ldots, \alpha^{m-1}\beta, \\ &\vdots \\ &\beta^{n-1}, \alpha\beta^{n-1}, \ldots, \alpha^{m-1}\beta^{n-1} \end{aligned}$$

using only coefficients from F. And moreover, it can be shown that these are linearly independent, so we found a basis for $F(\alpha, \beta)$ over F. The basis has size mn.

In fact, this process generalizes in a straightforward way to any chain of field extensions $F \subseteq K \subseteq L$. In words, a basis for L as a vector space over F can be found by multiplying a basis for K over F by the elements of a basis for L over K. This also yields an extremely useful multiplicative property for the degrees in a chain of field extensions, namely that $[L : F] = [L : K][K : F]$. The next fact summarizes our findings.

Fact 6.44. Let $F \subseteq K \subseteq L$ be fields. If $\{u_1, \ldots, u_m\}$ is basis for K over F and $\{w_1, \ldots, w_n\}$ is basis for L over K, then

$$\{u_1w_1, \ldots, u_mw_1, u_1w_2, \ldots, u_mw_2, \ldots, u_1w_n, \ldots, u_mw_n\}$$

is a basis for L over F. In particular, $[L : F] = [L : K][K : F]$.

Problem 6.45. Let's find a basis for $\mathbb{Q}(\sqrt[4]{2},\zeta_3)$ over $\mathbb{Q}$.

(1) Use the EIC to show x^4-2 is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$.

(2) Use Theorem 6.40 to find a basis for $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$.

(3) Use Theorem 5.64 to show x^2+x+1 is the minimal polynomial of ζ_3 over $\mathbb{Q}(\sqrt[4]{2})$.

(4) Use Theorem 6.40 to find a basis for $\mathbb{Q}(\sqrt[4]{2},\zeta_3)$ over $\mathbb{Q}(\sqrt[4]{2})$.

(5) Use Theorem 6.44 to find a basis for $\mathbb{Q}(\sqrt[4]{2},\zeta_3)$ over $\mathbb{Q}$ and determine $[\mathbb{Q}(\sqrt[4]{2},\zeta_3):\mathbb{Q}]$.

When exploring degrees of extensions, the following fact from linear algebra often comes up: if W is a subspace of V, then $\dim W = \dim V$ if and only if $W = V$. Applying this to field extensions yields the following.

Fact 6.46. Let $F \subseteq K \subseteq L$ be fields. Then $[K:F]=[L:F]$ if and only if $K=L$.

Problem 6.47. Let's revisit the fields $\mathbb{Q}(\sqrt{2}+i)$ and $\mathbb{Q}(\sqrt{2},i)$.

(1) Explain why $\mathbb{Q}(\sqrt{2}+i)\subseteq\mathbb{Q}(\sqrt{2},i)$.

(2) Use Theorem 6.40 and Problem 6.22 to determine $[\mathbb{Q}(\sqrt{2}+i):\mathbb{Q}]$.

(3) Use Theorem 6.44 and Problem 6.24 to determine $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}]$.

(4) Use the previous parts to show that $\mathbb{Q}(\sqrt{2}+i)=\mathbb{Q}(\sqrt{2},i)$.

The next couple of problems illustrate the power of the multiplicative property of field degrees for a chain of fields.

Problem 6.48. Let's take a look at $\mathbb{Q}(\sqrt[4]{2},\zeta_3)$ over $\mathbb{Q}(\zeta_3)$.

(1) Explain why the EIC can *not* be used to show that x^4-2 is irreducible in $\mathbb{Q}(\zeta_3)[x]$.

(2) Use that $\mathbb{Q}\subset\mathbb{Q}(\zeta_3)\subset\mathbb{Q}(\sqrt[4]{2},\zeta_3)$ together with the multiplicative property of field degrees (from Theorem 6.44) to determine $[\mathbb{Q}(\sqrt[4]{2},\zeta_3):\mathbb{Q}(\zeta_3)]$. Remember that you computed $[\mathbb{Q}(\sqrt[4]{2},\zeta_3):\mathbb{Q}]$ in Problem 6.45.

(3) Use the fact that $[\mathbb{Q}(\sqrt[4]{2},\zeta_3):\mathbb{Q}(\zeta_3)]$ equals the degree of $\sqrt[4]{2}$ over $\mathbb{Q}(\zeta_3)$ (by Theorem 6.40) to explain why x^4-2 is irreducible in $\mathbb{Q}(\zeta_3)[x]$.

