NOTES ON FINITE FIELDS

AARON LANDESMAN

CONTENTS

1. Introduction to finite fields

In this course, we'll discuss the theory of finite fields. Along the way, we'll learn a bit about field theory more generally. So, the natural place to start is: what is a field? Many fields appear in nature, such as the real numbers, the complex numbers the rational numbers, and even finite fields! Before giving a formal definition, let's see some examples.

Example 1.1. The rational numbers $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$ are a field. The key properties are that we can multiply rational numbers, add rational numbers (via addition of fractions) and further that nonzero rational numbers have inverses. That is, $\frac{a}{b} \cdot \frac{b}{a} = 1$ whenever $a \neq 0$.

Now, let's see some examples of finite fields.

Example 1.2. Consider the field $\mathbb{F}_2$, the finite field with two elements. Call these elements $0, 1$. The addition law is given by $0 + a = a + 0 = a$ and $1 + 1 = 0$. The multiplication law is given by $1 \cdot a = a$ and $0 \cdot a = 0$. 1 is invertible and its inverse is given by 1 since $1 \cdot 1 = 1$. This can succinctly be described by $\mathbb{Z}/2\mathbb{Z}$.

Example 1.3. Next, let's consider the finite field with 3 elements. As above, we can consider $\mathbb{Z}/3\mathbb{Z}$. Elements can be added and multiplied by reducing addition and multiplication in $\mathbb{Z}$ modulo 3. The key property to check is that nonzero elements have inverses (meaning that for any nonzero a there is some b with $ab = 1$). Indeed, $1 \cdot 1 = 1$ and $2 \cdot 2 = 1$.

Warning 1.4. So far, we have seen that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are fields. However, $\mathbb{Z}/4\mathbb{Z}$ is not a field! The way to see this is that there is no element $a \in \mathbb{Z}/4\mathbb{Z}$ with $2a = 1$. Indeed, either $2a = 2$ or $2a = 0$. So, $\mathbb{Z}/n\mathbb{Z}$ is not in general a field.

Question 1.5. Do you think there exists a finite field of order 4? Do you think there exists a finite field of order 5? Do you think there exists a finite field of order 6? For which $n \in \mathbb{Z}$ does there exist a finite field with n elements?

2. Definition and constructions of fields

Before understanding finite fields, we first need to understand what a field is in general. To this end, we first define fields. After defining fields, if we have one field K, we give a way to construct many fields from K by adjoining elements.

2.1. **The definition of a field.**

A field is a special type of ring. So, we first define a ring:

Definition 2.1. A **commutative ring with unit** is a set R together with two operations $(+, \cdot)$ satisfying the following properties:

(1) Associativity: $a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(2) Commutativity: $a + b = b + a, a \cdot b = b \cdot a$
(3) Additive identity: there exists $0 \in R$ so that $a + 0 = a$
(4) Multiplicative identity: there exists $1 \neq 0 \in R$ so that $1 \cdot a = a$
(5) Additive inverses: For every $a \in R$, there is a additive inverse, denoted $-a$ satisfying $a + (-a) = 0$
(6) Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Remark 2.2. Any mention of "ring" in what follows implicitly means "commutative ring with unit." There will be no noncommutative rings or rings without units.

Definition 2.3. A **field** is a ring K such that every nonzero element has a multiplicative inverse. That is, for each $a \in K$ with $a \neq 0$, there is some $a^{-1} \in K$ so that $a \cdot a^{-1} = 1$.

Definition 2.4. A **finite field** is simply a field whose underlying set is finite.

Example 2.5. Given any prime number p, the set $\mathbb{Z}/p\mathbb{Z}$ forms a field under addition and multiplication. This field is denoted $\mathbb{F}_p$. Nearly all the axioms are immediate, except possibly for the existence of multiplicative inverses.

Exercise 2.6. Verify that every nonzero element has a multiplicative inverse in two ways:

(1) Use the Euclidean algorithm to show that for any $a < p$ there exists some b with $ab \equiv 1 \bmod p$ and conclude that b is an inverse for a. *Hint:* Use that $\gcd(a, p) = 1$.
(2) Show that $a^{p-1} = 1$, so a^{p-2} is an inverse for a. This is also known as "Fermat's Little theorem," not to be confused with "Fermat's Last theorem," which is much more difficult. *Hint:*

Show that the powers of any element form a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times := \mathbb{Z}/p\mathbb{Z} - \{0\}$ under multiplication. Use Lagrange's theorem (i.e., the order of a subgroup divides the order of the ambient group) to deduce that this subgroup generated by a has order dividing $\#(\mathbb{Z}/p\mathbb{Z})^\times = p-1$. Conclude that $a^m = 1$ for some m dividing $p-1$ and hence $a^{p-1} = 1$.

