## 5. Fields

5.1. **Field extensions.** Let $F \subseteq E$ be a subfield of the field $E$. We also describe this situation by saying that $E$ is an *extension field* of $F$, and we write $E/F$ to express this fact. If $E/F$ is a field extension and $S \subseteq E$, then there is a smallest subfield of $E$ that contains $F$ and $S$. We denote it by $F(S)$. If $S = \{u_1, \ldots, u_n\}$, then we of course write $F(u_1, \ldots, u_n)$ for this field, as usual.

*Exercise* 5.1. Prove the existence of such a smallest subfield $F(S)$, and show that $(F(S))(T) = F(S \cup T)$.

*Exercise* 5.2. Show that $F(S) = \bigcup F(T)$, where the union is taken over the finite subsets $T \subseteq S$.

Let's now describe $F(u)$, $u \in E$, more explicitly. We discussed the analogous problem for rings in Section 4.3, and we denoted the sub*ring* generated by $F$ and $u$ by $F[u]$. Its elements are $f(u)$, for $f \in F[x]$. We also know from our more detailed analysis of Section 4.4 that two cases are possible here: in the first case, $u$ is *algebraic* over $F$. Recall that this means that $f(u) = 0$ for some $f \in F[x]$, $f \neq 0$. We then introduced the *minimal polynomial* of $u$ over $F$ as the unique monic polynomial $f$ with $f(u) = 0$ of smallest possible degree. In the sequel, we will occasionally use the notation $f_u$ for the minimal polynomial of $u$. We also saw in Proposition 4.22 that $F[u] \cong F[x]/(f)$ and now Theorem 4.23 says that this ring $F[x]/(f)$ is either a field or not a domain. The second case arises precisely if $(f)$ is reducible. However, we cannot be in this second case here because $F[u] \subseteq E$ certainly is a domain.

It follows that if $u$ is algebraic, then its minimal polynomial $f_u \in F[x]$ is irreducible and $F(u) = F[u] \cong F[x]/(f_u)$.

On the other hand, if $u$ is *transcendental,* then $F[u] \cong F[x]$, and this is not a field, so $F(u) \supsetneq F[u]$ in this case. We can now also describe $F(u)$ as the subfield generated by $F[u]$. In other words, we are looking for the smallest subfield of $E$ that contains the domain $F[u]$. This kind of assignment, build a minimal field out of a domain, is what the *field of fractions* construction achieves (in fact, the original construction took place in a more challenging situation, where the domain was not right away contained in a field). So we now obtain that

$$F(u) = \left\{ f(u)g(u)^{-1} : f, g \in F[x], g \neq 0 \right\}.$$

Of course, you don't need to be familiar with the field of fractions to arrive at this answer; this can be written down and checked directly. The field of fractions construction does become relevant if you want to

embed $F[x]$ in a field. As we know from Section 4.2, the smallest such field is the field of fractions of $F[x]$; we'll denote this by $F(x)$. Let's state this as a formal definition:

**Definition 5.1.** The *field of rational functions* $F(x)$ is defined as the field of fractions of the polynomial ring $F[x]$.

As the terminology suggests, the elements of $F(x)$ are the formal rational functions $f(x)/g(x)$, with $f, g \in F[x]$, $g \neq 0$, and these are multiplied and added in the expected way. Moreover, $f_1/g_1$ and $f_2/g_2$ represent the same element of $F(x)$ precisely if $f_1 g_2 = f_2 g_1$ in $F[x]$.

If $u \in E$ is transcendental over $F$, then $F(u) \cong F(x)$; an isomorphism is obtained by mapping $f/g \in F(x)$ to $f(u)g(u)^{-1}$.

*Exercise* 5.3. (a) Let $\varphi : F \to F'$ be a (ring) homomorphism between fields. Show that $\varphi$ is injective.
(b) Let $u$ be algebraic, and try to map $F(x) \to F(u)$, $f/g \mapsto f(u)g(u)^{-1}$, as we did above in the other case, when $u$ is transcendental. Is this still a homomorphism?

*Exercise* 5.4. Let $E/F$ be a field extension, and let $u \in E$ be algebraic over $F$. (a) Let $g \in F[x]$. Show that $g(u) = 0$ if and only if $f_u | g$.
(b) Now let $h \in E[x]$ with $h(u) = 0$. Can you still conclude that $f_u | h$ (in $E[x]$)?
(c) Show that if $g \in F[x]$ is an irreducible monic polynomial with $g(u) = 0$, then $g = f_u$.

Let's summarize what we have found so far.

**Theorem 5.2.** *Let $E/F$ be a field extension, and let $u \in E$.*
*(a) If $u$ is algebraic, then its minimal polynomial $f_u$ is irreducible in $F[x]$. It can in fact be characterized as the unique irreducible monic polynomial with $f(u) = 0$; equivalently, $f_u$ is the unique monic polynomial of smallest possible degree with $f(u) = 0$. Moreover, $F(u) = F[u] \cong F[x]/(f_u)$.*
*(b) If $u$ is transcendental, then $F(u) \supsetneq F[u]$; we have that $F(u) \cong F(x)$.*

Such an extension $E/F$, with $E = F(u)$ generated by a single element $u \in E$, is also called a *simple extension,* and $u$ is called a *primitive element.*

The next easy but far-reaching idea will be to view the extension field as a vector space over the ground field. Indeed, if $E/F$ is a field extension, then $E$ is an $F$-vector space: we add elements of $E$ and multiply them by elements of $F$ just like before, and we ignore the extra option of multiplying two "vectors" $x, y \in E$. We denote $\dim E$,

as an $F$-vector space, by $[E : F]$, and we also refer to this dimension as the *degree* of the field extension. If the degree is finite, we also speak of a *finite extension* (meaning: finite dimensional extension).

**Theorem 5.3.** *Let $E/F$, $E = F(u)$, be a simple field extension. Then $u$ is algebraic if and only if $E/F$ is finite. In this case, $[E : F] = \deg f_u$.*

*Proof.* If $u$ is transcendental, then $1, u, u^2, \ldots$ are linearly independent because otherwise we would obtain a polynomial $f \in F[x]$, $f \neq 0$, with $f(u) = 0$.

