Proposition 5.5.2 *Let V be a finite-dimensional vector space over F. Let $n = \dim_F(V)$ and let $B \subseteq V$. Any two of the following three conditions implies that B is a basis, and hence imply the third condition.*

1. *B is linearly independent.*
2. *B is a spanning set for V.*
3. *B has n elements.*

Exercise 5.5.2. Prove Proposition 5.5.2

Proposition 5.5.3 *If V is f.d. with $dim_F(V) = n$ then V is isomorphic to F^n.*

Corollary 5.5.4 *If F is countable and V is f.d. over F, then V is countable.*

It follows from this corollary that $\mathbb{R}$ is not finite dimensional as a vector space over $\mathbb{Q}$. It can be easily shown, using set theoretic cardinality arguments, that a basis for $\mathbb{R}$ as a v.s. over $\mathbb{Q}$ has to be uncountable.

Corollary 5.5.5 *If F is finite and V is f.d. over F, then V is finite. More precisely, if $|F| = q$ and $\dim_F(V) = n$ then $|V| = q^n$.*

Corollary 5.5.6 *If F is finite then $|F|$ is a power of a prime.*

Proof. Since F is finite, its characteristic cannot be zero. By Theorem **??** its prime subfield is isomorphic to $\mathbb{Z}_p$ where $p = \text{char}(F)$. The result now follows from the Corollary 5.5.5, and the fact that F is a v.s. over $\mathbb{Z}_p$. ■

Unlike what happens with groups and rings, where we have groups and rings of all finite cardinalities, the only finite cardinalities where we can have fields are the prime powers. There is no field of cardinality 6. More on finite fields in Section 6.6, where we'll give a complete classification of finite fields.

Part IV

Fields

field extension
extension
degree
index
finite extension
extension!finite
infinite extension
extension!infinite

Chapter 6

Field Theory

6.1 Field Extensions

Definition 6.1.1. Let F be a subfield of E. We say that E is a *field extension* of F, or just an *extension* of F. The dimension $\dim_F(E)$ of E as a vector space over F is called the *degree* or *index* of the extension, and it is denoted by $[E : F]$. We often refer to the pair of fields E and F as the "extension E/F". In this context, the bar / does **not** denote a quotient. Sometimes we picture this situation as follows:

$$\begin{array}{c} E \\ | \\ F \end{array} \qquad \text{or as} \qquad \begin{array}{c} E \\ | \, d \\ F \end{array}$$

where $d = [E : F]$.

We say that E is a *finite extension* of F, if it is an extension of finite degree. Otherwise we say that it is an *infinite extension*.

Examples 6.1.1. 1. E/F is an extension of degree 1 iff $E = F$.

2. As we have seen in Example **??**

$$\mathbb{Q}[\sqrt{2}\,] = \{a + b\sqrt{2}\,|a, b \in \mathbb{Q}\}$$

algebraic
transcendental
algebraic
transcendental
algebraic numbers

is a field. It clearly contains $\mathbb{Q}$ as a subfield, so $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ is a field extension. It is easy to see that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$, so we have an extension of degree 2.

3. $\mathbb{R}/\mathbb{Q}$ is an infinite field extension.

4. $\mathbb{C}/\mathbb{R}$ is an extension of degree 2, with basis $\{1, i\}$.

6.2 Algebraic Extensions

Proposition 6.2.1 *Let E/F be a finite extension with $n = [E : F]$. For each $\alpha \in E$, there is $f(x) \in F[x]$ such that $f(\alpha) = 0$. Moreover, $f(x)$ can be chosen such that $\deg(f(x)) \leq n$ and $f(x)$ is monic.*

Definition 6.2.1.

- Given $\alpha \in E/F$, we say that α is *algebraic* over F, if there is $f(x) \in F[x]$ such that $f(\alpha) = 0$. When $f(x)$ is of smallest possible degree k, we say that α has degree k over F, and write $\deg_F(\alpha) = k$.
- If α is not algebraic over F, we say that it is *transcendental* over F.
- We say that the extension E/F is *algebraic* is every $\alpha \in E$ is algebraic over F, otherwise we say that the extension is *transcendental*.

Board presentations PS 03 02/20/19

Test 1 02/22/19

Test 1 revisited 02/25/19

02/26/10

Examples 6.2.1.

1. $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$, so $\sqrt{2}$ is algebraic over $\mathbb{Q}$. Complex numbers that are algebraic over $\mathbb{Q}$ are called *algebraic numbers*.

2. The imaginary number i is a root of $x^2 + 1 \in \mathbb{R}[x]$, so it is algebraic over $\mathbb{R}$. It is also algebraic over $\mathbb{Q}$, so it is an algebraic number.

3. The numbers π and e are transcendental over $\mathbb{Q}$. We say they are *transcendental numbers*. We omit the proof here. transcendental numbers

4. Consider the real number $\alpha = \sqrt{2} + \sqrt{3}$. We have $\alpha^2 = 5 + 2\sqrt{6}$, so $(\alpha^2 - 5)^2 = 24$, i.e. $\alpha^4 - 10\alpha^2 + 1 = 0$. This shows that α is a root of the polynomial
$$f(x) = x^4 - 10x^2 + 1,$$
hence algebraic. Very similar calculations show that the four numbers $\pm\sqrt{2} \pm \sqrt{3}$ are roots of $f(x)$, and since $\deg(f(x)) = 4$, these are all the roots of $f(x)$, and they are all algebraic.

Remark 6.2.1. Algebraic v/s transcendental, can be seen in terms of the evaluation homomorphism. For $\alpha \in E$, consider

$$\begin{array}{rccc} \mathrm{ev}_\alpha : & F[x] & \to & E \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

α is transcendental over F iff ev_α is injective.

We can rephrase part of Proposition 6.2.1 as follows.

Theorem 6.2.2 *Every finite extension is algebraic.*

Proposition 6.2.3 *Let E/F be an extension and $\alpha \in E$. The kernel of the evaluation homomorphism $\mathrm{ev}_\alpha : F[x] \to E$, i.e.*

$$\{f(x) \in F[x] | f(\alpha) = 0\}$$

is an ideal of $F[x]$. Since $F[x]$ is a PID, this kernel is a principal ideal. When this kernel is non-zero, i.e. when α is algebraic over F, for $0 \neq f(x) \in F[x]$ TFAE:

i) $\ker(\mathrm{ev}_\alpha) = \langle f(x) \rangle$,

ii) $f(\alpha) = 0$ *and* $f(x)$ *is irreducible over* F, *(i.e. irreducible in* $F[x]$*)*

iii) $f(x)$ *is a polynomial of minimal degree in* $F[x]$ *having* α *as a root.*

Moreover, all polynomials satisfying these equivalent conditions are associate to each other, and there is a unique monic polynomial satisfying these properties.

minimal polynomial

Proof. ($i \iff iii$) Follows from the proof of Proposition 4.2.1.
($iii \Rightarrow ii$) Since $F[x]$ is a UFD, $f(x)$ has an irreducible factor which has α as a root. By minimality of $\deg(f(x))$, $f(x)$ and this irreducicible factor must have the same degree, hence they are associates. That makes $f(x)$ irreducible by Exercise 4.3.1.
($ii \Rightarrow i$) Assume $f(\alpha) = 0$ and $f(x)$ is irreducible over F. $f(\alpha) = 0$ yields $p(x) \in \ker(\mathrm{ev}_\alpha)$, hence $\langle f(x)\rangle \leq \ker(\mathrm{ev}_\alpha)$. For the other inclusion, let $g(x)$ be a generator of $\ker(\mathrm{ev}_\alpha)$. Then $f(x) = g(x)h(x)$ for some $h(x) \in F[x]$. Since $f(x)$ is irreducible, by Note 4.3.1, $f(x)$ must be associate to either $h(x)$ or $g(x)$, making the other factor a constant. However, $g(x)$ is not contant since $g(\alpha) = 0$. Therefore $f(x)$ is associate to $g(x)$, and by Proposition 4.2.5, $\langle f(x)\rangle = \langle g(x)\rangle = \ker(ev[\alpha])$.
The moreover part also follows from Proposition 4.2.5. To get a monic, take any generator and divide by the leading coefficient. For uniqueness, note that two associate monic polynomials must be equal. ■

Definition 6.2.2. For $\alpha \in E/F$, algebraic over F, the unique monic polynomial satisfying the properties in Proposition 6.2.3 is called the *minimal polynomial* of α over F, and it is denoted $\min_F(\alpha)$. The degree of this minimal polynomial is called the degree of α over F, and it is denoted $\deg_F(\alpha)$.