2.2. **Constructing field extensions by adjoining elements.** We now explain how to construct extensions of fields by adjoining elements. Here is a prototypical example:

Example 2.7. Consider the field $\mathbb{Q}\left(\sqrt{2}\right)$. How should we interpret this? The elements of this field are of the form

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}.$$

Multiplication works by

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Here is another perspective on this field: What is $\sqrt{2}$? It is simply a root of the polynomial $x^2 - 2$. Therefore, we could instead consider the field

$$\mathbb{Q}[x]/(x^2 - 2),$$

where this means the ring where we adjoin a root of the polynomial $x^2 - 2$. Concretely, $\mathbb{Q}[x]$ means polynomials with coefficients in $\mathbb{Q}$, and the notation $\mathbb{Q}[x]/(x^2 - 2)$ means that in any polynomial $f(x)$, we can replace x^2 by 2. So for example, if we had the polynomial $x^3 + 2x^2 + 3$ this would be considered equivalent to $(x^2) \cdot x + 2 \cdot (x^2) + 3 = 2x + 4 + 3 = 2x + 7$. In this way, we can replace any polynomial with a polynomial of degree 1 of the form $a + bx$. Identifying x with $\sqrt{2}$ gives the isomorphism of this ring with the above field $\mathbb{Q}\left(\sqrt{2}\right)$.

Exercise 2.8. Describe the elements of the fields K as in Example 2.7 for K one of the following fields

(1) $K = \mathbb{Q}\left(\sqrt{3}\right)$,
(2) $K = \mathbb{Q}\left(7^{1/5}\right)$,
(3) $K = \mathbb{Q}\left(\zeta_3\right)$, for ζ_3 a primitive cube root of unity.

In each of the above cases, write $K = \mathbb{Q}[x]/f(x)$ for an appropriate polynomial f. In each of the above cases, what is the dimension of K over $\mathbb{Q}$, when K is viewed as a $\mathbb{Q}$ vector space?

Definition 2.9. Let K be a field. Define the **polynomial ring**

$$K[x] := \left\{ \sum_{i=1}^{n} a_i x^i : a_i \in K \right\}.$$

For $f \in K[x]$, define

$$K[x]/(f) := K[x]/\sim$$

where $\sim$ is the equivalence relation defined by $g \sim h$ if $f \mid g - h$.

Exercise 2.10. Show that $K[x]/(x) \simeq K$, where the map is given by sending a polynomial to its constant coefficient.

Lemma 2.11. *Let K be a field and let $f \in K[x]$ be a monic irreducible polynomial. Then $K[x]/(f)$ is a field.*

Proof. Note that $K[x]/(f)$ is a ring as it inherits multiplication and addition and all the resulting properties of a ring from $K[x]$. (Check this!) Therefore, it suffices to check that if f is monic and irreducible, then every element has an inverse. In other words, given any $g \in K[x]/(f)$, we need to show there is some h with $gh = 1$. We can consider $g \in K[x]$ as a polynomial of degree less than f. Since f is irreducible, and $\deg g < \deg f$, it follows that the two polynomials share no common factors. Then, by the Euclidean algorithm for polynomials (if you have only seen the euclidean algorithm over the integers, check that the natural analog to the Euclidean algorithm for the integers works equally well in polynomial rings over arbitrary fields, where the remainder is then a polynomial of degree less than the polynomial you are dividing by) we obtain some $h, k \in K[x]$ with $gh + fk = 1$ as elements of $K[x]$. It follows that $gh \sim 1$ in $K[x]/(f)$ because $gh - 1 = fk$ in $K[x]$. □

Exercise 2.12. Let K be a field and $f \in K[x]$ a monic irreducible polynomial. Suppose $L = K[x]/(f)$. Show that $\dim_K L = \deg f$, where $\deg f$ denotes the degree of the polynomial f and $\dim_K L$ denotes the dimension of L as a K vector space.

Example 2.13. Consider the field $\mathbb{F}_2[x]/(x^2 + x + 1)$. We claim this is a finite field of order 4. Indeed, this holds because the polynomial $x^2 + x + 1$ is irreducible. To check this, we only need to check it has no linear factors. It has a linear factor if and only if $x^2 + x + 1$ has a root in $\mathbb{F}_2$. But, when we evaluate it at 0 we get 1 mod 2 and when we evaluate it at 1, we get 1 mod 2. So it has no roots, and the claim follows from Lemma 2.11.