Problem 6.49. Let's show that $\sqrt[3]{2}\notin\mathbb{Q}(\sqrt{2})$.

(1) Explain why $\sqrt[3]{2}\in\mathbb{Q}(\sqrt{2})$ would imply that $\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{Q}(\sqrt{2})$.

(2) Use the multiplicative property of field degrees to show that $\sqrt[3]{2}\in\mathbb{Q}(\sqrt{2})$ would imply that $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$ is a divisor of $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$.

(3) What is $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$? What is $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$? Prove that $\sqrt[3]{2}\notin\mathbb{Q}(\sqrt{2})$.

Theorem 6.50. Let $m,n\in\mathbb{Z}$ with $2\leq m<n$. If $p,q\in\mathbb{Z}$ are prime, then $\sqrt[n]{p}\notin\mathbb{Q}(\sqrt[m]{q})$.

Problem 6.51. Let's find the degree of $\mathbb{Q}(\sqrt[5]{3}, \zeta_5)$ over $\mathbb{Q}$.

(1) Show that $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$.

(2) Use that ζ_5 is a root of $x^4 + x^3 + x^2 + x + 1$ to explain why $[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}(\sqrt[5]{3})] \leq 4$. Then Use Theorem 6.44 to show that $[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}] \leq 20$.

(3) Use Problem 6.31 and Theorem 6.44 to show $[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}]$ is divisible by 4.

(4) Explain why $[\mathbb{Q}(\sqrt[5]{3}, \zeta_5) : \mathbb{Q}] = 20$.

Let's wrap up this section with a couple more results. The first says that if E is a *finite dimensional* extension of F, then every element of E is in fact algebraic over F. To prove this, we need to take an arbitrary $r \in E$, and show it is a root of some nonzero polynomial $F[x]$. But how do we find such a polynomial? To explore this, let's let $n = [E : F]$ (which we are assuming is finite). This means that every basis for E over F consists of n elements. And by a result from linear algebra, a set of $n+1$ vectors must be linearly dependent. If we apply this to the set $\{1, r, r^2, \ldots, r^n\}$, we see that there are elements $a_0, a_1, a_2, \ldots, a_n \in F$ that are *not* all zero such that

$$a_0 + a_1 r + a_2 r^2 + \cdots + a_n r^n = 0.$$

This implies that r is a root of the *nonzero* polynomial $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, so r is indeed algebraic over F. Also, $r \in E$ implies that $F(r) \subseteq E$, so we now have that $[E : F] = [E : F(r)][F(r) : F]$. Thus $[F(r) : F]$ divides $[E : F]$, so as $[F(r) : F]$ equals the degree of r over F (by Theorem 6.40), we also get that the degree of r over F divides $[E : F]$. Here is the summary.

Fact 6.52. Let E be an extension field of F. Assume that $[E : F]$ is finite. If $r \in E$, then r is algebraic over F, and the degree of r over F divides $[E : F]$.

Combining this with Theorem 6.40, we obtain the following characterization of algebraic elements in terms of the fields they generate.

Corollary 6.53. Let E be an extension field of F, and let $r \in E$. Then r is algebraic over F if and only if $[F(r) : F]$ is finite.

6.2.2 Linear transformations

Let's briefly explore linear transformations in the context of field extensions.

Definition 6.54. Let V and W be vector spaces over a field F. A map $\phi : V \to W$ is called an F-**linear transformation** (or **homomorphism of** F-**vector spaces**) if the following are true for all $u, v \in V$ and all $c \in F$:

(1) $\phi(u + v) = \phi(u) + \phi(v)$;

(2) $\phi(cu) = c\phi(u)$.

Problem 6.55. Show that $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ defined via $\phi(a+b\sqrt{2}) = a-b\sqrt{2}$ is a $\mathbb{Q}$-linear transformation.

Problem 6.56. Show that $\gamma : \mathbb{C} \to \mathbb{C}$ defined via $\gamma(z) = \overline{z}$ is an $\mathbb{R}$-linear transformation.