Proposition 6.2.3 gives us three equivalent conditions for $f(x)$ to be the minimal polynomial of α over F. The first one is often used when one has the minimal polynomial. The other two are often used to show that a polynomial is the minimal polynomial.

Examples 6.2.2.

1. Since $x^2 - 2$ has no rational roots, it is irreducible over $\mathbb{Q}$, hence $\min_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2$, and $\deg_{\mathbb{Q}}(\sqrt{2}) = 2$.

2. Since $x^2 + 1$ has no real roots, it is irreducible over $\mathbb{R}$, and $\min_{\mathbb{R}}(i) = x^2 + 1$. Moreover, $\deg_{\mathbb{R}}(i) = 2$.

3. Find the minimal polynomial and the degree of $\alpha = \sqrt{1 + \sqrt{3}}$ over Q. Since $\alpha^2 = 1 + \sqrt{3}$, we have $(\alpha^2 - 1)^2 = 3$, i.e. $\alpha^4 - 2\alpha^2 - 2 = 0$, so α is a root of $x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$. This polynomial is irreducible by Eisenstein's criterion, so $\min_{\mathbb{Q}}(\alpha) = x^4 - 2x^2 - 2$, and $\deg_{\mathbb{Q}}(\alpha) = 4$.

4. Find the minimal polynomial and the degree of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. We have already seen in Example 6.2.1.4, that $\alpha = \sqrt{2} + \sqrt{3}$ is a

root of $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. We claim that this polynomial is irreducible, hence it is the minimal polynomial, and $\deg_{\mathbb{Q}}(\alpha) = 4$. Note first, that $f(x)$ has no rational roots, and by Corollary 4.1.4 it has no linear factors. That still leaves the possibility of $f(x)$ factoring as a product $f(x) = g(x)h(x)$ of two quadratic factors. That would mean that the four roots of $f(x)$ split into two for $g(x)$ and the other two for $h(x)$. The four roots of $f(x)$ are $\pm\sqrt{2} \pm \sqrt{3}$, and the two that go with $g(x)$ must be such that their sum and their product are rational. One can easily check that there is no such pair. So $f(x)$ is irreducible over $\mathbb{Q}$.

In Proposition 6.2.1 we begin with an element α of a finite extension of F, and find a polynomial $f \in F[x]$ that has α as a root. We now want to go in the opposite direction. Given a polynomial $f \in F[x]$ we want to find a root α in some finite extension of F. We need some preparation work before we get there.

Proposition 6.2.4 *Let D be a PID and $0 \neq p \in D$. p is irreducible iff $\langle p \rangle$ is a maximal (proper) ideal of D.*

Proof. ($\Rightarrow$) Suppose p is irreducible, and $\langle p \rangle \subsetneqq I \leq D$ for some ideal I. Let $a \in I$ such that $a \notin \langle p \rangle$. Since p is irreducible and $p \nmid a$ we have that g.c.d.$(a, p) \sim 1$. Since D is a PID, there are $\alpha, \beta \in D$ such that

$$1 \sim \text{g.c.d.}(a, p) \sim \alpha a + \beta p \in I.$$

Therefore $I = D$.
($\Leftarrow$) Suppose $\langle p \rangle$ is a maximal proper ideal of D. By hypothesis, p is nznu. Assume $p = ab$ for some $a, b \in D$. If $p \mid a$ then $p \sim a$. Otherwise, $p \nmid a$, i.e. if $a \notin \langle p \rangle$, then $\langle p \rangle + \langle a \rangle = D$ and there exist $\alpha, \beta \in D$ such that $1 = \alpha a + \beta p$. We now have $b = \alpha ab + \beta pb = \alpha p + \beta pb$ is divisible by p, so $p \sim b$. ∎

Note that the hypothesis of D being a PID is used only in one direction. For an arbitrary ID we have:

$$\begin{array}{ccc} p \text{ is prime} & \Leftrightarrow & \langle p \rangle \text{ is a prime ideal} \\ \Downarrow & & \Uparrow \\ p \text{ is irreducible} & \Leftarrow & \langle p \rangle \text{ is a maximal ideal} \end{array}$$

In the UFD $D = \mathbb{Z}[x]$ we have x is irreducible, but $\langle x\rangle \lneq \langle 2, x\rangle \lneq D$, and $\langle x\rangle$ is not a maximal ideal. Thus, the hypothesis PID is needed for the bottom left to right direction.

When D is a PID, the one-way implications become equivalences and we have.

$$\begin{array}{ccc} p \text{ is prime} & \Leftrightarrow & \langle p\rangle \text{ is prime ideal} \\ \Updownarrow & & \Updownarrow \\ p \text{ is a irreducible} & \Leftrightarrow & \langle p\rangle \text{ is a maximal ideal} \end{array}$$

02/27/19

Corollary 6.2.5 *Let F be a field, and $f(x) \in F[x]$. If $f(x)$ is irreducible over F then $F[x]/\langle f(x)\rangle$ is a field.*

Recall the following notation from Chapter 3. For R, S rings with R a subring of S and $\alpha \in S$, we denote by $R[\alpha]$ the smallest subring of S that contains both R and α. For example, $\mathbb{Z}[\sqrt{-5}]$ is the smallest subring of $\mathbb{C}$ that contais $\mathbb{Z}$ and $\sqrt{-5}$. From Lemma 3.0.1 we ahve that the elements of $R[\alpha]$ consists of sums of powers of α multiplied by elements of R,

$$r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_n\alpha^n$$

that is, the image of the evaluation map

$$\mathrm{ev}_\alpha : R[x] \to S.$$

Now, when F, E are fields with F a subfield of E and $\alpha \in E$, we denote by $F(\alpha)$ the smallest subfield of E that contains both F and α. For example, $\mathbb{Q}(\sqrt{2}$ is the smallest subfield of $\mathbb{R}$ that contains both $\mathbb{Q}$ and $\sqrt{2}$. From Lemma 3.0.2, the elements of $F(\alpha)$ consists of all quotients of sums of powers of α times elements of R. In other words, $F(\alpha)$ is the field of fractions of $F[\alpha]$, and $F[\alpha]$ is a subring of $F(\alpha)$. We have shown that the ring $\mathbb{Q}[\sqrt{2}]$ is actually a field, so it follows that $\mathbb{Q}[\sqrt{2}]$=$\mathbb{Q}(\sqrt{2})$.

Examples 6.2.3. 1. $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible, so $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is a field. But we can do better. Note that $x^2 - 2 = \min_{\mathbb{Q}}(\sqrt{2})$, so $\langle x^2 - 2\rangle$

equals the kernel of the evaluation homomorphism $\mathrm{ev}_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}$. By the first isomorphism theorem $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is isomorphic to the image of $\mathrm{ev}_{\sqrt{2}}$, which is $\mathbb{Q}[\sqrt{2}]$, confirming that it is a field.

2. $x^2 + 1$ is irreducible over $\mathbb{R}$. A similar argument shows that
$$\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C} \approx \mathbb{R}[x]/\langle x^2 + 1\rangle.$$

3. The polynomial $x^2+x+1 \in \mathbb{Z}_2[x]$ is irreducible. Therefore, the quotient $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ is a field. We will say more about this example.

The following lemma follows immediately from the fact that a field F is a simple ring, i.e. has no ideals other that F and $\{0\}$.