Exercise 2.14. For any $p > 2$, show that there are exactly $\frac{p+1}{2}$ elements $x \in \mathbb{F}_p$ with $x = y^2$ for some $y \in \mathbb{F}_p$. We call such x squares. Conclude that there is some $x \in \mathbb{F}_p$ which is not a square whenever $p > 2$. *Hint:* Show that if $x = y^2$ then we also have $x = (-y)^2$ and further that there y and $-y$ are the only two elements of $\mathbb{F}_p$ squaring to x.

Example 2.15. Let $p > 2$ be a prime and let $\varepsilon \in \mathbb{F}_p$ be an element which is not a square (which exists by Exercise 2.14). Then,

$$\mathbb{F}_p[x]/(x^2 - \varepsilon)$$

is a finite field of order p^2. It is order p^2 because it is a two dimensional vector space over $\mathbb{F}_p$ spanned by the basis 1 and x. It is a field because $x^2 - \varepsilon$ is irreducible in $\mathbb{F}_p[x]$. Indeed, to see this, note that if it were not irreducible, it would factor as a product of two linear factors, which means it would have a root. But, if it had a root, there would be some $y \in \mathbb{F}_p$ so that $y^2 = \varepsilon$. However, we chose ε not to be a square, and so no root exists.

3. A QUICK INTRO TO FIELD THEORY

In order to classify finite fields, we'll need some inputs from field theory. In particular, we'll need to understand maps of fields and the characteristic of a field, which we discuss in this section.

3.1. **Maps of fields.**

Definition 3.1. Given two fields K and L, a **map** $\phi : K \to L$ is a map of sets sending $1 \mapsto 1, 0 \mapsto 0$ such that $\phi(a +_K b) = \phi(a) +_L \phi(b)$ and $\phi(a \cdot_K b) = \phi(a) \cdot_L \phi(b)$.

Remark 3.2. Sometimes, a map of fields is referred to as a homomorphism or extension. Whenever we have a map of fields, it is required to be compatible with the addition and multiplication operations, as defined above. If we do not wish to require such compatibility, we will call the map "a map of sets"

Remark 3.3. We shall typically drop the subscript $+_K, \cdot_K$ on addition and multiplication when it is clear from context.

Exercise 3.4. Verify from the definition of map that

$$\phi(a^{-1}) = \phi(a)^{-1}$$

and

$$\phi(-a) = -\phi(a).$$

We next prove that maps of fields are injective. If you have not worked much with the notion of injectivity before, you may want to try the following exercise first.

Exercise 3.5. Show that a map of rings is injective (using the definition that $f : R \to S$ is injective if $f(a) = f(b)$ implies $a = b$) if and only if the only element mapping to 0 is 0. *Hint:* Consider $f(a - b)$.

Lemma 3.6. *Any map of fields is injective.*

Proof. By Exercise 3.5 it suffices to show that any $c \neq 0$ does not satisfy $\phi(c) = 0$. Suppose there is some such c. But note that $1 = \phi(1) = \phi(cc^{-1}) = \phi(c)\phi(c^{-1}) = 0\phi(c^{-1}) = 0$, a contradiction. Therefore, every nonzero element does not map to 0 and the map is injective. □

Remark 3.7. Because of Lemma 3.6, a map of fields is also typically called an **extension of fields** or a field extension.

Remark 3.8. The property that maps of fields are injective is very special to fields. Indeed, it is not true for groups. For example, the map $\mathbb{Z} \to \{1\}$ is not injective!

Remark 3.9. Using Lemma 3.6, whenever we have a map of fields $\phi : K \to L$, we can consider L as a vector space over K. The map $K \times L \to L$ corresponding to scalar multiplication is given by

$$K \times L \to L$$
$$(a, b) \mapsto \phi(a) \cdot b$$

3.2. **Characteristic of a field.**

Definition 3.10. Let K be a field. If there is some n so that

$$n := \underbrace{1 + 1 + \cdots + 1}_{n} \tag{3.1}$$

is equal to 0 in K, the the minimal such n is defined to be the **characteristic** of K, denoted $\mathrm{char}(K)$. If no such $n \in \mathbb{Z}_{\geq 0}$ exists, then we say K has characteristic 0.

Example 3.11. The rational numbers $\mathbb{Q}$ has characteristic 0, but the field $\mathbb{F}_p$ has characteristic p.

Exercise 3.12 (Important exercise)**.** Let p be a prime number and suppose K is a field of characteristic p. Show that for any $x, y \in K$, we have

$$(x + y)^p = x^p + y^p.$$

Hint: Expand the left hand side using binomial coefficients, and show that p divides nearly all of the binomial coefficients.