If $u$ is algebraic and $n = \deg f_u$, then I claim that $1, u, \ldots, u^{n-1}$ is a basis of $E$ as an $F$-vector space. To confirm this, observe first of all that these elements are linearly independent, by the argument from the previous paragraph: if we had a linear relation $a_0 + a_1 u + \ldots + a_{n-1}u^{n-1} = 0$ with coefficients $a_j \in F$, not all equal to zero, then we would obtain a (monic, after division by the highest non-zero coefficient) polynomial $g \in F[x]$, $g \neq 0$, with $g(u) = 0$, $\deg g < n$, but this contradicts the definition of the minimal polynomial as the polynomial of smallest possible degree for which this happens.

To see that $1, u, \ldots, u^{n-1}$ span $E$, recall that $E = F[u]$, so any element of $E$ is a linear combination of powers $u^j$, $j \geq 0$. Now from $f_u(u) = 0$, we obtain a formula of the type $u^n = b_{n-1}u^{n-1} + \ldots + b_0$. So powers $u^j$ with $j \geq n$ may be expressed in terms of powers with smaller exponents, and by applying this repeatedly, we can completely eliminate powers $u^j$ with $j \geq n$ from our linear combination. □

*Example* 5.1. Clearly $\mathbb{C} = \mathbb{R}(i)$, and since $1, i$ is a basis of $\mathbb{C}$ over $\mathbb{R}$, we have that $[\mathbb{C} : \mathbb{R}] = 2$; this is of course consistent with $f_i = x^2 + 1$. So if $u \in \mathbb{C}$ is an arbitrary complex number, then $[\mathbb{R}(u) : \mathbb{R}] = 1$ or $= 2$. The first case means that $u \in \mathbb{R}$, and then $f_u = x - u$. If $u \notin \mathbb{R}$, so $[\mathbb{R}(u) : \mathbb{R}] = 2$ and thus $\mathbb{R}(u) = \mathbb{C}$, then Theorem 5.3 tells us that $\deg f_u = 2$. It follows from this that no $f \in \mathbb{R}[x]$ with $\deg f \geq 3$ is irreducible.

*Exercise* 5.5. Please give a more detailed argument for this step; use the *fundamental theorem of algebra,* which says that every non-constant $f \in \mathbb{C}[x]$ has a zero in $\mathbb{C}$.

This could have been seen directly, as follows. Let $a \in \mathbb{C}$ be a zero of $f \in \mathbb{R}[x]$, $\deg f \geq 3$ (again, we are using the fundamental theorem of algebra here). If $a \in \mathbb{R}$, then $(x - a)|f$ and $f$ is not irreducible. If $a \notin \mathbb{R}$, then we observe that $f(\overline{a}) = 0$ also, so $(x - a)(x - \overline{a}) = x^2 - (2 \operatorname{Re} a)x + |a|^2 \in \mathbb{R}[x]$ divides $f$, and again $f$ is reducible.

*Exercise* 5.6. (a) Show that $f(x) = x^3 + 9x + 6 \in \mathbb{Q}[x]$ is irreducible; (b) Let $u \in \mathbb{C}$ be a zero of $f$ (it doesn't matter which one). Express $(1+u)^{-1} \in \mathbb{Q}(u)$ as a linear combination of the basis elements $1, u, u^2$.

Next, we show that repeated finite field extensions produce another finite extension:

**Theorem 5.4.** *Suppose that $L/E$, $E/F$ are finite field extensions. Then $L/F$ is finite and $[L : F] = [L : E][E : F]$.*

*Proof.* Let $a_1, \ldots, a_m$ be a basis of $E$ over $F$, and let $b_1, \ldots, b_n$ be a basis of $L$ over $E$. I then claim that $\{a_j b_k : 1 \leq j \leq m, 1 \leq k \leq n\}$ is a basis of $L$ as an $F$-vector space.

Clearly, this set spans $L$ because an arbitrary element of $L$ can be written as a linear combination $\sum c_k b_k$ with coefficients $c_k \in E$, and then we can similarly expand $c_k = \sum d_{kj} a_j$, with coefficients $d_{kj} \in F$.

A similar argument establishes that the $a_j b_k$ are linearly independent: suppose that $\sum d_{jk} a_j b_k = 0$, with coefficients $d_{jk} \in F$. Then $\sum_j d_{jk} a_j \in E$, so the linear independence of the $b_k$ over $E$ now implies that $\sum_j d_{jk} a_j = 0$ for all $k$, but then the linear independence of the $a_j$ shows that $d_{jk} = 0$ for all $j, k$. □

**Definition 5.5.** A field extension $E/F$ is called *algebraic* if every $u \in E$ is algebraic over $F$.

*Exercise* 5.7. Deduce from Theorem 5.3 that a finite field extension is algebraic.

**Theorem 5.6.** *Suppose that $L/E$, $E/F$ are algebraic field extensions. Then $L/F$ is algebraic.*

This is not just an immediate consequence of Theorem 5.4 because the converse of Exercise 5.7 does not hold: algebraic extensions need not be finite.

*Proof.* Let $u \in L$, and let $f_u \in E[x]$ be its minimal polynomial over $E$. Let $a_0, \ldots, a_n \in E$ be the coefficients of $f_u$. Then $u$ is also algebraic over $F(a_0, \ldots, a_n) \subseteq E$, with the same minimal polynomial as over $E$, so $F(u, a_0, \ldots, a_n)/F(a_0, \ldots, a_n)$ is a finite extension, by Theorem 5.3.