Lemma 6.2.6 *Let F be a field, R a non-trivial ring, and $\varphi : F \to R$ a ring homomorphism. Then φ is injective, and R contains a subfield, $\varphi(F)$, isomorphic to F.*

Example 6.2.4. This is a continuation of Example 6.2.3.3. Let $f(x) = x^2 + x + 1$, $I = \langle f(x)\rangle$, and $E = Z_2[x]/\langle f(x)\rangle$. The composition of the inclusion and quotient maps
$$\mathbb{Z}_2 \overset{\iota}{\hookrightarrow} Z_2[x] \overset{q}{\twoheadrightarrow} Z_2[x]/\langle f(x)\rangle$$
is an injective homomorphism, so we want to think of $E = Z_2[x]/\langle f\rangle$ as a field extension of Z_2. If we let $\alpha := x + I$, then $f(\alpha) = (x^2 + x + 1) + I = I$, so $\alpha \in E$ is a root of $f(x)$, and $\alpha^2 = \alpha + 1$ $(*)$. Morevoer, $f(\alpha + 1) = (\alpha+1)^2+(\alpha+1)+1 = \alpha^2+1+\alpha+1+1 = 0$, so $(\alpha+1) \in E$ is the other root of f. By the division algorithm, for any $g(x) \in F[x]$ there are $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x)+r(x)$ and $r(x) = 0$ or $\deg(r(x)) < \deg(f(x)) = 2$. This means that $f(x) + I = r(x) + I$, so the elements of E are represented by polynomials of degree less than 2. This yields
$$E = \{0 + I, 1 + I, x + I, (x + 1) + I\} = \{0, 1, \alpha, \alpha + 1\},$$
so E is a field with 4 elements, and $E/\mathbb{Z}_2$ is a field extension of degree 2. The addition and multiplication tables can be computed using $(*)$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha=1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Class cancelled 03/01/19

This example is a guide to prove the following lemma. 03/04/19

Lemma 6.2.7 *Let $f(x) \in F[x]$ be irreducible of degree n. There is an extension E of F of degree n such that $f(x)$ has a root $\alpha \in E$. Moreover, there is a basis for E as a vector space over F consisting of powers of α.*

Proof. By Corollary 6.2.5, $F[x]/\langle f(x)\rangle$ is a field, and by Lemma 6.2.6 the The composition of the inclusion and quotient maps

$$\mathbb{F} \overset{\iota}{\hookrightarrow} F[x] \overset{q}{\twoheadrightarrow} F[x]/\langle f(x)\rangle$$

is an injective homomorphism, so we want to think of $E = F[x]/\langle f\rangle$ as a field extension of F. If we let $I = \langle f(x)\rangle$ and $\alpha := x + I$, then $f(\alpha) = f(x) + I = I = 0 + I$, so $\alpha \in E$ is a root of $f(x)$. By the division algorithm, for any $g(x) \in F[x]$ there are $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and $r(x) = 0$ or $\deg(r(x)) < \deg(f(x)) = n$. This means that $f(x)+I = r(x)+I$, so the elements of E are represented by polynomials of degree less than n. Therefore, the set

$$B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

is a spanning set for E as a vector space over F. The facts that $f(x)$ is irreducible, and has α as a root, imply that the minimal polynomial of α over F, $\min_F(\alpha)$, is a constant multiple of $f(x)$, and therefore $\deg_F(\alpha) = n$. This implies that no non-trivial linear combination of the vectors in B with coefficients in F will equal zero. In other words, B is linearly independent, hence a basis for E over F, and $[E : F] = |B| = n$. ∎

Remark 6.2.2. When $f(x)$ is a linear polynomial, i.e. of degree 1, then $E = F$. When $n := \deg(f(x)) > 1$, E is a proper extension of F, and f is not irreducible over E, since it has a root, hence a linear factor. Factoring out this linear factor, the rest can be factored into irreducible factors, and we could apply the lemma again to one of this irreducible factors, to get an extension of E that has a second root of $f(x)$. Repeating the process we can get an extension of F where $f(x)$ has n roots, counting multiplicities, i.e. factors into linear factors. We will do this more carefully in Corollary 6.4.6 to get an upper bound on the degree of such extension.

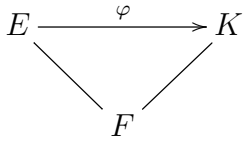
Corollary 6.2.8 *Given $\alpha \in E$ be algebraic over F, and $f(x) = \min_F(\alpha)$. Then $[F(\alpha) : F] = \deg(f(x))$.*

6.3 Homomorphisms of Extensions

extension homomorphism
extension isomorphism
extension endomorphism
extension automorphism

Next, we consider homomorphisms of field extensions. Recall from Lemma 6.2.6, that every unitary homomorphisms from F to any non-trivial ring has to be injective. When we consider two field extensions with the same field F at the bottom, we want to consider homomorphisms at the top that fix the bottom. More precisely,

Definition 6.3.1. Given two field extensions E/F and K/F, an *extension homomorphism* from E/F to K/F is a field homomorphism $\varphi : E \to K$ such that $\varphi|_F = \mathrm{id}_F$, i.e. $\varphi(a) = a$ for all $a \in F$. By Lemma 6.2.6 any field extension homomorphism is injective. But just like in the definition of homomorphisms of rings, we have special names for extension homomorphisms that are bijective, i.e. *extension isomorphism*; from an extension to itself, i.e. *extension endomorphism*; and *extension automorphism* a bijective homomorphism form an extension to itself.



Note that an extension homomorphism $\varphi : E/F \to K/F$ is not only a field homomorphism from E to K, but it is also a linear transformation of F-vector spaces.

Exercise 6.3.1. Let $\varphi : E/F \to K/F$ be an extension homomorphism. Prove that φ is a linear transformation of F-vector spaces.

Theorem 6.3.1 *Let $f(x) \in F[x]$ be irreducible of degree n. There is an extension E of F of degree n such that $f(x)$ has a root in E. Such extension is unique, up to isomorphism.*

Proof. The existence part was already established in Lemmma 6.2.7, where we showed that $E = F[x]/\langle f(x)\rangle$ works, i.e. it is an extension of F of degree n, and it contains a root $\alpha = x + \langle f(x)\rangle$ of $f(x)$.

For the uniqueness, suppose K is an extension of F of degree n, and with a root β of $f(x)$. The evaluation homomorphism

$$\begin{array}{rccc} \mathrm{ev}_\beta: & F[x] & \to & K \\ & g(x) & \mapsto & g(\beta) \end{array}$$

is a non-zero homomorphism, whose kernel contains $f(x)$, and is generated by $\min_F(\beta)$. Since $f(x)$ is irreducible, $f(x)$ is associate of $\min_F(\beta)$ and $\ker(\mathrm{ev}_\beta) = \langle f \rangle$. Clearly, $\mathrm{Im}(\mathrm{ev}_\beta) = F(\beta)$, so by the first isomorphism theorem, if we denote by I the kernel of ev_β,

$$\begin{array}{rccc} \widehat{\mathrm{ev}_\beta}: & E = F[x]/\langle f(x)\rangle & \to & F(\beta) \\ & g(x) + I & \mapsto & g(\beta) \\ & g(\alpha) & \mapsto & g(\beta) \end{array}$$

is an isomorphism of fields. By Exercise 6.3.1, $\widehat{\mathrm{ev}_\beta}$ is a linear transformation, hence an isomorphism of vector spaces. Therefore, $n = \dim_F(E) = \dim_F(F(\beta)) \leq \dim_F(K) = n$, and by Exercise 5.4.2.2, we get $F(\beta) = K$. ■

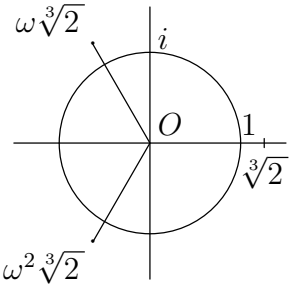
03/05/19

Scholium 6.3.2 *If $f(x) \in F[x]$ is irreducible of degree n, and β is a root of $f(x)$ in an extension K of F, then $F(\beta)/F$ is an extension of degree n with basis $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$. Moreover, $F[\beta] = F(\beta)$ is isomorphic to $F[x]/\langle p(x)\rangle$. Denoting by I the ideal $\langle f(x)\rangle$, the isomorphism is given by*

$$\begin{array}{rccc} \hat{\varphi}: & F[x]/\langle p(x)\rangle & \to & F(\beta) \\ & g(x) + I & \mapsto & g(\beta) \\ & g(\alpha) & \mapsto & g(\beta) \end{array}$$

Note that in this scholium the degree $[K : F]$ is at least n, so the extension $E = F[x]/\langle p(x)\rangle$ in Theorem 6.3.1 is of minimum degree possible.

Remark 6.3.1. The uniqueness up to isomorphism of the extension in Theorem 6.3.1, should not be confused with equality. The polynomial $x^3 - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein criterion). It has a single real root $\sqrt[3]{2}$, and two non real roots, $\sqrt[3]{2}\,\omega$, and $\sqrt[3]{2}\,\omega^2$, where $\omega = \mathrm{cis}(2\pi/3)$. Even though $\mathbb{Q}(\sqrt[3]{2}) \approx \mathbb{Q}(\sqrt[3]{2}\,\omega)$ as fields, they are not equal, since the first one is contained in $\mathbb{R}$, but the second one is not.