Problem 6.57. The results of Problem 6.24 show that

$$\mathbb{Q}(\sqrt{2}, i) = \left\{a_0 + a_1\sqrt{2} + a_2 i + a_3 i\sqrt{2} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\right\}.$$

Consider $\phi : \mathbb{Q}(\sqrt{2}, i) \to \mathbb{Q}(\sqrt{2}, i)$ defined by $\phi(z) = \overline{z}$. As $\mathbb{Q}(\sqrt{2}, i)$ is an extension of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$ is a vector space over $\mathbb{Q}(\sqrt{2})$. Show that ϕ is a $\mathbb{Q}(\sqrt{2})$-linear transformation.

6.3 Isomorphisms of fields

We are closing in on our goal of understanding when a polynomial is solvable by radicals or not. Recall that $p(x) \in F[x]$ is solvable by radicals if all of the roots of $p(x)$ are contained in some radical extension of F. This implies that if $r_1, \ldots, r_n$ are the roots of $p(x)$, then $F(r_1, \ldots, r_n)$ must also be contained in a radical extension. We've been working hard to understand fields like $F(r_1, \ldots, r_n)$, and with Theorem 6.44, we are now able to explicitly describe the elements of $F(r_1, \ldots, r_n)$ as linear combinations of a particular basis, which involves certain powers of $r_1, \ldots, r_n$. But, we still need tools for analyzing $F(r_1, \ldots, r_n)$ in order to understand if it could be contained a radical extension or not.

It turns out that the key idea is to study certain functions from $F(r_1, \ldots, r_n)$ to itself. Remembering that $F(r_1, \ldots, r_n)$ is a field (hence a ring) and also a vector space over F, we look at functions that preserve both structures, namely ring homomorphism that are also F-linear transformations. The next theorem provides a convenient characterization of F-linear transformation for maps that are already known to be ring homomorphisms.

Theorem 6.58. Let K and L be extension fields of F, and let $\phi : K \to L$ be a surjective ring homomorphism. Then ϕ is an F-linear transformation if and only if $\phi(c) = c$ for all $c \in F$.

In Theorem 6.58, the property that "$\phi(c) = c$ for all $c \in F$" will be written as ϕ *fixes* F or ϕ *leaves* F *fixed*.

Definition 6.59. Let $\phi : X \to Y$ be a function.

- Let $A \subseteq X$. We say that ϕ **fixes** A if $\phi(a) = a$ for all $a \in A$.
- Define $\operatorname{Fix}(\phi)$ to be the set of *all* $x \in X$ such that $\phi(x) = x$.

In fact, we've already seen many examples of morphisms that fix a field; the next problem highlights two of them.

Problem 6.60. Let's explore a couple familiar maps and show that they fix certain fields.

(1) Define $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ via $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$. Show that ϕ fixes $\mathbb{Q}$.

(2) Define $\gamma : \mathbb{C} \to \mathbb{C}$ via $\gamma(z) = \overline{z}$. Show that γ fixes $\mathbb{Q}$. What is $\operatorname{Fix}(\gamma)$?

We now start to expose the implications of a morphism fixing a field. The next theorem is quite important.

Theorem 6.61. Let K and L be extension fields of F, and let $p(x) \in F[x]$. Suppose that $\phi : K \to L$ is a ring homomorphism that fixes F. If $\alpha \in K$ is a root of $p(x)$, then $\phi(\alpha)$ is also a root of $p(x)$.

Problem 6.62. Suppose that $\phi : \mathbb{Q}(\sqrt[3]{7}) \to \mathbb{C}$ is a ring homomorphism that fixes $\mathbb{Q}$. Use the fact that $\sqrt[3]{7}$ is a root of $x^3 - 7$ together with Theorems 3.26 and 6.61 to list the possible values of $\phi(\sqrt[3]{7})$.

Problem 6.63. Suppose that $\psi : \mathbb{C} \to \mathbb{C}$ is an isomorphism that fixes $\mathbb{Q}$. Use Theorem 6.61 (and the idea of Problem 6.62) to list the possible values of $\psi(\sqrt{5})$ and $\psi(\zeta_5)$. Try to make each list as short as possible, and explain your reasoning.

Problem 6.64. Show that each map below fixes $\mathbb{Q}$, and then use Theorem 6.61 to explain why neither map is a homomorphism.