Observe that $F(a_0)/F$ is a finite extension because $a_0 \in E$ is algebraic over $F$. Next, $F(a_0, a_1)/F(a_0)$ is also finite because $a_1$ is algebraic over $F$ and thus also over the larger field $F(a_0)$. Continue in this style and then apply Theorem 5.4 repeatedly. We conclude that $F(a_0, \ldots, a_n)/F$ is finite. Then one more application of Theorem 5.4 shows that $F(u, a_0, \ldots, a_n)/F$ and thus also $F(u)/F$ are finite as well. Now Theorem 5.3 implies that $u$ is algebraic over $F$, as desired. □

**Theorem 5.7.** *Let $E/F$ be a field extension. Define*

$$A = \{a \in E : a \text{ is algebraic over } F\}.$$

*Then $A$ is a field, and $F \subseteq A \subseteq E$.*

*Proof.* The inclusions are clear because every $a \in F$ is algebraic, with minimal polynomial $f_a = x - a$. So we must show that $A$ is a subfield of $E$. Let $a, b \in A$. We must show that then $a - b$ and $ab^{-1}$ (if $b \neq 0$) are in $A$ as well.

Now $F(a, b)/F$ is a finite extension, by the same arguments as in the previous proof (adjoin $a$, $b$ separately and successively and observe that each individual extension is finite). Moreover, $a - b, ab^{-1} \in F(a, b)$, so $F(a - b) \subseteq F(a, b)$ also is a finite extension of $F$, and thus $a - b$ is algebraic by Theorem 5.3 (and similarly for $ab^{-1}$). □

*Example* 5.2. Consider the field extension $\mathbb{C}/\mathbb{Q}$, and form the intermediate field $A$ of algebraic numbers, as in Theorem 5.7. The theorem guarantees that any combination of algebraic numbers (using field operations) will be algebraic again. For example, $a = \sqrt{2} + \sqrt{3}$ and $b = (5^{1/3} - 1)/(3^{1/5} - 2^{1/6})$ are algebraic. In more concrete terms, this means that $a, b$ are zeros of polynomials with rational coefficients. It is not really very clear how to produce such polynomials systematically from the fact that the ingredients $\sqrt{2}$, $\sqrt{3}$ etc. satisfy polynomial equations, so the proof of Theorem 5.7 is a nice illustration of the power of abstract tools.

Observe also that while $A/\mathbb{Q}$ is of course algebraic, by construction, this extension is not finite. For example, $2^{1/n}$ has minimal polynomial $f = x^n - 2$. To confirm this, we can refer to Eisenstein's criterion with $p = 2$ to establish that $f$ is irreducible, so must be the minimal polynomial. Since $\deg f = n$, it follows that $[\mathbb{Q}(2^{1/n}) : \mathbb{Q}] = n$, so $[A : \mathbb{Q}] \geq n$, and this holds for arbitrary $n \geq 1$.

On the other hand, $A$ is still a countable field because a given polynomial $f \in \mathbb{Q}[x]$ is the minimal polynomial of at most $\deg f$ different numbers and there are only countably many polynomials $f \in \mathbb{Q}[x]$.

*Exercise* 5.8. Find the minimal polynomials $f_a \in \mathbb{Q}[x]$ of $a = \sqrt{2} + \sqrt{3}$ and $a = (1 + 2^{1/3})^{-1}$.

*Exercise* 5.9. Show that $2^{1/6} \notin \mathbb{Q}(2^{1/10})$.

*Exercise* 5.10. Consider a field extension $E/F$, and let $a \in E$ be transcendental. Show that then every $b \in F(a)$, $b \notin F$, is transcendental over $F$.

*Exercise* 5.11. Let $E/F$ be a field extension. Suppose that $a \in E$ is algebraic, with a minimal polynomial of odd degree. Show that then $F(a^2) = F(a)$.

*Exercise* 5.12. Let $E/F$ be an algebraic field extension, and suppose that $R$ is a ring with $F \subseteq R \subseteq E$ (and $R$ is a subring of $E$). Show that $R$ is a field.

Finally, recall our discussion of the prime ring of a given ring $R$ from pg. 71. This was defined as the smallest subring of $R$. Also recall the notion of the *characteristic* of a ring $R$, defined as the smallest integer $n \geq 1$ for which $n1 = 1 + 1 + \ldots + 1 = 0$, or $\mathrm{char}(R) = 0$ if there is no such $n$. If $\mathrm{char}(R) = n$, then the prime ring is isomorphic to $\mathbb{Z}_n$, and it is isomorphic to $\mathbb{Z}$ if $\mathrm{char}(R) = 0$. If $R = F$ is a field, then the characteristic can only be zero or a prime $n = p$ because otherwise $\mathbb{Z}_n$ is not a domain.

We now similarly define the *prime field* of a given field $F$ as the smallest sub*field* of $F$. This can equivalently be described as the smallest subfield that contains the prime ring of $F$. If $\mathrm{char}(F) = p$, then the prime ring $\cong \mathbb{Z}_p$ already is a field and thus coincides with the prime field. If $\mathrm{char}(F) = 0$, then we are looking for the smallest field containing a ring $\cong \mathbb{Z}$, and this will be isomorphic to the field of fractions of $\mathbb{Z}$, which is $\mathbb{Q}$. We summarize:

**Proposition 5.8.** *The characteristic of a field is zero or a prime $p$. The prime field is isomorphic to $\mathbb{Q}$ in the first case and to $\mathbb{Z}_p$ in the second case. If $F$ is a finite field, then* $\mathrm{char}(F) = p \geq 2$*, and in this case, $|F| = p^n$ for some $n \geq 1$.*

*Proof.* Except for the final claims, on finite fields, we discussed this already. Clearly, a field of characteristic zero is infinite because it contains a subfield isomorphic to $\mathbb{Q}$. To see that the order of a finite field is a power of its characteristic, we view it as a vector space over its prime field $P \cong \mathbb{Z}_p$: if $[F : P] = n$, then $F \cong P^n$ as a $P$-vector space, so in particular $|F| = |P|^n = p^n$. □

Later we will see that for each prime power $p^n$, there is exactly one finite field, up to isomorphism, of this order.

*Exercise* 5.13. Are there infinite fields of positive characteristic?