Exercise 6.3.2. Show that the polynomial $f = x^5 + 2x + 7$ is irreducible over $\mathbb{Q}$, and it has exactly one real root. Show that f has roots α_1 and α_2 such that $\mathbb{Q}(\alpha_1) \approx \mathbb{Q}(\alpha_2)$, but $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$. Hint: For the irreducibility, reduce coefficients (mod 3).

splits over E
splitting field

Solution. ■

Corollary 6.3.3 [Kronecker, 1887] *Let $f(x) \in F[x]$ be a polynomial of degree $n > 0$. There is a finite extension E of F of degree $\leq n$ such that $f(x)$ has a root in E.*

Proof. Apply the theorem to any irreducible factor of $f(x)$. ■

Definition 6.3.2. When $f(x) \in F[x]$ factors into linear factors over an extension E of F, we say that $f(x)$ *splits over* E. If moreover, E is minimal with this property, i.e. no proper subfield of E has the property, then we say that E is a *splitting field* for $f(x)$ over F.

Corollary 6.3.4 *Let $f(x) \in F[x]$ be a polynomial of degree $n > 0$. There is an extension K of F where $f(x)$ has n roots, counting multiplicities. i.e. $f(x)$ factors into linear factors in $K[x]$.*

Exercise 6.3.3. Prove Corollary 6.3.4. Hint: use induction on n.

6.4 Splitting Field

Corollary 6.3.4 tells us that for any polynomial $f(x) \in F[x]$ there is an extension K of F where it splits. Note, however, that it says nothing about the degree of such extension, or about the existence of a splitting field. We now discuss these two issues. First, to say something about the degree, we will need Theorem 6.4.2 below. We will consider the existence and uniqueness of splitting field after that.

Proposition 6.4.1 *Let E/F be an extension with basis $B = \{b_i | i \in I\}$ and K/E an extension with basis $C = \{c_j | j \in J\}$. Then the extension K/F has basis $D = \{b_i c_j | i \in I, j \in J\}$.*

multiplicative property of extension degrees

Proof. To see that D is a spanning set for K over F, note that each element of $\alpha \in K$ can be written as a (finite) linear combination

$$\alpha = \sum_{j \in J} \beta_j c_j$$

of elements of C with coefficients $\beta_j \in E$. But each of these coefficients β_j can be written as a (finite) linear combination

$$\beta_j = \sum_{i \in I} \gamma_{i,j} b_i$$

of elements in B with coefficents $\gamma_{i,j} \in F$. Combining these equations we get

$$\alpha = \sum_{j \in J} \sum_{i \in I} \gamma_{i,j} b_i c_j$$

To see that D is linearly independent, suppose there is a (finite) linear combination of elements of D equal to 0.

$$\sum_{j \in J} \sum_{i \in I} \gamma_{i,j} b_i c_j = 0$$

then grouping terms

$$\sum_{j \in J} \left(\sum_{i \in I} \gamma_{i,j} b_i \right) c_j = 0$$

and using the linear independence of C we get that for each $j \in J$,

$$\sum_{i \in I} \gamma_{i,j} b_i = 0$$

Now the linear independence of B implies that each $\gamma_{i,j} = 0$. ■

As an immediate consequence of this proposition and the definition of extension degree we get the *multiplicative property of extension degrees*.

Theorem 6.4.2 *[Multiplicative Property of Extension Degrees] Let E/F and K/E be field extensions. Then*

$$[K : F] = [K : E][E : F]$$

When the extensions are finite, the statement of this theorem deals with the product of natural numbers. However, if any of the extensions is infinite, then this result should be interpreted as dealing with product of cardinals. The same comment applies to Corollary 6.4.5 below. extension tower

Definition 6.4.1. An *extension tower* is a sequence of fields extensions $F_0 \leq F_1 \leq \cdots \leq F_n$. We say that this tower has height n.

$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$|$
$\mathbb{Q}(\sqrt{2})$
$|$
$\mathbb{Q}$

Example 6.4.1. Consider the tower $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. We have seen that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (why?), we must have $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$. But $\sqrt{3}$ is a root of $x^2-3 \in \mathbb{Q}(\sqrt{2})[x]$, so we get $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Combining these two inequalities we get $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ By the multiplicative property of extension degrees, we conclude that

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

03/06/19 Recall from Example 6.2.2.4 that for $\alpha = \sqrt{2}+\sqrt{3}$, $\min_{\mathbb{Q}}(\alpha) = x^4-10x^2+1$, and $\deg_{\mathbb{Q}}(\alpha) = 4$. Since $\alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, using the multiplicative property of extensions degree, it follows that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

The notation used in the previous example, i.e. $\mathbb{Q}(\sqrt{2},\sqrt{3})$, is justified in the following proposition.

Proposition 6.4.3 *Let E/F be a field extension, and $\alpha_1,\ldots,\alpha_n \in E$. The intersection of all subfields of E that contain $\alpha_1,\ldots,\alpha_n$ and F is itself a subfield of E; it contains $\alpha_1,\ldots,\alpha_n$ and F, and it is minimal with this property.*

Exercise 6.4.1. Prove Proposition 6.4.3.

Definition 6.4.2. The field constructed in Proposition 6.4.3 is called the subextension of E/F generated by $\alpha_1,\ldots,\alpha_n$ and we denote it by $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Exercise 6.4.2. From Example 6.4.1 above, it follows that $\sqrt{2} \in \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2}+\sqrt{3}$. Write an explicit expression in α that equals $\sqrt{2}$. Something similar can be done for $\sqrt{3}$.

An immediate consequence of Theorem 6.4.2 is the following

Corollary 6.4.4 *Let $K/E/F$ be a filed tower. K/F is a finite extension iff K/E and E/F are finite extensions.*

Using the multiplicative property in Theorem 6.4.2, and induction, we get:

Corollary 6.4.5 *Let $F = F_0 \leq F_1 \leq \cdots \leq F_n = K$ be an extension tower. Then*

$$[K : F] = \prod_{i=1}^{n} [F_i : F_{i-1}]$$

In particular, the overall extension F_n/F_0 is a finite extension iff each step F_{i+1}/F_i is a finite extension.

We can now improve on Corollary 6.3.4 by giving an upper bound on the degree of an extension where $f(x)$ splits.

Corollary 6.4.6 *Let $f(x) \in F[x]$ be a polynomial of degree n. There is an extension K of F where $f(x)$ splits and has degree $[K : F] \leq n!$.*

Exercise 6.4.3. Prove Corollary 6.4.6. Hint: use induction on n. See Remark 6.2.2.

We now consider the existence of a splitting field. Later in this section we will consider uniqueness. Let's begin with a generalization of Lemma 3.0.2.

Proposition 6.4.7 *Let $f(x) \in F[x]$, and K an extension of F where $f(x)$ splits. There is a unique splitting field E of $f(x)$ over F contained in K.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$ in K. It suffices to take $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. ∎

Note that Proposition 6.4.7 tells us of the uniqueness of a splitting field for $f(x)$ inside K, where $f(x)$ splits. However, $f(x)$ may split in several extensions $K_1, K_2, \ldots$, of F, and in each one of them there will be a splitting field for $f(x)$. We aim to show that any two such splitting fields are isomorphic to each other as extensions of F. In other words, we will show that splitting field for $f(x) \in F[x]$ is unique up to isomorphim of F-extensions. See Corollary 6.4.15 below.

simple extension
primitive element

Proposition 6.4.8 *Let $f(x) \in F[x]$. There is a splitting field E for $f(x)$ over F.*

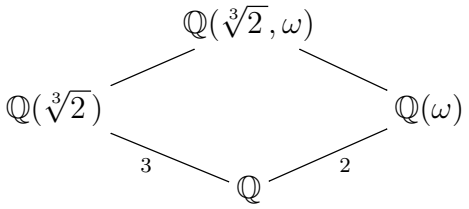
Proof. By Corollary 6.4.6 there is an extension K/F where $f(x)$ splits. Apply now Proposition 6.4.7. ∎

In Example 6.4.1 we showed that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. This shows that the extension $\mathbb{Q}(\sqrt{2},\sqrt{3})$ generated by two elements, $\sqrt{2}$ and $\sqrt{3}$, can also be generated by a single element, i.e. $\sqrt{2}+\sqrt{3}$.

Definition 6.4.3. Let F be a field and u an element in some extension of F. The extension $F(u)/F$ is called a *simple extension*. The element u is called a *primitive element* of the extension.

For a simple extension, a primitive element is not necessarily unique. For example, the extensiion $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ has primitive element $\sqrt{2}+\sqrt{3}$, but it is easy to see that $\sqrt{2}-\sqrt{3}$ is also a primitive element for this extension.

Not every extension is simple, not even the finite ones. We will see a counterexample later on. However, many finite extensions are simple, in particular every finite extension over $\mathbb{Q}$ is simple as we will prove in the Primitive Element Theorem 7.2.8.