3.3. **Showing the characteristic of any finite field is a prime.**

Lemma 3.13. *The characteristic of any field is either* 0 *or prime.*

Proof. Note that the characteristic cannot be 1 because $1 \neq 0$. So, we have to show that the characteristic is never composite.

Let n be a composite number with $n = fg$ for $f, g > 1$ two factors of n.

Exercise 3.14. Suppose $a, b \in K$ with $ab = 0$. Then show either $a = 0$ or $b = 0$.

By the above exercise, if $n = fg = 0$, then either $f = 0$ or $g = 0$. Say $f = 0$. But then, we obtain that $f < n$, and so K does not have characteristic n. □

Definition 3.15. For K a field, we say a subset $K' \subset K$ is a **subfield** if it is a field and the inclusion $K' \subset K$ is a map of fields (meaning $1 \mapsto 1, 0 \mapsto 0$ and the multiplication and addition are compatible).

Exercise 3.16. Verify similarly that any field of characteristic 0 contains $\mathbb{Q}$ as a subfield. *Hint:* Define a map of fields

$$\begin{aligned} \phi\colon \mathbb{Q} &\to K \\ \frac{a}{b} &\mapsto ab^{-1}. \end{aligned}$$

Use that $b \in K$ is nonzero by the assumption that K has characteristic 0 to show this is well defined.

Lemma 3.17. *The characteristic of any finite field is prime (and, in particular, never 0).*

Proof. By Lemma 3.13, we only need to show the characteristic of a finite field is nonzero. So, it suffices to show every characteristic 0 field is infinite. But, by Exercise 3.16, every characteristic 0 field contains $\mathbb{Q}$ as a subfield, and is therefore infinite. □

Lemma 3.18. *Any field K of characteristic $p > 0$ (for p a prime) contains $\mathbb{F}_p$ as a subfield.*

Proof. Inside K, consider the subset $\{0, 1, 2, \ldots, p-1\}$. These form p distinct elements because $\operatorname{char} K = p$. By definition, of $n = \underbrace{1 + 1 + \cdots + 1}_{n}$, the elements $0, 1, \ldots, p-1$ satisfy the same addition and multiplication rules as $\mathbb{F}_p \simeq (\mathbb{Z}/p\mathbb{Z})$. Therefore, when we restrict the multiplication and addition from K to $\{0, 1, 2, \ldots, p-1\}$, we realize $\mathbb{F}_p$ as this subfield. □

Lemma 3.19. *Any finite field K has order p^n for p a prime and $n \in \mathbb{Z}$.*

Proof. By Lemma 3.18, K contains $\mathbb{F}_p$ as a subfield, so we have an inclusion $\mathbb{F}_p \to K$. Observe that this makes K into a vector space over $\mathbb{F}_p$. Because K is finite, it must even be a finite dimensional vector space over $\mathbb{F}_p$. Say it has dimension n. Then we see that as a vector space, $K \simeq \mathbb{F}_p^n$, so $|K| = |\mathbb{F}_p|^n = p^n$, as desired. □

So, we have established that every finite field has order a prime power. Our next goal is to show that there is a unique finite field of order p^n. However, for this, we will need to introduce algebraic closures, which we do now.

4. Algebraic closures

To hit the ground running on finite fields, we'll need to know about "algebraic closures."

Definition 4.1. An extension of fields $\phi : K \to L$ is **finite** if ϕ makes L into a finite dimensional vector space over K. An extension of fields $\phi : K \to L$ is **algebraic** if for every $a \in L$, there is a finite extension $K \to L_a$ with $L_a \subset L$ a subfield containing a.

In order to get the theory of finite fields off the ground, we will need the existence of an algebraic closure. It is not too difficult to show this exists, but to jump to the interesting stuff, we will defer it for later:

Definition 4.2. A field K is **algebraically closed** if any finite field extension $K \to L$ is an isomorphism.

Exercise 4.3. Show that the real numbers are not algebraically closed. Show that the rational numbers are not algebraically closed.

Lemma 4.4. *Let K be a field. The following are equivalent.*

1. *K is algebraically closed.*
2. *Every monic irreducible polynomial over K has a root.*
3. *Every monic irreducible polynomial over K factors as a product of linear polyomials.*

Proof. For $(1) \implies (2)$, we suppose K is algebraically closed and show every monic irreducible polynomial over K has a root. Let f be any monic irreducible polynomial over K. Then, $K[x]/(f)$ is a field extension of K. Because K is algebraically closed, the natural map $K \to K[x]/(f)$ is an isomorphism. Therefore, $\dim_K K[x]/(f) = 1$ and so f has degree 1 by Exercise 2.12 (which says $\deg f = \dim_K K[x]/(f)$), and hence has a root.