(1) $\delta : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(i)$ defined by $\delta(a + b\sqrt{5}) = a + bi$

(2) $\sigma : \mathbb{Q}(\sqrt[3]{7}) \to \mathbb{Q}(\sqrt[3]{7})$ defined by $\sigma(a + b\sqrt[3]{7} + c(\sqrt[3]{7})^2 = a - b\sqrt[3]{7} + c(\sqrt[3]{7})^2$

Let's use what we've learned so far to explore which subfields L of $\mathbb{C}$ could be isomorphic to $\mathbb{Q}(\sqrt[3]{11})$ (just as an example). Let $\phi : \mathbb{Q}(\sqrt[3]{11}) \to L$ be an isomorphism—we'll try to determine the possibilities for L. Notice that Theorem 6.61 may be helpful, but only if we know that ϕ fixes the coefficients of a polynomial that has $\sqrt[3]{11}$ as a root. Let's first show that ϕ must fix all of $\mathbb{Q}$.

Problem 6.65. Let K and L be extension fields of $\mathbb{Q}$. Suppose that $\phi : K \to L$ is a surjective ring homomorphism. We'll show that ϕ fixes $\mathbb{Q}$.

(1) Use Theorem 5.111 (and properties of homomorphisms) to show that ϕ fixes every positive integer n. Remember that $2 = 1 + 1$, $3 = 1 + 1 + 1$, etc.

(2) Use Theorem 5.110 to conclude that ϕ fixes all integers.

(3) Let $\frac{a}{b} \in \mathbb{Q}$ be any rational number (with $a, b \in \mathbb{Z}$). Use Theorem 5.111, to show that ϕ fixes $\frac{a}{b}$.

Problem 6.66. Assume that $\phi : \mathbb{Q}(\sqrt[3]{11}) \to L$ is an isomorphism for some subfield L of $\mathbb{C}$. Recall from Problem 6.41 that $1, \sqrt[3]{11}, (\sqrt[3]{11})^2$ is a basis for $\mathbb{Q}(\sqrt[3]{11})$, so

$$\mathbb{Q}(\sqrt[3]{11}) = \{a + b\sqrt[3]{11} + c(\sqrt[3]{11})^2 \mid a, b, c \in \mathbb{Q}\}.$$

(1) Use Theorem 6.61 and Problem 6.65 to list the three possible values of $\phi(\sqrt[3]{11})$.

(2) Use Problem 6.65 to describe the possible values of $\phi(a + b\sqrt[3]{11} + c(\sqrt[3]{11})^2)$.

(3) What does this imply are the possibilities for L?

Problem 6.66 raises an important question: can we always create an isomorphism taking $\sqrt[3]{11}$ to β whenever β is a root of the same minimal polynomial as $\sqrt[3]{11}$? The next fact answers the quesion—it will be *extremely important* for us. The proof is not too difficult, but we will take it as fact. The main ingredients are some of the linear algebra that we've developed and (perhaps not surprisingly) the division algorithm.

Fact 6.67. Let F be a subfield of E. Suppose that $\alpha \in E$ is algebraic over F. Let $m(x)$ be the minimal polynomial of α over F, and let n be the degree of α over F. Suppose that β is also a root of $m(x)$, and define $\phi : F(\alpha) \to F(\beta)$ by

$$\phi(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}$$

for all $a_0, a_1, \ldots, a_{n-1} \in F$. Then ϕ is an isomorphism, and ϕ fixes F.

Problem 6.68. Use Theorem 6.61 (together with Problem 6.65) and Fact 6.67 to determine if each pair of fields are isomorphic or not. If they are, write down a formula for an isomorphism; if they are not, explain why not.

(1) $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$

(2) $\mathbb{Q}(\sqrt[4]{11})$ and $\mathbb{Q}(i\sqrt[4]{11})$

6.3.1 Automorphisms

As mentioned earlier, we really want to study maps from a field to itself. We now define one of the keys ingredients in our eventual solution to the insolvability of the quintic.

Definition 6.69. Let K be a field. An isomorphism from K to K is called an **automorphism** of K. We define $\mathrm{Aut}(K)$ to be the set of all automorphisms of K. If F is a subfield of K, we define $\mathrm{Aut}(K/F)$ to be the set of all automorphisms of K that fix F.

Unpacking the definition, we see that automorphisms of K are bijections from K to K (i.e permutations of K) that are also homomorphisms. Since we know that the composition of two bijections is a bijections and the composition of two homomorphisms is a homomorphism (see Theorem 5.112), we see that $\mathrm{Aut}(K)$ is closed under function composition. Moreover, each element of $\mathrm{Aut}(K)$ is a bijection, hence has an inverse, and it is not too difficult to show that the inverse is also a homomorphism. Thus, $\mathrm{Aut}(K)$ is closed under taking inverses. Of course, $\mathrm{Aut}(K)$ contains the identity function from K to K, so we conclude that $\mathrm{Aut}(K)$ is a group with respect to function composition.