Example 6.4.2. Consider $\mathbb{Q}(\sqrt[3]{2},\omega)$, the splitting field of $x^3-2 \in \mathbb{Q}[x]$ in $\mathbb{C}$ as an extension of $\mathbb{Q}$. From Remark 6.3.1, we have $\min_{\mathbb{Q}} \sqrt[3]{2} = x^3-2$. We also know that $\min_{\mathbb{Q}}(\omega) = x^2+x+1$. Therefore $[\mathbb{Q}(\sqrt[3]{2}) : Q] = 3$ and $[\mathbb{Q}(\omega) : Q] = 2$. By the multiplicative property of extension degrees we get that $[Q(\sqrt[3]{2},\omega) : \mathbb{Q}]$ is a multiple of 2 and 3, hence a multiple of 6. On the other hand, $[Q(\sqrt[3]{2},\omega) : \mathbb{Q}(\sqrt[3]{2})] \leq 2$ since ω is a root of $x^2+x+1 \in \mathbb{Q}(\sqrt[3]{2})[x]$. It follows that $[Q(\sqrt[3]{2},\omega) : \mathbb{Q}] = 6$. Take $u = \sqrt[3]{2}+\omega$. Then $(u-\omega)^3 = 2$, i.e. $u^3 - 3u^2\omega + 3u\omega^2 - 3 = 0$. But $\omega^2+\omega+1 = 0$, so we get

$$\omega = \frac{u^3-3u-3}{3(u^2+u)} \in \mathbb{Q}(u),$$

and $\sqrt[3]{2} = u-\omega \in \mathbb{Q}(u)$. Thus, we get $\mathbb{Q}(\sqrt[3]{2},\omega) = \mathbb{Q}(u)$.

algebraic numbers

Exercise 6.4.4. Find the minimal polynomial $\min_{\mathbb{Q}}(u)$, where $u = \sqrt[3]{2} + \omega$.

03/08/19

Proposition 6.4.9 *An extension E/F is finite iff $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$, algebraic over F.*

Proof. Use Proposition 6.2.1, Example 6.1.1.1, the multiplicative property of extensions, and induction. ■

The following corollary extends Corollary 6.4.4 to algebraic extensions, and can be easily extended to towers.

Corollary 6.4.10 *Let $K/E/F$ be an extension tower. K/F is algebraic iff K/E and E/F are algebraic.*

Proof. ($\Rightarrow$) Immediate from the definition and the fact that $F[x] \leq E[x]$.
($\Leftarrow$) Suppose K/E and E/F are algebraic extension, and let $\alpha \in K$. There is a polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in E[x]$$

such that $f(\alpha) = 0$. Since $a_0, a_1, \ldots, a_n \in E$ are algebraic over F, by Proposition 6.4.9 $F(a_0, a_1, \ldots, a_n)$ is a finite extension of F. We also have that $F(a_0, a_1, \ldots, a_n, \alpha)$ is a finite extension over $F(a_0, a_1, \ldots, a_n)$. Using the multiplicative property we conclude that $F(a_0, a_1, \ldots, a_n, \alpha)$ is a finite extension of F, and therefore α is algebraic over F. ■

As mentioned earlier, not all algebraic extensions are finite extensions.

Definition 6.4.4. Those complex numbers which are algebraic over $\mathbb{Q}$ are called *algebraic numbers*. The set of all algebraic numbers is denoted by $\mathbb{A}$.

Corollary 6.4.11 *The set $\mathbb{A}$ of all algebraic numbers is a subfield of $\mathbb{C}$, the field of complex numbers. It is an infinite, algebraic extension of $\mathbb{Q}$.*

Proof. Let $\alpha, \beta \in \mathbb{A}$. By Proposition 6.4.9, $\mathbb{Q}(\alpha, \beta)$ is a finite extension of $\mathbb{Q}$, and all its elements are algebraic over $\mathbb{Q}$. That includes $\alpha \pm \beta$, $\alpha\beta$ and α/β when $\beta \neq 0$. ■

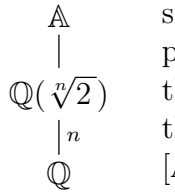
The same argument used to prove that $\mathbb{A}$ is a subfield of $\mathbb{C}$ can be used to show.

Corollary 6.4.12 *Let E/F be a field extension. The set*

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

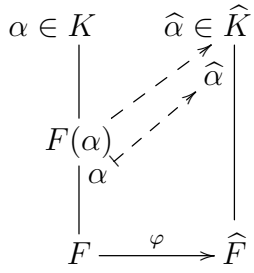
is a subfield of E that contains F, and it is an algebraic extension of F.

We can finally give an example of an algebraic extension that is not finite, to show that the converse of Proposition 6.2.1 does not hold.



Example 6.4.3. The extension $\mathbb{A}/\mathbb{Q}$ is an infinite algebraic extension. This extension is algebraic by definition. Consider now the polynomial $x^n - 2$. By Eisenstein criterion it is irreducible over $\mathbb{Q}$, so the number $\sqrt[n]{2}$ has degree n over $\mathbb{Q}$, i.e. $[Q(\sqrt[n]{2} : \mathbb{Q}] = n$. Applying the multiplicative property to the tower $\mathbb{A}/\mathbb{Q}(\sqrt[n]{2})/Q$, we get that $[\mathbb{A} : \mathbb{Q}] \geq n$ for every $n \in \mathbb{N}$, and therefore must be infinite.

We now begin to build toward the proof that the splitting field of a polynomial is unique up to isomorphism. See Theorem 6.4.16 below.



Lemma 6.4.13 *Let F and $\widehat{F}$ be fields, and $\varphi : F \to \widehat{F}$ a homomorphism. Denote also by φ the homomorphism induced on the polynomial rings $\varphi : F[x] \to \widehat{F}[x]$, according to Lemma 3.0.3. Let $p(x) \in F[x]$ be an irreducible polynomial, and denote by $\widehat{p}(x)$ its image $\varphi(p(x)) \in \widehat{F}[x]$. Let α be a root of $p(x)$ in some extension K of F, and $\widehat{\alpha}$ a root of $\widehat{p}(x)$ in some extension $\widehat{K}$ of $\widehat{F}$. There is a homomorphism from $F(\alpha)$ to $\widehat{K}$ which agrees with φ on F and maps α to $\widehat{\alpha}$.*

03/11/19

Proof. Consider the map $\theta = \mathrm{ev}_{\widehat{\alpha}} \circ \varphi$

$$F[x] \xrightarrow{\varphi} \widehat{F}[x] \xrightarrow{\mathrm{ev}_{\widehat{\alpha}}} \widehat{K}$$

The kernel contains $p(x)$ since $\widehat{\alpha}$ is a root of $\widehat{p}(x)$, but it is not all of $F[x]$. By maximality of $\langle p(x)\rangle$ we must have $\ker\theta = \langle p(x)\rangle$. By the first isomorphism theorem there is an monomorphism, call it also θ from $F[x]/\langle p(x)\rangle$ to $\widehat{K}$,

$$\begin{array}{rccc} \theta: & F[x]/\langle p(x)\rangle & \to & \widehat{K} \\ & f(x) + \langle p(x)\rangle & \mapsto & \widehat{f}(\widehat{\alpha}) \end{array}$$

Composing with the inverse of the isomorphism from Scholium 6.3.2

$$\begin{array}{rccc} \nu: & F[x]/\langle p(x)\rangle & \to & F(\alpha) \\ & f(x)+\langle p(x)\rangle & \mapsto & f(\alpha) \end{array}$$

yields a homomorphism $\Phi = \theta \circ \nu^{-1} : F(\alpha) \to \widehat{K}$. Note that for $a \in F$, we have

$$\Phi(a) = \theta(\nu^{-1}(a)) = \theta(a + \langle p(x)\rangle) = \varphi(a)$$

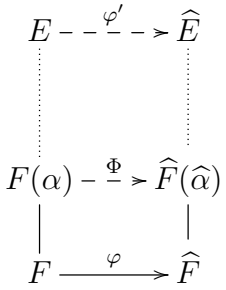
and

$$\Phi(\alpha) = \theta(\nu^{-1}(\alpha)) = \theta(x + \langle p(x)\rangle) = \widehat{\alpha}.$$