Next, if (2) holds, one can prove (3) by induction on the degree of the polynomial.

Finally, for $(3) \implies (1)$, suppose K is not algebraically closed. We want to show there is some irreducible polynomial over K which does not factor completely. Let L be a finite extension of K with the inclusion $K \to L$ not an isomorphism. Since $K \to L$ is an injection it is not a surjection, so we may take some $y \in L \setminus K$. We claim there is some monic irreducible polynomial $f \in K[x]$ with $f(y) = 0$. Indeed, this is the content of the following exercise.

Exercise 4.5. Let $K \to L$ be an algebraic extension. Show that any element $x \in L$ satisfies some monic irreducible polynomial $f(x) =$

$x^n + k_{n-1}x^{n-1} + \cdots + k_0$, for $k_i \in K$. *Hint:* By definition of an algebraic extension, show that the powers of x satisfy some linear dependence relation, and obtain the monic irreducible polynomial from this relation.

Note that since $y \notin K$, the polynomial f with $f(y) = 0$ has degree more than 1. Since f is irreducible and has degree more than 1, f does not have a root in K, as we wanted to show. □

Exercise 4.6. Show that the complex numbers are algebraically closed (you may assume that every polynomial over the complex numbers has a root).

Definition 4.7. A field extension $K \to \overline{K}$ is an **algebraic closure** if

(1) $K \to \overline{K}$ is algebraic and
(2) $\overline{K}$ is algebraically closed.

Exercise 4.8. Let $K \to L$ be an algebraic extension and let $\overline{L}$ denote an algebraic closure of L. Show that $\overline{L}$ is also an algebraic closure of K.

Theorem 4.9 (Existence of algebraic closures)**.** *Let K be a field.*

(1) K has an algebraic closure.
(2) Any two algebraic closures of K are isomorphic as field extensions (meaning that for two algebraic closures $\overline{K}, \overline{K}'$, with K as a subfield via the maps $\phi : K \to \overline{K}, \phi' : K \to \overline{K}'$, there is an isomorphism $f : \overline{K} \to \overline{K}'$ so that $f \circ \phi = \phi'$).

5. Characterization of finite fields

Using the existence of an algebraic closure, we are now ready to show there is a unique finite field of order p^n, for every prime p and every $n \geq 1$.

First, we need a preparatory definition and lemma.

Definition 5.1. If K is a field and $f := \sum_{i=1}^n a_i x^i \in K[x]$ is a polynomial, we define the derivative of f, denoted f', to be $\sum_{i=1}^n i a_i x^{i-1}$.

Lemma 5.2. *Let K be an algebraically closed field and let $f \in K[x]$ be a polynomial. Then, if $\gcd(f, f') = 1$, f has no repeated roots. That is, there is no $a \in K$ with $(x-a)^2 \mid f$.*

Proof. Suppose f has a repated root. Call that root $r \in K$. Then since $(x-r)^2 \mid f$, it follows from the product rule that $x - r \mid f'$. Therefore, $x - r \mid \gcd(f, f')$, and so $\gcd(f, f') \neq 1$, as desired. □

We can now state and prove our main result.

Theorem 5.3. *Let p be a prime and $n \geq 1$.*

1. *There exists a finite field of order p^n, notated $\mathbb{F}_{p^n}$. Further, $\mathbb{F}_{p^n}$ is realized as the set of elements of $\overline{\mathbb{F}}_p$ satisfying $x^{p^n} = x$.*
2. *Any two finite fields of order p^n are isomorphic.*

Proof. First let us show there exists a finite field of order p^n. Let $\overline{\mathbb{F}}_p$ denote an algebraic closure of $\mathbb{F}_p$. Define

$$\mathbb{F}_{p^n} := \left\{ x \in \overline{\mathbb{F}}_p : x^{p^n} = x \right\}.$$

We claim $\mathbb{F}_{p^n}$ is a field. To check this, the essential points to verify are that $\mathbb{F}_{p^n}$ is closed under multiplication, addition, and inversion.

1. Addition: We need to show that if $x^{p^n} = x, y^{p^n} = y$ then $(x+y)^{p^n} = x + y$. Indeed, this follows from Exercise 3.12.
2. Multiplication: We need to show that if $x^{p^n} = x, y^{p^n} = y$ then $(xy)^{p^n} = xy$. Indeed, this is clear by commutativity of $\overline{\mathbb{F}}_p$.
3. Inversion: Given $x \neq 0$ with $x^{p^n} = x$, we want to show x^{-1} (which exists as an element of $\overline{\mathbb{F}}_p$) satisfies $(x^{-1})^{p^n} = x^{-1}$. But indeed,
$$(x^{-1})^{p^n} = (x^{p^n})^{-1} = x^{-1},$$
as desired.