5.2. **Splitting fields.** Let $f \in F[x]$ be a polynomial. We would like to be able to factor ("split") $f$ into linear factors $f = c\prod(x - a_j)$. Of course, this can only work if $F$ contains the roots $a_j$. For example, if $f \in \mathbb{Q}[x]$ is $f = x^2 - 4$, then $f = (x + 2)(x - 2)$, but we cannot factor

$g = x^2 - 2$ in $\mathbb{Q}[x]$ in this way. So, in general, a polynomial will only split in a suitable extension field $E \supseteq F$, and such an $E$ must contain all the roots of $f$, in the sense that if $L \supseteq E$ is an extension of $E$, then all roots of $f$ in $L$ are in fact contained in $E$.

*Exercise* 5.14. Can you prove this (unsurprising) fact in more formal style? So show that if $L \supseteq E \supseteq F$ and $f = \prod(x - a_j)$ in $E[x]$ and $f(b) = 0$ for some $b \in L$, then in fact $b \in E$ (more precisely, $b = a_j$ for some $j$).

**Definition 5.9.** Let $f \in F[x]$. An extension field $E \supseteq F$ is called a *splitting field* of $f$ if $f(x) = c\prod(x - a_j)$ in $E[x]$ and $E = F(a_1, \ldots, a_n)$.

More generally, if $\mathcal{P} \subseteq F[x]$ is a collection of polynomials, then we call $E \supseteq F$ a splitting field for $\mathcal{P}$ if each $f \in \mathcal{P}$ splits in $E$ and, moreover, $E$ is generated by the roots of all $f \in \mathcal{P}$.

So a splitting field is a field extension that lets us factor a given set of polynomials into linear factors, and it is minimal with this property in the sense that it is generated by those roots that we had to adjoin to make the polynomials split. These roots are of course automatically algebraic over the base field, so the following does not come as a surprise.

**Proposition 5.10.** *Let $E \supseteq F$ be a splitting field of a set of polynomials $\mathcal{P} \subseteq F[x]$. Then $E/F$ is algebraic.*

*Proof.* We know that $E = F(S)$, where $S$ is the set of roots of the $f \in \mathcal{P}$. Moreover, by Exercise 5.2, $F(S) = \bigcup F(T)$, with the union taken over the finite subsets $T \subseteq S$.

Let $a \in E$. Then, as just observed, $a \in F(s_1, \ldots, s_n)$ for suitable $s_1, \ldots, s_n \in S$, and this extension $F(s_1, \ldots, s_n)/F$ is finite because the $s_j$ are algebraic over $F$, being roots of polynomials from $F[x]$. □

Splitting fields are easy to find if we can embed $F$ in a larger field that contains roots of polynomials in sufficiently large supply. We make one more definition along these lines.

**Definition 5.11.** A field $F$ is called *algebraically closed* if every non-constant polynomial $f \in F[x]$ has a root in $F$. We call an extension field $E \supseteq F$ an *algebraic closure* of $F$ if $E/F$ is algebraic and $E$ is algebraically closed.

Observe that any polynomial splits in an algebraically closed field $F$ because if $f \in F[x]$ and $f(a) = 0$, then we can factor out the corresponding linear factor, $f = (x - a)g$, but then $g \in F[x]$ has a root too unless $g$ is constant, so we can repeat this step as many times as needed.

*Example* 5.3. Consider $F = \mathbb{Q}$ or $F = \mathbb{R}$. In both cases, we have the field extension $\mathbb{C}/F$, and $\mathbb{C}$ is algebraically closed. So if $f \in F[x]$ is any polynomial, then it splits in $\mathbb{C}$, and if the roots are $a_1, \dots, a_n \in \mathbb{C}$, then $F(a_1, \dots, a_n)$ is a splitting field. For example, if $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, then $\mathbb{Q}(-\sqrt{2}, \sqrt{2}) = \mathbb{Q}(\sqrt{2})$ is a splitting field. Splitting fields of sets of polynomials can be obtained in the same way.

This procedure works for any algebraically closed extension $E \supseteq F$; in particular, we could have taken $E$ as an algebraic closure (if there is one, but, as we will discuss below, these always exist). This doesn't change anything in the case $F = \mathbb{R}$ because $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$, but in the case of $F = \mathbb{Q}$, the much smaller extension field $A$ of the algebraic numbers, as discussed in Theorem 5.7, would have sufficed. As we will show below, in a more general context, $A$ is an algebraic closure of $\mathbb{Q}$; see Theorem 5.19(b).

If a field $F$ does not right away come with an algebraically closed extension, then it is not so obvious how to produce splitting fields; at this point, we can't even be sure that these always exist. For example, $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ does not have a root in $\mathbb{Z}_2$. Is there a splitting field $E \supseteq \mathbb{Z}_2$? Or, more ambitiously, does $\mathbb{Z}_2$ have an algebraic closure?

To attack these questions in a general setting, we recall Theorem 5.2(a). If we already had a field extension $E/F$ that contains a root $a \in E$ of a given polynomial $f \in F[x]$, then $a$ is also contained in the potentially smaller extension field $F(a)$, and this can be described as $F(a) = F[a] \cong F[x]/(f_a)$. We now turn this around to obtain an extension with a zero.

**Lemma 5.12.** *Let $f \in F[x]$ be a non-constant polynomial. Then there is an extension field $E \supseteq F$ that contains a zero of $f$.*

*Proof.* It suffices to discuss the case of an irreducible $f$ because a general polynomial can be factored into irreducible factors. In that case, $E = F[x]/(f)$ is a field, and we can think of $F$ as a subfield of $E$ by identifying $a \in F$ with the corresponding constant polynomial. More formally, we send $a \mapsto a + (f) \in E$ to obtain an embedding of $F$ in $E$; this works because $F \cap (f) = 0$.