So, Φ is the desired homomorphism. ■

Corollary 6.4.14 *Let F and $\widehat{F}$ be fields, and $\varphi : F \to \widehat{F}$ a homomorphism. Denote also by φ the homomorphism induced on the polynomial rings $\varphi : F[x] \to \widehat{F}[x]$, according to Lemma 3.0.3. Let $f(x) \in F[x]$ be a non-constant polynomial, and denote by $\widehat{f}(x)$ its image $\varphi(f(x)) \in \widehat{F}[x]$. Let E be a splitting field of $f(x)$ over F, and $\widehat{E}$ an extension of $\widehat{F}$ where $\widehat{f}(x)$ splits. There is a homomorphism $\varphi' : E \to \widehat{E}$ which agrees with φ on F. Moreover $\widehat{f}(x)$ splits in $\mathrm{Im}(\varphi')$, so that if $\widehat{E}$ is a splitting field of $\widehat{f}(x)$ over $\mathrm{Im}(\varphi')$, then φ' is an isomorphism.*

Proof. The proof is by induction on $\deg(f(x))$. When $\deg(f(x)) = 1$ then $E = F$. Take $\varphi' = \varphi$. When $\deg(f(x)) > 1$ let $\alpha \in E$ be one of the roots of $f(x)$ and let $p(x)$ be an irreducible factor of $f(x)$ that has α as a root. Note that $\widehat{p}(x) = \varphi(p(x))$ is a factor of $\widehat{f}(x)$ and therefore it has a root $\widehat{\alpha}$ in $\widehat{E}$. By the lemma, there is a homomorphism $\Phi : F(\alpha) \to \widehat{F}(\widehat{\alpha})$ that agrees with φ on F and $\Phi(\alpha) = \widehat{\alpha}$. In $F(\alpha)[x]$ we have $f(x) = (x-\alpha)g(x)$ with $\deg(g(x)) = \deg(f(x)) - 1$, and E is a splitting field for $g(x)$ over $F(\alpha)$. $\widehat{g}(x) = \Phi(g(x)) \in \widehat{F}(\widehat{\alpha})[x]$ splits in $\widehat{E}$, so by induction there is a homomorphism $\varphi' : E \to \widehat{E}$ that agrees with Φ on $F(\alpha)$. Hence it agrees with φ on F. Moreover, by induction, $\widehat{g}(x)$ splits in $\mathrm{Im}(\varphi')$, and so does $\widehat{f}(x) = (x-\widehat{\alpha})\widehat{g}(x)$. If $\widehat{E}$ is splitting field of $\widehat{f}(x)$ over $\widehat{F}$, by minimality of splitting field, it must equal $\mathrm{Im}(\varphi')$, so φ' is surjective. Finally, a field homomorphism is always injective. ■



By taking $\widehat{F} = F$ and φ the identity map of F, we get the following corollary. 03/12/19

Corollary 6.4.15 *Let $f \in F[x]$ be a non-constant polynomial. If E and $\widehat{E}$ are two splitting fields of f, then E and $\widehat{E}$ are isomorphic as extensions of F.*

Combining Proposition 6.4.8 with this corollary we get.

Theorem 6.4.16 *Let $f(x) \in F[x]$. There is a splitting field for $f(x)$ over F, which is unique up to isomorphism of extensions of F.*

Example 6.4.4. We want to find the splitting field for

$$f(x) = x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x].$$

Note that 1 is a root of $f(x)$, so, using synthetic division

$$\begin{array}{c|ccccc} 1 & 1 & 1 & 1 & 0 & 1 \\ & & 1 & 0 & 1 & 1 \\ \hline & 1 & 0 & 1 & 1 & 0 \end{array}$$

we can see that it factors as $f(x) = (x+1)(x^3 + x + 1)$. The first factor is linear, hence irreducible. The second factor is cubic with no roots in $\mathbb{Z}_2$, so it is also irreducible over $\mathbb{Z}_2$. Let α be a root of $x^3 + x + 1$ in some extension of $\mathbb{Z}_2$, so that we have $\alpha^3 + \alpha + 1 = 0$, i.e. $\alpha^3 = \alpha + 1$. Once again, synthetic division

$$\begin{array}{c|cccc} \alpha & 1 & 0 & 1 & 1 \\ & & \alpha & \alpha^2 & \alpha^3 + \alpha \\ \hline & 1 & \alpha & 1 + \alpha^2 & 0 \end{array}$$

yields $f(x) = (x+1)(x+\alpha)(x^2 + \alpha x + (1+\alpha^2))$. A direct calculation shows that this last factor has roots α^2 and $\alpha^2 + \alpha$ in $\mathbb{Z}_2(\alpha)$. Therefore, $\mathbb{Z}_2(\alpha)$ is the splitting field of $f(x)$. Since $\min_{\mathbb{Z}_2}(\alpha) = x^3 + x + 1$, we have $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 3$, and $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Z}_2(\alpha)$ as a vector space over $\mathbb{Z}_2$. Thus,

$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}.$$

The multiplication in $\mathbb{Z}_2(\alpha)$ is done using the fact that $\alpha^3 = \alpha + 1$. Note that the multiplicative group $\mathbb{Z}_2(\alpha)^*$ of non-zero elements, is a group of order 7,

hence cyclic, and is generated by any element different from 1. In particular, it is generated by α, so we have

$$\mathbb{Z}_2(\alpha)^* = \{\alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1, \alpha^7 = 1\}$$

Here are the addition and multiplication tables for

$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\},$$

a field with 8 elements, satisfying $\alpha^3 = \alpha + 1$.

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

All of these elements satisfy $x^7 = 1$, i.e. are roots of $x^7 - 1$. If we multiply by $x - 0$, we get that the elements of $\mathbb{Z}_2(\alpha)$ are roots of $x^8 - x$. This

polynomial has at most 8 distinct roots, so it has exactly 8 roots, precisely the elements of $\mathbb{Z}_2(\alpha)$. $\mathbb{Z}_2(\alpha)$ is the splitting field for this polynomial.

We will see in Section 6.6 that this previous example is typical of all finite fields.

6.5 Algebraic Closure

The Fundamental Theorem of Algebra (FTAlg) tells us that every polynomial with complex coefficients has a root in $\mathbb{C}$. From this, it follows easily that any polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$. This connection holds in a more general setting, as the following proposition indicates.

Proposition 6.5.1 *Let F be a field. TFAE:*

1. *Every nonconstant polynomial in $F[x]$ has a root in F.*
2. *Every nonconstant polynomial in $F[x]$ splits over F.*
3. *Every irreducible polynomial in $F[x]$ is linear.*
4. *For any algebraic extension E/F one has $E = F$.*

Proof. $(1 \Rightarrow 2)$ Use Corollary 4.1.4 and induction.
$(2 \Rightarrow 3)$ If every nonconstant polynomial splits over F, then no polynomial of degree 2 or higher is irreducible. By Proposition 4.3.2.**??** every linear polynomial is irreducible.
$(3 \Rightarrow 4)$ Suppose E/F is an algebraic extension. If $\alpha \in E$, then $\min_F(\alpha) \in F[x]$ is irreducible, and by assumption it is linear. That means $\deg_F(\alpha) = 1$, hence $\alpha \in F$.
$(4 \Rightarrow 1)$ If $f(x) \in F[x]$ is a nonconstant polynomial, by Corollary 6.3.3 there is a finite extension E of F which contains a root of $f(x)$. By Proposition 6.2.1 E/F is algebraic, and by assumption, $E = F$, so $f(x)$ has a root in F. ■

The last property in Proposition 6.5.1 tells us that F does not have any proper algebraic extension. Fields that satisfy this property, and hence all

algebrically closed
algebraic closure

four properties in Proposition 6.5.1 are called *algebrically closed*. The FTAlg then tells us that $\mathbb{C}$ satisfies Proposition 6.5.1.2, hence it is algebraically closed, and it has no proper algebraic extension.

Corollary 6.5.2 *Let E/F be a field extension, with E algebraically closed. The set*

$$\overline{F} = \{\alpha \in E | \alpha \text{ is algebraic over } F\}$$

is an algebraic extension of F, and it is algebraically closed.

Proof. In Corollary 6.4.12 we showed that $\overline{F}$ is a subfield of E. Clearly, it contains F and is an algebraic extension of F. If $f(x) \in \overline{F}[x]$ is a nonconstant polynomial, then it has a root $\alpha \in E$. So, α is algebraic over $\overline{F}$ and $\overline{F}$ is algebraic over F, so α is algebraic over F, and therefore $\alpha \in \overline{F}$. ■

Definition 6.5.1. Given a field extension E/F, we say that E is an *algebraic closure* of F if

- E/F is algebraic, and
- E is algebraically closed.