Exercise 5.4. Verify the remaining properties such as distributivity and commutativity to show that $\mathbb{F}_{p^n}$ is indeed a field. *Hint:* You may be able to inherit many of these properties from $\overline{\mathbb{F}}_p$.

To complete the proof of existence, we have to check that $|\mathbb{F}_{p^n}| = p^n$. Indeed, by construction, the elements of $\mathbb{F}_{p^n}$ are the set of roots to the polynomial $f(t) = t^{p^n} - t$. So, it suffices to show this has p^n distinct roots in $\overline{\mathbb{F}}_{p^n}$. Note that $f(t)$ has at most p^n roots because it has degree p^n. Since $\overline{\mathbb{F}}_{p^n}$ is algebraically closed, $f(t)$ factors as a product of p^n distinct linear factors, by Lemma 4.4. Further, the roots of $f(t)$ are all distinct by Lemma 5.2 because $f'(t) = p^n \cdot t^{p^n-1} - 1 = -1$.

So, we have shown existence of finite field over order p^n. It remains to show uniqueness up to isomorphism.

Let K be some finite field of size p^n. We want to construct an isomorphism $K \simeq \mathbb{F}_{p^n}$. Because K is finite, hence algebraic over $\mathbb{F}_p$, it follows from Exercise 4.8 that an algebraic closure of K is also an algebraic closure of $\mathbb{F}_p$, and we denote this algebraic closure by $\overline{\mathbb{F}}_p$. Choose an extension $\phi : K \to \overline{\mathbb{F}}_p$. We will show $\operatorname{im}\phi \subset \mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$. This will complete the proof as it will imply that ϕ defines a map between two fields of size p^n. It is then injective by Lemma 3.6 and hence it will be surjective because it is an injective map between two sets of the same finite size.

So, we will now show $\operatorname{im}\phi \subset \mathbb{F}_{p^n}$. For this, it suffices to show that any $x \in K$ satisfies $\phi(x)^{p^n} = \phi(x)$. For this, it suffices to show $x^{p^n} = x$. This clearly holds for $x = 0$, so after dividing by x, it suffices to show $x^{p^n-1} = 1$. But now, note that $K^\times := K - \{0\}$ is a multiplicative group of size $|K^\times| = |K| - 1 = p^n - 1$. Lagrange's theorem tells us that the order of any element of a group divides the order of the group. This implies that $x^m = 1$ for some $m \mid p^n - 1$, which implies that $x^{p^n-1} = 1$. $\square$

6. Properties of finite fields

We next develop several interesting properties of finite fields.

6.1. **The multiplicative group of a finite field.** As we saw near the end of the proof of Theorem 5.3, because multiplicative inverses exist, for any field K, the nonzero elements $K^\times$ form a group under multiplication. The identity element is 1. It turns out that finite fields have a particularly nice multiplicative structure.

Proposition 6.1. *There is an isomorphism $\mathbb{F}_{p^n}^\times \simeq (\mathbb{Z}/(p^n-1)\mathbb{Z})$. That is, $\mathbb{F}_{p^n}^\times$ is cyclic.*

Proof. To show $\mathbb{F}_{p^n}^\times$ is cyclic of order p^n-1, since we know it has order p^n-1 as a group, it suffices to show there is some element of order p^n-1.

Exercise 6.2 (Tricky exercise)**.** Verify using that all finite abelian groups are products of cyclic groups (the fundamental theorem for finite abelian groups) that if there is no element of order p^n-1 then there is some $m < p^n-1$ with $x^m = 1$ for all $x \in \mathbb{F}_{p^n}^\times$. *Hint:* Show that if $G \simeq \prod_i \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, (where the isomorphism holds by the fundamental theorem of finite abelian groups) has some $p_i = p_j$ for $i \neq j$ then then every element of G has order strictly less than $|G| = \prod_i p_i^{n_i}$. For this it may help to consider the subgroup $\mathbb{Z}/p_i^{n_i} \times \mathbb{Z}/p_j^{n_j}$. Then, show using the Chinese Remainder theorem that if $p_i \neq p_j$ for any $i \neq j$ then G is cyclic.