Moreover, if we let $t := x + (f) \in E$, then $f(t) = f(x) + (f) = 0$ (in $E$), so $t$ is the desired root of $f$. □

In this form, this looks like a rather abstract construction. Note, however, that we really just implemented the following obvious idea: we want a field extension that contains a root of an irreducible polynomial $f \in F[x]$. To do this, just invent a new element, and call it $t$, say, and insist that $f(t) = 0$. If we can make this work, then the field $E$ we're

trying to build will be spanned by the powers $t^j$, $0 \le j \le n-1$, as an $F$-vector space, since $t$ is algebraic over $F$ with minimal polynomial $f$. We now just add and multiply such linear combinations in the obvious way; to evaluate products, we also make use of the relation $f(t) = 0$. It then needs to be checked that this procedure delivers a field, and this works best in the abstract style from the proof of Lemma 5.12. Recall in this context that we can think of $F[x]$ as $F$ with a new element $x$ adjoined that satisfies no relations. Then passing to the quotient $F[x]/(f)$ amounts to introducing the relation $f(x) = 0$.

For example, $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$: we obtain the field $E = \mathbb{R}[x]/(x^2+1)$ by adjoining a new element $t$ to $\mathbb{R}$, and this satisfies $t^2 + 1 = 0$. The elements of $E$ are represented by linear combinations $a + bt$, $a, b \in \mathbb{R}$, and we add and multiply these formally, and when we multiply, we also make use of the relation $t^2 = -1$. It is clear (especially if you rename $t = i$) that this produces a field isomorphic to $\mathbb{C}$.

*Exercise* 5.15. What happens when we run the procedure from the proof of Lemma 5.12 with a polynomial $f$ that already splits in $F$?

By iterating the basic step from Lemma 5.12, we obtain splitting fields for individual polynomials:

**Corollary 5.13.** *Let $f \in F[x]$. Then $f$ has a splitting field $E \supseteq F$.*

*Proof.* Let $E_1$ be a field as in Lemma 5.12, with $f(a_1) = 0$ for some $a_1 \in E_1$. Then $f = (x - a_1)f_2$ in $E_1[x]$. We now repeat this step to obtain a field $E_2 \supseteq E_1$ with a zero $a_2 \in E_2$ of $f_2$ etc. until we have enough zeros $a_j$ so that $f$ splits in $E_n$. Then $E = F(a_1, \dots, a_n)$ is a splitting field. □

*Example* 5.4. Let's now return to the example $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ that was mentioned above. This polynomial is irreducible because a non-unit proper factor would have to be linear, but $f(0) = f(1) = 1$, so $f$ has no roots in $\mathbb{Z}_2$. Let's follow the procedure from Lemma 5.12, in the concrete version discussed after the proof. Let's form $E = \mathbb{Z}_2(t)$, where $f(t) = 0$. Notice that $E$ is a splitting field already because $f = (x-t)g$ in $E[x]$, but here $g$ must be linear also, so $f$ splits in $E[x]$.

We have that $[E : \mathbb{Z}_2] = 2$ (why?), so the elements of $E$ are $a + bt$, $a, b \in \mathbb{Z}_2$. There are four of these, and we add and multiply in the obvious way, with help from the relation $f(t) = 0$ in the case of multiplication. For example, $t(1 + t) = t + t^2 = -1 = 1$. One can now check, by comparing the addition and multiplication tables, that we have recovered the field with four elements from Example 4.5; in fact, we saw in that example that this field may be obtained as $\mathbb{Z}_2[x]/(x^2+x+1)$, which is exactly the construction from Lemma 5.12,

specialized to our situation. (Also, as mentioned earlier, there is only one finite field of order $p^n$ for any possible order, so it has to be this one.)

*Example* 5.5. Consider now $f = x^3 + x + 1 \in \mathbb{Z}_2[x]$. This is again irreducible, by the same argument: a non-trivial factorization would have to contain a linear factor, but $f(0) = f(1) = 1$. Proceed as in the preceding example and adjoin a root $t$ and form $E = \mathbb{Z}_2(t)$. This time, $[E : \mathbb{Z}_2] = 3$, so $E$ contains the eight elements $a + bt + ct^2$, $a, b, c \in \mathbb{Z}_2$. We also have the factorization

$$f = x^3 + x + 1 = (x - t)(x^2 + tx + t^2 + 1) = (x - t)g$$

(check that this is correct, or run a long division style algorithm to find this systematically).

Now a splitting field for $f$ must contain roots of $g \in E[x]$ also. We don't know at this point if these are already in $E$, or if we need to adjoin further elements. If we just try out the eight elements of $E$, then we find that

$$g(t^2) = t^4 + t^3 + t^2 + 1 = t^2 + t + t + 1 + t^2 + 1 = 0$$

(recall that $\mathrm{char}(E) = 2$, so $a + a = 0$ for all $a \in E$). So $g$ does have a zero in $E$, and since $\deg g = 2$, this means that $g$ splits in $E$. We have shown that $E$ is a splitting field of $f$.

*Exercise* 5.16. Find the third root of $f$ in $E$.

*Example* 5.6. Let's now discuss $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ in the same style, by successively adjoining roots. We already observed earlier that our task is easier here because $\mathbb{C} \supseteq \mathbb{Q}$ is an algebraically closed extension, and splitting fields can be obtained as subfields of $\mathbb{C}$. We adjoint $t_1 = \sqrt{2}$ and form $E_1 = \mathbb{Q}(\sqrt{2})$. Obviously, $E_1$ contains a second root $t_2 = -\sqrt{2}$, and $f = (x - \sqrt{2})(x + \sqrt{2})$ splits completely already in $E = E_1$. Notice that $[E : \mathbb{Q}] = 2$.

Now let's look at $f = x^3 - 2 \in \mathbb{Q}[x]$ in the same way. We adjoin $t_1 = 2^{1/3}$, form $E_1 = \mathbb{Q}(2^{1/3})$, and split off $x - 2^{1/3}$ in $E_1[x]$. This gives $f = (x - 2^{1/3})(x^2 + 2^{1/3}x + 2^{2/3}) = (x - 2^{1/3})g$. We of course know that the zeros of $g$ in $\mathbb{C}$ are $2^{1/3}e^{2\pi ik/3}$, $k = 1, 2$. These are not in $E_1$; the elements of $E_1$ are $a + b2^{1/3} + c2^{2/3}$, $a, b, c \in \mathbb{Q}$, and these are all real. Therefore, we must adjoin another zero, let's say $t_2 = 2^{1/3}e^{2\pi i/3}$, and form $E_2 = E_1(t_2) = \mathbb{Q}(t_1, t_2)$. Now $f$ splits in $E = E_2$, so this is a splitting field. We obtained $E_2$ from $\mathbb{Q}$ by first doing a three-dimensional extension and then a two-dimensional extension, so $[E : \mathbb{Q}] = 2 \cdot 3 = 6$.