Corollary 6.5.2 proves that if E is algebraically closed, then any subfield F of E has an algebraic closure contained in E, namely $\overline{F}$.

It can be shown, using Zorn's Lemma, that any field F has an algebraic closure, unique up to isomorphism of extensions of F. We will not prove this theorem, but here is the basic idea. Just like we used Kronecker's lemma and induction to construct a splitting field of a polynomial, one can use that lemma and Zorn's lemma to construct a splitting field for an arbitrary set of polynomials. In particular, a splitting field for the set $F[x]$ of **all** polynomials over F will be an algebraic closure of F. Using Lemma 6.4.13 and Zorn's lemma, one proves the uniqueness up to isomorphism.

Exercise 6.5.1.

1. Let E be a field extension of F. Prove that E is an algebraic closure of F iff E is minimal with the property that every polynomial $f(x) \in F[x]$ splits over E.
2. Let E be an algebraic closure of F. Prove that for any field K such that $F \leq K \leq E$, E is an algebraic closure of K.

6.6 Finite Fields

multiplicity
simple root
multiple root
derivative

We have already seen in Corollary 5.5.6 that for a finite F, the number of elements of F is a prime power of p^n, where p is the characteristic of F.

In this section we will show that for any prime p and any $n \geq 1$, there is a field with p^n elements, unique up to isomorphism. This result completely characterizes all finite fields.

Let E/F be a field extension, $f(x) \in F[x]$ and $a \in E$. Recall from Corollary 4.1.4 that a is a root of $f(x)$ iff $(x-a)$ is a factor of $f(x)$. Recall also from Definition 4.1.2 that the *multiplicity* of a as a root of $f(x)$ is the largest $m \in \mathbb{N}$ such that $(x-a)^m$ is a factor of $f(x)$. That is, $f(x) = (x-a)^m \cdot g(x)$ and $(x-a) \nmid g(x)$. A *simple root* is a root of multiplicity $m = 1$. A *multiple root* is a root of multiplicity $m \geq 2$. Proposition 6.6.2 will give us a criteria to distinguish simple roots from multiple roots. First we need the concept of derivative of a polynomial.

Definition 6.6.1. Let F be a field and $f(x) \in F[x]$, written as

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

The *derivative* of $f(x)$ is defined to coincide with the calculus derivative. However, there is no need for limits. We define

$$f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

Examples 6.6.1.

1. For $f(x) = 2x^3 - 3x^2 - 12x - 20 \in \mathbb{Q}[x]$, we have $f'(x) = 6x^2 - 6x - 12$.
2. For $f(x) = x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$, we have $f'(x) = x^2$.

Note that the degree of $f'(x)$ is at least one less than the degree of $f(x)$. However, when the $\mathrm{char}(F) \neq 0$, the degree can be even lower, as Example 6.6.1.2 shows. We could even have $f'(x) = 0$ without $f(x)$ being a constant.

Proposition 6.6.1 *Let F be a field, $f(x), g(x) \in F[x]$, $c \in F$.*

1 $(cf(x))' = cf'(x)$,

2 $(f(x)+g(x))' = f'(x)+g'(x)$,

3 $(f(x)g(x))' = f(x)g'(x)+f'(x)g(x)$,

4 $(f(g(x)))' = f'(g(x))\cdot g'(x)$.

Exercise 6.6.1. Prove Proposition 6.6.1.

Proposition 6.6.2 *Let F be a field, $f(x) \in F[x]$, and E an extension of F. An element $a \in E$ is a multiple root of $f(x)$ iff a is a root of both $f(x)$ and $f'(x)$.*

Proof. First of all, factor $f(x)$ in $E[x]$ as $f(x) = (x-a)^m g(x)$ with the largest possible m, i.e. such that $(x-a) \nmid g(x)$, i.e. $g(a) \neq 0$. Thus, m is the multiplicity of a as a root of $f(x)$.
($\Rightarrow$) Assume $m > 1$. Then, using Proposition 6.6.1, we get

$$f'(x) = m(x-a)^{m-1}g(x)+(x-a)^m g'(x) = (x-a)^{m-1}(mg(x)+(x-a)g'(x)).$$

Evaluating at a, we get $f(a) = 0$ and $f'(a) = 0$.
($\Leftarrow$) Assume $f(a) = 0$ and $f'(a) = 0$. From the first we get that $m \geq 1$. If we had $m = 1$, then $f'(a) = g(a) \neq 0$. Therefore, we must have $m > 1$. ■

Examples 6.6.2.

1. The polynomial $f(x) = x^4+x^3+x^2+1 \in \mathbb{Z}_2[x]$ has derivative $f'(x) = 1$, which has no roots. Therefore 1 is a simple root of $f(x)$, and so are all the roots of $f(x)$. Hence, $f(x)$ has 4 distinct roots in its splitting field, as we had already seen in Example 6.4.4.

2. The same argument applies to $f(x) = x^4+x^2+x+1 \in \mathbb{Z}_2[x]$.

3. From Example 6.6.1.2 we have that for $f(x) = x^4+x^3+x^2+1 \in \mathbb{Z}_2[x]$, the derivative is $f'(x) = x^2$. The only root of the derivative is 0, but 0 is not a root of $f(x)$. Therefore, $f(x)$ does not have any multiple roots.

4. From Example 6.6.1.1 we have that for $f(x) = 2x^3-3x^2-12x-20 \in \mathbb{Q}[x]$, the derivative is $f'(x) = 6x^2-6x-12$, i.e. $f'(x) = 6(x-1)(x+2)$, which has roots 1 and -2. A direct calculation shows that $f(-2) = 0$, and therefore -2 is a root of $f(x)$ with multiplicity greater than 1. Using synthetic division one can easily show that

   $$f(x) = 2x^3+3x^2-12x-20 = (x+2)(2x^2-x-10) = (x+2)(x+2)(2x-5).$$

fixed field
fixed field
Frobeniüs endomorphism

Lemma 6.6.3 *Let F be a field and $\varphi : F \to F$ an endomorphism of F. The set*

$$F_\varphi = \{a \in F | \varphi(a) = a\}$$

is a subfield of F. It contains the prime subfield of F. It is called the fixed field *of φ.*

Exercise 6.6.2. Prove Lemma 6.6.3.

Corollary 6.6.4 *Let F be a field and G a set of endomorphisms of F. The set*

$$F_G = \{a \in G | \varphi(a) = a, \text{ for all } \varphi \in G\}$$

is a subfield of F. It contains the prime subfield of F. It is called the fixed field *of G.*

Lemma 6.6.5 *Let p be a prime and R be a commutative ring with unity of characteristic p. The map*

$$\begin{array}{rccc} \Phi: & R & \to & R \\ & a & \mapsto & a^p \end{array}$$

is an endomorphism of R. It is called the Frobeniüs endomorphism *of R.*
For a finite field F, the Frobeniüs endomorphism is an automorphism.

Theorem 6.6.6 *Let p be a prime and $n \geq 1$. There is a field of order p^n, and it is unique up to isomorphism.*

Proof. Following the idea of Example 6.4.4, consider the polynomial $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Let E be a splitting field for $f(x)$ over $\mathbb{Z}_p$. Let Φ be the Frobeniüs endomorphism of E, and $\Psi = \Phi^n$ the endormorphism that results from composing Φ with itself n times. The roots of $f(x)$ are precisely the elements of E that satisfy $\Psi(a) = a$, i.e. the fixed subfield of Ψ. Since E is minimal containing the roots of $f(x)$ we get that $E = E_\Psi$ is the set of all roots of $f(x)$. Now, $f'(x) = -1$ has no roots, so by Proposition 6.6.2, $f(x)$ has no multiple roots, i.e. it has p^n distinct roots. Therefore E is a field with p^n elements. This proves the existence part of the theorem.
For the uniqueness, we once again follow the idea of Example 6.4.4. If F is a field with p^n elements, then F^* is a multiplicative group with $p^n - 1$ elements, and all its elements satisfy $x^{p^n-1} = 1$, i.e. they are roots of the polynomial $x^{p^n-1} - 1$. Multiplying by x, we also get 0 as a root, so F is the set of roots

Galois field

of $f(x) = x^{p^n} - x$. So, F is the splitting field of $f(x)$. By Theorem 6.4.16, tells us that F is unique up to isomorphism. ■

03/15/19

Definition 6.6.2. Let p be a prime, $n \geq 1$ and $q = p^n$. The unique field with q elements is called the *Galois field* of order q, and it is denoted by $GF(q)$, or by $\mathbb{F}_q$. Note that $\mathbb{F}_p = \mathbb{Z}_p$.