However, we cannot have $x^m = 1$ for all $x \in \mathbb{F}_{p^n}^\times$ with $m < p^n-1$ because $x^m - 1$ only has $m < p^n-1$ roots in $\overline{\mathbb{F}}_p$. Hence, there is some element of $\mathbb{F}_{p^n}^\times$ of order exactly p^n-1, and so it is isomorphic to $\mathbb{Z}/(p^n-1)\mathbb{Z}^\times$. □

Exercise 6.3. Using Proposition 6.1 we can now prove results about roots of unity modulo primes.

(1) Let p be an odd prime. Using Proposition 6.1, show that -1 is a square mod p if and only if $p \equiv 1 \bmod 4$.
(2) Let p be an odd prime. Show that there is some $x \not\equiv 1 \bmod p$ so that $x^3 \equiv 1 \bmod p$ if and only if $p \equiv 1 \bmod 3$.
(3) Let p be an odd prime. Determine a necessary and sufficient condition on p modulo n such that there will be n distinct roots of unity modulo p, i.e., there are n distinct residues $x_1, \dots, x_n \bmod p$ with $x_i^n \equiv 1 \bmod p$.

(4) Given n and p, determine the number of nth roots of unity $\bmod p$. That is, determine the number of residues x so that $x^n \equiv 1 \bmod p$.

Exercise 6.4. Prove Wilson's theorem: show that $(p-1)! \equiv -1 \bmod p$.

6.2. **Frobenius.** In what follows, we will let q denote a power of p, say $q = p^n$.

Definition 6.5. The map

$$\begin{aligned} \mathrm{Frob}_p \colon \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto x^p \end{aligned}$$

is the **Frobenius** map.

Exercise 6.6. Verify that Frob_p is a map $\mathbb{F}_q \to \mathbb{F}_q$ over $\mathbb{F}_p$. That is, show that the natural inclusion $i : \mathbb{F}_p \to \mathbb{F}_q$ respects Frob_p in the sense that $\mathrm{Frob}_p \circ i = i$. *Hint:* Show that for any $x \in \mathbb{F}_p$, $x^p = x$. See Exercise 2.6(2) for further help.

Our next goal is to show that the automorphisms of $\mathbb{F}_q$ over $\mathbb{F}_p$ (i.e., maps $\mathbb{F}_q \to \mathbb{F}_q$ as vectors spaces over $\mathbb{F}_p$) are precisely $\mathrm{id}, \mathrm{Frob}_p, \ldots, \mathrm{Frob}_p^{n-1}$, where $q = p^n$. First, we show that these are all distinct:

Lemma 6.7. *Let $q = p^n$. The maps $\mathrm{id}, \mathrm{Frob}_p, \ldots, \mathrm{Frob}_p^{n-1}$ are distinct as maps $\mathbb{F}_q \to \mathbb{F}_q$.*

Proof. We wish to show $\mathrm{Frob}_p^a \neq \mathrm{Frob}_p^b$ for $0 \leq a < b \leq n-1$. After composing with Frob_p^{-a}, it suffices to show that Frob_p^{b-a} is not the identity for any $0 < b-a \leq n-1$. That is, we have to show $\mathrm{Frob}_p, \ldots, \mathrm{Frob}_p^{n-1}$ are all distinct from id.

To show that Frob_p^c is not the identity, we have to show there is some $x \in \mathbb{F}_q$ with $x^{p^c} \neq x$. However, since $x^{p^c} - x$ is a polynomial of degree p^c, there are at most p^c such elements. Since $|\mathbb{F}_q| = p^n > p^c$, there is some element $x \in \mathbb{F}_q$ with $x^{p^c} \neq x$. □

Hence, we have produced that there are at least p distinct automorphisms of $\mathbb{F}_q$ given by powers of Frobenius. We next want to show that these are all the automorphisms of $\mathbb{F}_q$. For this, we will now give an explicit construction of $\mathbb{F}_q$ as a field, by adjoining an element to $\mathbb{F}_p$, via the method in subsection 2.2.

Lemma 6.8. *We can express $\mathbb{F}_{p^n}$ in the form $\mathbb{F}_p[x]/(f)$ for $f \in \mathbb{F}_p[x]$ of degree n.*

Proof. Pick $y \in \mathbb{F}_{p^n}$ to be a generator of $\mathbb{F}_{p^n}^\times$ (which is possible by Proposition 6.1). Note that y generates $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ because all nonzero elements of $\mathbb{F}_{p^n}$ are powers of y. Further, by Exercise 4.5, (recall this says that any element in an algebraic extension satisfies some monic irreducible polynomial) y satisfies some irreducible monic polynomial f over $\mathbb{F}_p$. We obtain that $\mathbb{F}_p[x]/(f)$ is a field by Lemma 2.11. We obtain a map

$$\begin{aligned} \phi\colon \mathbb{F}_p[x]/(f) &\to \mathbb{F}_q \\ x &\mapsto y. \end{aligned}$$

Exercise 6.9. Verify this is a well defined map.