*Exercise* 5.17. Let $E \supseteq F$ be a splitting field of $f \in F[x]$, and thus $f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$ in $E[x]$. Show that then $E = F(a_1, a_2, \ldots, a_{n-1})$.

*Exercise* 5.18. Let $f \in F[x]$, $\deg f = n$, and let $E \supseteq F$ be a splitting field of $f$. Show that then $[E:F] \leq n!$.

*Exercise* 5.19. Let $E$ be a splitting field over $\mathbb{Q}$ of: (a) $f(x) = x^4 - 1$; (b) $f(x) = x^4 + 1$; (c) $f(x) = x^4 + 2$; (d) $f(x) = x^4 + 4$. Find $[E:\mathbb{Q}]$ in each case (this dimension will not depend on how you construct a splitting field, as we will show below).

*Exercise* 5.20. Let $f \in F[x]$ be irreducible, with $\deg f = n \geq 1$, and let $g \in F[x]$ be an arbitrary polynomial. (a) Show that $h(x) = f(g(x))$ need not be irreducible; (b) show that the degree of each irreducible factor of $h$ is a multiple of $n$. *Suggestion:* Let $a$ be a zero of $h$ in a splitting field. What can you say about $[F(a):F]$?

Next, we discuss uniqueness of splitting fields. We return to Lemma 5.12, and we now want to show that the underlying procedure (adjoin a root of an irreducible polynomial) always gives the same result in the sense that any simple extension by a root of a given irreducible polynomial is isomorphic to the one from Lemma 5.12. Basically, this seems clear already, from the comments on the proof that we made, but we'll give a precise formal treatment, and we will in fact consider a slightly more general situation, which will involve two isomorphic fields. We will tacitly extend such an isomorphism $\varphi : F_1 \to F_2$ to an isomorphism $F_1[x] \to F_2[x]$ of the polynomial rings by mapping field elements by $\varphi$ and sending $x \mapsto x$. If $f_1 \in F_1[x]$, I'll just write $f_2$ for the image of $f_1$ under this isomorphism.

**Lemma 5.14.** *Let $F_j$ be isomorphic fields, with an isomorphism $\varphi : F_1 \to F_2$. Let $E_j/F_j$ be field extensions, and suppose that $a_1 \in E_1$ is algebraic, with minimal polynomial $f_1 \in F_1[x]$. Suppose that $E_2$ contains a root $a_2$ of $f_2 \in F_2[x]$. Then $\varphi$ may be extended to an isomorphism $\varphi : F_1(a_1) \to F_2(a_2)$ that sends $a_1 \mapsto a_2$.*

*Proof.* We'll make two attempts here, the first one in concrete style, and then a more abstract version of essentially the same argument, more in line with the proof of Lemma 5.12 we gave above.

Observe first of all that $f_1$ is irreducible, being a minimal polynomial, and thus so is $f_2$. If $n$ denotes the (common) degree, then $[F_j(a_j) : F_j] = n$, and a basis is given by the powers $a_j^k$, $k = 0, 1, \ldots, n-1$. So if we want a $\varphi : F_1(a_1) \to F_2(a_2)$ as in the statement of the Lemma,

we are really forced to map

$$b_0 + b_1 a_1 + \ldots + b_{n-1} a_1^{n-1} \mapsto \varphi(b_0) + \varphi(b_1) a_2 + \ldots + \varphi(b_{n-1}) a_2^{n-1}.$$

Or, in more compact notation, we send $g_1(a_1) \mapsto g_2(a_2)$, where $g_1 \in F_1[x]$, and $g_2 \in F_2[x]$ is the image of $g_1$ under the isomorphism $F_1[x] \to F_2[x]$ that is induced by $\varphi$. At first sight, it seems completely obvious that this map is a homomorphism, but something must be missing here because we will certainly have to use the fact that $f_2(a_2) = 0$ at some point.

*Exercise* 5.21. Can you elaborate on this? Complete the argument please. What goes wrong here if we take other elements $a_2 \in E_2$ instead of a root of $f_2$?

Now let's start over and give a second proof, or it would perhaps be more accurate to say that we are going to give a second, abstract version of the same argument. Recall that $F_j(a_j) \cong F_j[x]/(f_j)$. More specifically, we map $F_j[x] \to F_j(a_j)$, $b \mapsto b$ ($b \in F_j$), $x \mapsto a_j$, and since the kernel of this map is the ideal $(f_j)$, we obtain an isomorphism between $F_j[x]/(f_j)$ and $F_j(a_j)$. This isomorphism maps $x + (f_j) \mapsto a_j$. We can now obtain the desired isomorphism from the following diagram:

$$\begin{array}{ccc} F_1[x] & \xrightarrow{\quad\varphi\quad} & F_2[x] \\ {\scriptstyle q_1}\downarrow & \swarrow & \downarrow{\scriptstyle q_2} \\ F_1[x]/(f_1) & \xrightarrow[\psi]{} & F_2[x]/(f_2) \end{array}$$

First obtain a homomorphism along the diagonal by composing $q_2 \circ \varphi$. Since $\varphi$ is an isomorphism, the kernel of this map is $\varphi^{-1}((f_2)) = (f_1)$, and this is exactly the kernel of $q_1$, so by factoring through this quotient $F_1[x]/(f_1)$, we obtain an isomorphism $\psi$ along the bottom row. Since $\varphi(x) = x$, we have that $\psi(x + (f_1)) = x + (f_2)$, so if we now identity the quotients $F_j[x]/(f_j)$ with the $F_j(a_j)$, using the isomorphisms that were set up above, then $b \mapsto \varphi(b)$ for $b \in F_1$ and $a_1 \mapsto a_2$, as desired. □

**Definition 5.15.** Let $E/F$ be a field extension. We say that two elements $a, b \in E$ are *conjugates* if they (are algebraic and) have the same minimal polynomial.