We now want to show that any finite field $\mathbb{F}_q$ is a simple extension of $\mathbb{F}_p$ where p is the characteristic.

First, we need a lemma about finite abelian groups. Recall that the expoenet of a group is the least common multiple of the orders of its elements. Back in Chapter 1, Exercise **??** we had that if G is a group and $a, b \in G$ have finite order and commute with each other, then there is $c \in G$ whose order is l.c.m.$\{o(a), o(b)\}$. Repeated application of this result yields the following.

Lemma 6.6.7 *Let G be a finite abelian group with $\exp(G) = k$. There is $u \in G$ such that $o(u) = k$.*

Exercise 6.6.3. Prove Lemma 6.6.7.

Proposition 6.6.8 *If G be a finite subgroup of the multiplicative group F^* of a field F, then G is cyclic.*

Proof. Let $k = \exp(G)$. This means that all elements of G satisfy the equation $x^k = 1$, i.e. they are roots of the polynomial $x^k - 1 \in F[x]$. Since a polynomial of degree k has at most k distinct roots, it follows that $|G| \leq k$. On the other hand, we know, from Lagrange's Theorem, that for any group $\exp(G)$ is a divisor of $|G|$. It then follows that $|G| = k$. By Lemma 6.6.7, G has an element of order k, hence G is cyclic as desired. ■

Corollary 6.6.9 *The multiplicative group $\mathbb{F}_q^*$ of a finite field is cyclic.*

Corollary 6.6.10 *Let p be a prime and $q = p^n$ a power of p. The finite field $\mathbb{F}_q$ is a simple extension of its prime subfield $\mathbb{F}_p$, i.e. $\mathbb{F}_q = \mathbb{F}_p(u)$, for some $u \in \mathbb{F}_q$.*

Proof. Just take u to be a generator of the cyclic group $\mathbb{F}_a^*$. ■

Corollary 6.6.11 *Let p be prime and $n \geq 1$. There exist an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.*

Proof. Take $f(x) = \min_{\mathbb{F}_p}(u)$ where $u \in \mathbb{F}_{p^n}$ is such that $\mathbb{F}_{p^n} = \mathbb{F}_p(u)$. ■

Lemma 6.6.12 *Let $p, n, d \in \mathbb{N}$. If $d|n$ then $p^d - 1$ is a divisor of $p^n - 1$.*

Proof. Write $n = kd$, and $r = p^d$, so that $p^n = r^k$. Note that

$$r^k - 1 = (r-1)(r^{k-1} + r^{k-2} + \cdots + r^2 + r + 1),$$

in other words,

$$p^n - 1 = (p^d - 1)(p^{d(k-1)} + p^{d(k-2)} + \cdots + p^{2d} + p^d + 1,$$

and $(p^d - 1)|(p^n - 1)$. ■

We now have the tools to classify all the subfields of a finite field $\mathbb{F}_q$.

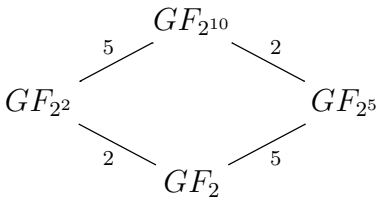
Theorem 6.6.13 *Let p be a prime, $n \geq 1$, and $q = p^n$.*

1. *If K is a subfield of $\mathbb{F}_q$, then $K \approx \mathbb{F}_{p^d}$ for some d divisor of n, and $[\mathbb{F}_q : K] = \frac{n}{d}$.*
2. *If d is a divisor of n, there is exactly one subfield of $\mathbb{F}_{p^n}$ of order p^d, namely the splitting field of $x^{p^d} - x$.*

Proof. (1) Since K is a finite field of characteristic p, we know that $K \approx \mathbb{F}_{p^d}$ for some $d \geq 1$. By the multiplicative property of degrees we have $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] \cdot [\mathbb{F}_{p^d} : \mathbb{F}_p]$, i.e. $n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] \cdot d$, so $d|n$ and $[\mathbb{F}_{p^n} : \mathbb{F}_{p^r}] = \frac{n}{d}$. (2) Assume $d|n$. By Lemma 6.6.12, $p^d - 1$ is a divisor of $p^n - 1$. Since $\mathbb{F}^*_{p^n}$ is a cyclic group or order $p^n - 1$, it has a unique subgroup H of order $p^d - 1$. All the elements of H are roots of the polynomial $x^{p^d-1} - 1$, so $H \cup \{0\}$ is the set of roots of $x^{p^d} - x$. The proof of Theorem 6.6.6 shows that $H \cup \{0\}$ is a field of order p^d. ■

Exercise 6.6.4. Prove the converse of Lemma 6.6.12 with the extra assumption the p is prime.

Example 6.6.3. Consider the field with 1024 elements. It has four subfields: $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^5}$, and $\mathbb{F}_{2^{10}}$ itself.



The elements of $\mathbb{F}_2$ are the roots of $x^2 - x = x(x-1)$, i.e. 0 and 1.

The elements of $\mathbb{F}_4$ are the roots of $x^4 - x$. Other than 0 and 1, the other two elements of $\mathbb{F}_4$ have degree 2 over $\mathbb{F}_2$, so $x^4 - x$ must have an irreducible quadratic factor. In fact, $x^4 - x = x(x-1)(x^2+x+1)$ is a factorization into irreducible factors, and $x^2 + x + 1$ is the only monic irreducible quadratic polynomial in $\mathbb{F}_2[x]$.

$\mathbb{F}_{32}$ has $32 - 2 = 30$ elements of degree 5 over $\mathbb{F}_2$. Each one of them is a root of an irreducible polynomial of degree 5, and each such irreducible polynomial contributes 5 elements to $\mathbb{F}_{32}$. Since $x^{32} - x$ has no multiple roots, its factorization into irreducible factors cannot have repeated factors. It then follows that $x^{32} - x = x(x-1)f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)f_6(x)$ where $f_1(x), f_2(x), f_3(x), f_4(x), f_5(x), f_6(x)$ are distinct irreducible polynomials of degree 5. Moreover, any irreducible polynomial of degree 5 over $\mathbb{F}_2$ has a root in an extension of degree 5 over $\mathbb{F}_2$. But $\mathbb{F}_{32}$ is the only extension of degree 5 over $\mathbb{F}_2$, up to isomorphism. So, any irreducible of degree 5 over $\mathbb{F}_2$ has a root in $\mathbb{F}_{32}$, and it must be one of $f_1(x), f_2(x), f_3(x), f_4(x), f_5(x), f_6(x)$. We have shown, that there are exactly 6 irreducible polynomials of degree 5 over $\mathbb{F}_2$, i.e. the factors of $\dfrac{x^{32} - x}{x(x-1)}$.

There are 32 monic quintic polynomials over $\mathbb{F}_2$. Half of them, have 0 constant term, so they have 0 as a root and are reducible. Of the other 16, the ones with contant term 1, half of them have an even number of non-zero coefficients, so they have 1 as a root, and are reducible. This leaves 8 potential irreducible quintic polynomials. Those that have constant term 1, and an odd number of non-zero coefficients. But they are not all irreducible. A quintic polynomial may factor as a product of a quadratic irreducible and a cubic irreducible. There is only one monic quadratic irreducible polynomial in $\mathbb{F}_2[x]$, namely $x^2 + x + 1$, and exactly 2 monic cubic irreducible polynomials, namely $x^3 + x^2 + 1$ and $x^3 + x + 1$, there are two quintic polynomials that factor as a product of a quadratic and a cubic:

$$\begin{aligned}(x^2 + x + 1)(x^3 + x^2 + 1) &= x^5 + x + 1\\ (x^2 + x + 1)(x^3 + x + 1) &= x^5 + x^4 + 1\end{aligned}$$

When we exclude these two polynomials from the 8 potential irreducibles we

had, we are left with the 6 quintic irreducible polynomials over $\mathbb{F}_2$

$$\begin{array}{lllllllllll}
x^5 & & & & & + & x^2 & & & + & 1 \\
x^5 & & & + & x^3 & & & & & + & 1 \\
x^5 & & & + & x^3 & + & x^2 & + & x & + & 1 \\
x^5 & + & x^4 & & & + & x^2 & + & x & + & 1 \\
x^5 & + & x^4 & + & x^3 & & & + & x & + & 1 \\
x^5 & + & x^4 & + & x^3 & + & x^2 & & & + & 1
\end{array}$$

Exercise 6.6.5. How many monic irreducible polynomials of degree 10 are there over $\mathbb{F}_2$?