Theorem 6.70. Let K be a field. Then $\mathrm{Aut}(K)$ is a group with respect to function composition. The identity is the identity function, which will be denoted id.

Let's show that $\mathrm{Aut}(K/F)$ is also a group—to do that we need to show that if two automorphisms of K fix F, then their composition does too.

Theorem 6.71. If F is a subfield of K, then $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$.

In light of Theorems 6.70 and 6.71, $\mathrm{Aut}(K)$ will be referred to as the **automorphism group** of K and $\mathrm{Aut}(K/F)$ will be called the **automorphism group of** K **over** F. While we're at it, let's extend Theorem 6.71 a bit.

Theorem 6.72. If $F \subseteq K \subseteq L$ is a chain of fields, then $\mathrm{Aut}(L/K)$ is a subgroup of $\mathrm{Aut}(L/F)$.

Theorem 6.72 is starting to build a correspondence from subfields of L to subgroups of $\mathrm{Aut}(L/F)$. However, notice that the correspondence is inclusion reversing.

$$\begin{tikzcd}
L \arrow[r] & \mathrm{Aut}(L/L) \arrow[d, phantom, sloped, "\subseteq"] \\
K \arrow[r] \arrow[u, phantom, sloped, "\subseteq"] & \mathrm{Aut}(L/K) \arrow[d, phantom, sloped, "\subseteq"] \\
F \arrow[r] \arrow[u, phantom, sloped, "\subseteq"] & \mathrm{Aut}(L/F)
\end{tikzcd}$$

In the picture above we listed the group $\mathrm{Aut}(L/L)$. These are the automorphism of L that fix all of L—there is only one such automorphism: the identity. Thus, $\mathrm{Aut}(L/L) = \{\mathrm{id}\}$.

Let's further explore these automorphism groups with some examples.

Example 6.73. Let's try to compute $\mathrm{Aut}(\mathbb{Q}(\zeta_5/\mathbb{Q})$. First, we know that $x^4 + x^3 + x^2 + x + 1$ is the minimum polynomial for ζ_5 over $\mathbb{Q}$, so by Theorem 6.40

- $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ is a basis for $\mathbb{Q}(\zeta_5)$ over $\mathbb{Q}$, and
- $\mathbb{Q}(\zeta_5) = \{a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 \mid a, b, c, d \in \mathbb{Q}\}$.

Thus, every function $\phi \in \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ can be expressed by a formula of the form

$$\phi(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3) = \ ???$$

Now, if $\phi \in \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, then ϕ fixes $\mathbb{Q}$. By Theorem 6.58, ϕ is a $\mathbb{Q}$-linear transformation from $\mathbb{Q}(\zeta_5)$ to itself, and by a result from linear algebra, ϕ is completely determined by its values on a basis. That is, once we determine the values of $\phi(1)$, $\phi(\zeta_5)$, $\phi(\zeta_5^2)$, and $\phi(\zeta_5^3)$, we will know a formula for ϕ. In fact, this is easy to see directly:

$$\begin{aligned}
\phi(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3) &= \phi(a) + \phi(b\zeta_5) + \phi(c\zeta_5^2) + \phi(d\zeta_5^3) \\
&= \phi(a) + \phi(b)\phi(\zeta_5) + \phi(c)\phi(\zeta_5^2) + \phi(d)\phi(\zeta_5^3) \\
&= a + b\phi(\zeta_5) + c\phi(\zeta_5^2) + d\phi(\zeta_5^3).
\end{aligned}$$

In fact, we can take this further:

$$\begin{aligned}
\phi(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3) &= a + b\phi(\zeta_5) + c\phi(\zeta_5^2) + d\phi(\zeta_5^3) \\
&= a + b\phi(\zeta_5) + c\phi(\zeta_5)^2 + d\phi(\zeta_5)^3.
\end{aligned}$$

So, to find a formula for ϕ we just need to determine the value for $\phi(\zeta_5)$; it can then be plugged into the above formula to find the value of ϕ on an arbitrary element of $\mathbb{Q}(\zeta_5)$.