For example, $\pm\sqrt{2}$ are conjugates in $\mathbb{C}/\mathbb{Q}$ because both elements share the minimal polynomial $f = x^2 - 2$.

*Exercise* 5.22. Consider the field extension $\mathbb{C}/\mathbb{Q}$. Find all conjugates of the following elements $a \in \mathbb{C}$: (a) $a = 1 + \sqrt{5}$; (b) $a = 1 + i$; (c) $a = (1 + i)/\sqrt{2}$

If we specialize Lemma 5.14 to $F_1 = F_2 =: F$, $E_1 = E_2 =: E$, and $\varphi$ the identity of $F$, then we obtain that $a, b \in E$ are conjugates precisely if there exists an isomorphism $F(a) \to F(b)$ that maps $a \mapsto b$ and leaves $F$ invariant pointwise. We make a formal definition along these lines:

**Definition 5.16.** Let $E_j/F$, $j = 1, 2$, be field extensions. An *$F$-homomorphism* is a homomorphism $\varphi : E_1 \to E_2$ that fixes $F$ pointwise, that is, $\varphi(a) = a$ for all $a \in F$.

In particular, we can consider $F$-automorphisms of a field extension $E/F$; these are the central objects of *Galois theory,* and we will study them in detail in the next chapter.

To state our observation from above one more time in this new terminology, we can now say that if $E/F$ is a field extension, then two algebraic elements $a, b \in E$ are conjugate precisely if there is an $F$-isomorphism $\varphi : F(a) \to F(b)$ with $\varphi(a) = b$. In fact, all this basically just restates one more time what we noticed earlier, namely that, up to isomorphism, the relevant information about the algebraic structure of $F(a)$ is contained in the minimal polynomial of $a$ over $F$.

*Exercise* 5.23. Let $E/F$ be a field extension, and assume that $a, b \in E$ are transcendental. Show that there is an $F$-isomorphism $\varphi : F(a) \to F(b)$ that maps $\varphi(a) = b$.

*Exercise* 5.24. Show that extensions by more than one zero of an irreducible polynomial need not be isomorphic. More specifically, find an example of an irreducible polynomial $f \in F[x]$ such that $F(a_1, a_2) \ncong F(a_3, a_4)$ for suitable zeros $a_j$ of $f$ (do this for $F = \mathbb{Q}$ perhaps).

Just as iterating the step from Lemma 5.12 gave us the existence of splitting fields, their uniqueness will now follow by repeatedly applying Lemma 5.14. As above, we first deal with the following slightly more general situation: let $\varphi : F_1 \to F_2$ be an isomorphism, and extend this to an isomorphism $F_1[x] \to F_2[x]$, by sending $a \mapsto \varphi(a)$, $a \in F_1$, $x \mapsto x$. Let $f_1 \in F_1[x]$, and denote its image by $f_2 \in F_2[x]$.

**Theorem 5.17.** *In the situation just described, if $E_j \supseteq F_j$ is a splitting field of $f_j$ ($j = 1, 2$), then $\varphi : F_1 \to F_2$ can be extended to an isomorphism $E_1 \to E_2$.*

**Corollary 5.18.** *Let $E_1, E_2 \supseteq F$ be splitting fields of an $f \in F[x]$. Then $E_1 \cong E_2$; in fact, there is an $F$-isomorphism between these fields.*

To obtain the Corollary from the Theorem, we take $F_1 = F_2 = F$ and let $\varphi : F \to F$ be the identity map.

*Proof.* As already announced, essentially this just follows by applying Lemma 5.14 repeatedly. We organize the formal argument as an induction on $\deg f_1$. The claim is of course clear if $\deg f_1 \leq 1$ because then $E_j = F_j$.

So assume now that $\deg f_1 > 1$, and assume also that the claim holds for all polynomials of smaller degree (= induction hypothesis). Let $a_1 \in E_1$ be a root of a monic irreducible factor $g_1 \in F_1[x]$ of $f_1$. Let $a_2 \in E_2$ be a root of its image $g_2 \in F_2[x]$. Now Lemma 5.14 provides an extension of $\varphi$ that maps $F_1(a_1)$ isomorphically onto $F_2(a_2)$ and sends $a_1 \mapsto a_2$. Split off the corresponding linear factors: write $f_j = (x - a_j)h_j$, with $h_j \in F_j(a_j)[x]$. These polynomials have smaller degree, and $E_j$ is a splitting field of $h_j$ over $F_j(a_j)$, so now the induction hypothesis lets us extend to an isomorphism $E_1 \to E_2$. □

*Exercise* 5.25. Where in these final steps do we make use of the fact that the continuation of $\varphi$ (which maps $F_1(a_1) \to F_2(a_2)$) sends $a_1 \mapsto a_2$?

*Exercise* 5.26. Let $p$ be a prime. Show that the polynomial

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1} \in \mathbb{Z}[x]$$

is irreducible in $\mathbb{Q}[x]$. *Suggestion:* Replace $x$ by $x + 1$ and discuss the resulting polynomial with the help of Eisenstein's criterion.

*Exercise* 5.27. Find a splitting field $E \subseteq \mathbb{C}$ and determine $[E : \mathbb{Q}]$ for $f(x) = x^6 - 1 \in \mathbb{Q}[x]$.

**Theorem 5.19.** *(a) An extension field $E \supseteq F$ is an algebraic closure of $F$ if and only if $E$ is a splitting field for $\mathcal{P} = F[x]$.*

*(b) Let $E/F$ be a field extension, and suppose that $E$ is algebraically closed. Then the field $A$ of algebraic numbers (compare Theorem 5.7) is an algebraic closure of $F$.*

*Proof.* (a) If $E$ is an algebraic closure, then $E$ is in particular algebraically closed, so any $f \in F[x]$ splits in $E$. Moreover, any $a \in E$ is algebraic over $F$, so is a zero of some $f \in F[x]$. This shows that $E$ is generated by the zeros of the $f \in F[x]$, and it follows that $E$ is a splitting field for $F[x]$.

Conversely, suppose now that $E$ is a splitting field for $F[x]$. Then $E/F$ is algebraic by Proposition 5.10. To show that $E$ is algebraically closed, let $f \in E[x]$ be a non-constant polynomial. Let $a$ be a root of $f$, in an extension field $E(a)$ if necessary. Then $a$ is algebraic over $E$, but also over $F$, by Theorem 5.6 and Proposition 5.10. Let $f_E$, $f_F$ be the minimal polynomials of $a$ over $E$ and $F$, respectively. Then $f_F \in E[x]$ also, so $f_E | f_F$ in $E[x]$. However, $f_F = \prod(x - b_j)$ splits in $E$. Since

$f_E$ is irreducible, this shows that $f_E = x - b_j$, and thus $a = b_j \in E$. We have found a root $a \in E$ of $f \in E[x]$, and this shows that $E$ is algebraically closed.

(b) $A$ is clearly a splitting field for $\mathcal{P} = F[x]$, so this follows from part (a). □

So since algebraic closures are also splitting fields (for *all* polynomials over the base field), we can perhaps expect results similar to the ones we established above for splitting fields of individual polynomials. This impression is correct, and in fact the same basic ideas still work. However, additional technical problems arise, which are not particularly relevant for us, so I'll just report quickly on this.

**Theorem 5.20.** *(a) Every field has an algebraic closure.*
*(b) If $E_1, E_2 \supseteq F$ are algebraic closures of $F$, then there is an $F$-isomorphism between them.*

In view of part (b) of the Theorem and Corollary 5.18 above, it also makes sense to speak of *the* algebraic closure of a given field and *the* splitting field of a polynomial.

*Exercise* 5.28. Show that the algebraic closure of any field is infinite. *Hint:* If $E = \{a_1, a_2, \ldots, a_n\}$, find an $f \in E[x]$ with $f(a_j) \neq 0$ for all $j$.

*Exercise* 5.29. Do the following fields have irreducible polynomials $f \in F[x]$ of arbitrarily high degree? If not, then find the maximal degree of an irreducible polynomial. (a) $F = \mathbb{R}$; (b) $F = \mathbb{C}$; (c) $F = \mathbb{Q}$; (d) $F = \mathbb{Z}_2$. *Suggestion:* Use the previous Exercise for part (d).

We are now also in a great position to evaluate, one more time, Hamilton's quest for field structures on $\mathbb{R}^n$ that come from an algebra structure. Note that in any algebra $A$ (with multiplicative identity 1), the field of scalars $F$ is naturally embedded in $A$ via the map $F \to A$, $c \mapsto c1$; moreover, (algebra) multiplication by $c1 \in A$, $c \in F$, then is really the same as (scalar) multiplication by $c \in F$. In the case at hand this means that $\mathbb{R}^n$ with a field structure of the desired type would automatically be a field extension of $\mathbb{R}$, and $[\mathbb{R}^n : \mathbb{R}] = n$. Since this is finite, such a field would be an algebraic extension of $\mathbb{R}$, so the following observation puts Hamilton's original hopes to rest once and for all.

**Theorem 5.21.** *Let $F/\mathbb{R}$ be an algebraic field extension. Then $F = \mathbb{R}$ or $F \cong \mathbb{C}$.*

*Proof.* If $F \neq \mathbb{R}$, then pick an $a \in F$, $a \notin \mathbb{R}$. Its minimal polynomial $f_a \in \mathbb{R}[x]$ is irreducible, so must be of degree 2, as discussed above, in

Example 5.1. Then $f_a = (x-a)g$ splits in $\mathbb{R}(a)$; note that necessarily $\deg g = 1$ here. Another splitting field of $f_a$ is obtained by letting the complex roots $b, \overline{b} \in \mathbb{C}$ generate a subfield of $\mathbb{C}$, but since $b \notin \mathbb{R}$, this is just $\mathbb{C}$ itself. So $\mathbb{R}(a) \cong \mathbb{C}$ by Corollary 5.18.

Now $\mathbb{R}(a)$ does not admit further algebraic extension since this field is algebraically closed: if $b \in F$, then its minimal polynomial over $\mathbb{R}(a)$ splits over $\mathbb{R}(a) \cong \mathbb{C}$ (any polynomial does), so is linear and thus $b \in \mathbb{R}(a)$. □

If the requirement of commutativity is dropped, then success is possible: Hamilton's quaternions are a four-dimensional $\mathbb{R}$-algebra that, at the same time, is a division ring. The leap from two dimensions, for $\mathbb{C} = \mathbb{R}^2$, to four is necessary. This follows from essentially the same arguments: an extension by a single element, $\mathbb{R}(a)$, is necessarily two-dimensional because irreducible polynomials of other degrees $> 1$ are unavailable as minimal polynomials (and minimal polynomials are irreducible because the extension $F \supseteq \mathbb{R}$ is a domain). This part of the argument does not require commutativity of $F$, and, in fact, it *follows* that $\mathbb{R}(a)$ is commutative (and then again $\mathbb{R}(a) \cong \mathbb{C}$) because $1, a$ is a possible basis of $\mathbb{R}(a)$ as an $\mathbb{R}$-vector space. If $\mathbb{R}(a)$ isn't all of $F$ yet, then any further extension can be viewed as a $\mathbb{C}$-vector space (though not as a $\mathbb{C}$-algebra!), and thus its dimension over $\mathbb{R}$ is at least 4.

More careful analysis reveals that $\mathbb{H}$, $\mathbb{C}$, $\mathbb{R}$ are the only division rings that are at the same time finite-dimensional algebras over $\mathbb{R}$ (or, in short, they are the only finite-dimensional *division algebras* over $\mathbb{R}$).