Now, since ζ_5 is a root of $x^4 + x^3 + x^2 + x + 1$, Theorem 6.61 says that $\phi(\zeta_5)$ must be one of the roots of $x^4 + x^3 + x^2 + x + 1$, which are ζ_5, ζ_5^2, ζ_5^3, and ζ_5^4. The possibilities are named below. We will use repeatedly that $\zeta_5^5 = 1$; if desired, we could also use $\zeta_5^4 = -\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1$.

- ϕ_1 sends $\zeta_5 \mapsto \zeta_5$, which implies $\phi_1(a+b\zeta_5+c\zeta_5^2+d\zeta_5^3) = a+b\zeta_5+c\zeta_5^2+d\zeta_5^3$;
- ϕ_2 sends $\zeta_5 \mapsto \zeta_5^2$, which implies $\phi_2(a+b\zeta_5+c\zeta_5^2+d\zeta_5^3) = a+b\zeta_5^2+c\zeta_5^4+d\zeta_5$;
- ϕ_3 sends $\zeta_5 \mapsto \zeta_5^3$, which implies $\phi_3(a+b\zeta_5+c\zeta_5^2+d\zeta_5^3) = a+b\zeta_5^3+c\zeta_5+d\zeta_5^4$;
- ϕ_4 sends $\zeta_5 \mapsto \zeta_5^4$, which implies $\phi_4(a+b\zeta_5+c\zeta_5^2+d\zeta_5^3) = a+b\zeta_5^4+c\zeta_5^3+d\zeta_5^2$.

Here's another way to organize the possibilities.

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

We now have to determine if each ϕ_i is in $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ or not. As ϕ_1 is just the identity, $\phi_1 \in \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. To check the other possibilities, we can use Fact 6.67. For example, Fact 6.67 says that ϕ_2 is an isomorphism from $\mathbb{Q}(\zeta_5)$ to $\mathbb{Q}(\zeta_5^2)$. Since $\mathbb{Q}(\zeta_5^2) = \mathbb{Q}(\zeta_5)$ (because $\zeta_5^2 \in \mathbb{Q}(\zeta_5)$ and $\zeta_5 \in \mathbb{Q}(\zeta_5^2)$), ϕ_2 is indeed an automorphism of $\mathbb{Q}(\zeta_5)$, so $\phi_2 \in \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. Similarly, $\phi_3, \phi_4 \in \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. These are all possibilities, so

$$\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \{\phi_1, \phi_2, \phi_3, \phi_4\} = \{\mathrm{id}, \phi_2, \phi_3, \phi_4\}.$$

We now know that $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is a group of order 4. What group is it?

Problem 6.74. Let's determine what group $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is isomorphic to.

(1) Which element of $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is $(\phi_2)^2$ equal to? (Remember $(\phi_2)^2$ means $\phi_2 \circ \phi_2$.)

(2) Do the same for $(\phi_2)^3$ and $(\phi_2)^4$. Are either $(\phi_2)^3$ or $(\phi_2)^4$ equal to id? What is the order of ϕ_2? (The order of ϕ_2 will be the smallest positive k such that $(\phi_2)^k = \mathrm{id}$.)

(3) What are the orders of ϕ_3 and ϕ_4?

(4) Is $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ cyclic or not? Is $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ isomorphic to $\mathbb{Z}_4$ or V_4?

An important observation in Example 6.73 was that the possibilities for ϕ are determined simply by the possible values of $\phi(\zeta_5)$. This is true in general.

Fact 6.75. Let F be a subfield of E. Suppose that $\alpha \in E$ is algebraic over F, and let n be the degree of α over F. Then each $\phi \in \mathrm{Aut}(F(\alpha)/F)$ is completely determined by the value $\phi(\alpha)$. Consequently, $|\mathrm{Aut}(F(\alpha)/F| \leq n = [F(\alpha) : F]$.

Problem 6.76. Follow Example 6.73 to determine $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. What familiar group is it isomorphic to?

Problem 6.77. Let's determine $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.

(1) First explain why $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{2}\zeta_3)$ and why $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$.

(2) Follow Example 6.73 to show that $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$.

What happens if we adjoin more than one element? Can we compute $\mathrm{Aut}(F(\alpha_1,\alpha_2)/F)$ in a similar way as to how we computed $\mathrm{Aut}(F(\alpha)/F)$? The answer is yes, and the starting point is the following analog of Fact 6.75.

Fact 6.78. Let F be a subfield of E. Suppose that $\alpha_1,\ldots,\alpha_k \in E$ are algebraic over F. Then each $\phi \in \mathrm{Aut}(F(\alpha_1,\ldots,\alpha_k)/F)$ is completely determined by the values of $\phi(\alpha_1),\ldots,\phi(\alpha_k)$. Consequently, $|\mathrm{Aut}(F(\alpha_1,\ldots,\alpha_k)/F| \leq [F(\alpha_1,\ldots,\alpha_k):F]$.

Problem 6.79. Let's determine $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$.

(1) Let $\phi \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$. Explain why there are only two choice for $\phi(\sqrt{2})$ and only two choice for $\phi(i)$. What are they?

(2) Combine the different possibilities for $\phi(\sqrt{2})$ and $\phi(i)$ to complete the table below.

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

(3) Follow Example 6.73 to determine $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$.

(4) What familiar group is $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$ isomorphic to?

Problem 6.80. Set $L = \mathbb{Q}(\sqrt{2},i)$. In Problem 6.79 we determined $\mathrm{Aut}(L/\mathbb{Q})$. Let's connect the subfields of L with subgroups of $\mathrm{Aut}(L/\mathbb{Q})$ using Theorem 6.72.

(1) Let $K_1 = \mathbb{Q}(\sqrt{2})$. Find $\mathrm{Aut}(L/K_1)$ by determining which of $\phi_1,\phi_2,\phi_3,\phi_4$ are in $\mathrm{Aut}(L/K_1)$.

(2) Repeat for $K_2 = \mathbb{Q}(i)$. Find $\mathrm{Aut}(L/K_2)$.

(3) Repeat for $K_3 = \mathbb{Q}(i\sqrt{2})$. Find $\mathrm{Aut}(L/K_3)$.

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

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2},i) \arrow[rrrr] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & & & \{\mathrm{id}\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] \arrow[rr] & & \boxed{\mathrm{Aut}(L/K_1)} \arrow[dr, dash] & \boxed{\mathrm{Aut}(L/K_2)} \arrow[d, dash] & \boxed{\mathrm{Aut}(L/K_3)} \arrow[dl, dash] \\
& \mathbb{Q} \arrow[rrrr] & & & & \{\phi_1,\phi_2,\phi_3,\phi_4\} &
\end{tikzcd}$$

Problem 6.80 highlights quite well the tight connection between subfields of an extension field L of F and subgroups of $\mathrm{Aut}(L/F)$. So far, we've seen how each subfield K gives rise to a subgroup $\mathrm{Aut}(L/K)$. The next theorem indicates how we might reverse this.

Theorem 6.81. Let F be a subfield of L and H a subgroup of $\mathrm{Aut}(L/F)$. Define

$$\mathrm{Fix}_L(H) = \{k \in L \mid k \text{ is fixed by every } \phi \in H\}.$$

Then $\mathrm{Fix}_L(H)$ is a subfield of L, and $F \subseteq \mathrm{Fix}_L(H) \subseteq L$.

The picture is as follows.

$$\begin{tikzcd}
L & \{\mathrm{id}\} \\
\mathrm{Fix}_L(H) \arrow[u, phantom, sloped, "\subseteq"] & H \arrow[u, phantom, sloped, "\supseteq"] \arrow[l] \\
F \arrow[u, phantom, sloped, "\subseteq"] & \mathrm{Aut}(L/F) \arrow[u, phantom, sloped, "\supseteq"]
\end{tikzcd}$$

Taking a closer look at Problem 6.80, we can see that the maps $K \mapsto \mathrm{Aut}(L/K)$ and $H \mapsto \mathrm{Fix}_L(H)$ are actually inverses of each other. For example, $\mathrm{Fix}_L(\mathrm{Aut}(L/K_1)) = K_1$, so the composition of the maps looks like $K_1 \mapsto \mathrm{Aut}(L/K_1) \mapsto \mathrm{Fix}_L(\mathrm{Aut}(L/K_1)) = K_1$. However, this is not true for all fields, and Problem 6.77 gives an example. In the next chapter we'll study an important collection of fields (in fact, *the* collection of fields) for which $K \mapsto \mathrm{Aut}(L/K)$ and $H \mapsto \mathrm{Fix}_L(H)$ are always inverses.