This map is necessarily injective by Lemma 3.6 but it is also surjective because y generates $\mathbb{F}_q$. Therefore it is an isomorphism. It follows that f must have degree n since $\mathbb{F}_p[x]$ is a dimension $\deg f$ vector space over $\mathbb{F}_p$, but it is also isomorphic to $\mathbb{F}_{p^n}$, which is a dimension n vector space over $\mathbb{F}_p$. □

Corollary 6.10. *The automorphisms of $\mathbb{F}_q$ over $\mathbb{F}_p$ are precisely* $\mathrm{id}, \mathrm{Frob}_p, \dots, \mathrm{Frob}_p^{n-1}$.

Proof. We have seen in Lemma 6.7 that these are all distinct, so it suffices to show there are at most n automorphisms of $\mathbb{F}_q$ over $\mathbb{F}_p$. However, by Lemma 6.8, we have $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$. Note that any map $\mathbb{F}_p[x]/(f) \to \mathbb{F}_p[x]/(f)$ must send x to some root of f, and further the map is determined by where it sends x. Since $\deg f = n$, there are at most $\deg f = n$ roots of f and hence at most n such maps, as we wanted to show. □

6.3. **Containments of finite fields.** Let us now determine when $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ for $m, n > 0$. First, we establish this containment when $m \mid n$.

Lemma 6.11. *If $m \mid n$ then $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$.*

Proof. Recall from Theorem 5.3 that $\mathbb{F}_{p^m}$ was precisely the set of elements in $\overline{\mathbb{F}}_p$ with $x^{p^m} = x$. We also have $x^{p^{2m}} = x^{p^m} = x$. If $m \mid n$, say $m = dn$ then iterating this d times we obtain $x^{p^n} = x^{p^{dm}} = x^{p^{(d-1)m}} = \cdots = x^{p^m} = x$, so $x \in \mathbb{F}_{p^n}$. □

In fact, the above case is the only case that $n \mid m$, as we will now see.

Proposition 6.12. *For p a prime and $n, m > 0$, we have $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m \mid n$.*

Proof. If $m \mid n$, then the inclusion holds by Lemma 6.11. Conversely, if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ then $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^m}$. Say $\mathbb{F}_{p^n}$ has dimension d over $\mathbb{F}_{p^m}$. It follows that $|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d$, so $p^n = (p^m)^d = p^{md}$ and so $m \mid n$. $\square$

APPENDIX A. EXISTENCE OF ALGEBRAIC CLOSURES

We now guide the reader through a proof of the existence of algebraic closures in series of exercises.

We first prove the existence of an algebraic closure Theorem 4.9(1), and then show it is unique up to (non-unique) isomorphism. The key to proving the existence of an algebraic closure will be Zorn's lemma, which we now recall:

Lemma A.1. *Suppose I is a partially ordered set. Suppose any totally ordered subset $I' \subset I$ has a maximum element, i.e., there is some $i \in I$ with $i \geq j$ for all $j \in I'$. Then I contains a maximal element, i.e., there is some $i \in I$ so that for any $j \in I, j \not> i$.*

Remark A.2. Zorn's lemma is not a lemma in the conventional sense because it is equivalent to the axiom of choice. Therefore, we will not prove it, but rather take it as an axiom.

We next aim to prove existence of algebraic closures. Logically, if you'd like, you can skip directly to Exercise A.5. However, it may help your understanding of that exercise if you do the prior exercises first.

Exercise A.3. We now prove some basic properties about cardinalities of field extensions.

(1) Show that if L is an algebraic extension of a finite field K, then $|L| \leq |\mathbb{Z}|$. Here $|S|$ denotes the set-theoretic **cardinality** of a set S.
(2) Show that if L is an algebraic extension of an infinite field K, then $|L| = |K|$. *Hint:* Show that K has the same cardinality as $K[x]$ and defined a map of sets $L \to K[x]$ by sending an element to its minimal polynomial. Show that there are only finitely many elements with a given minimal polynomial and deduce $|K| = |L|$.
(3) Conclude that for any infinite field K, if T is a set with $|T| > |K|$ then for any algebaic extension L of K, we have $|T| > |L|$.
(4) Conclude that for any field K if T is an infinite set with $|T| > |K|$, then $|T| \geq |L|$ for any algebraic extension L of K. (By the above, the only interesting case is the case that K is finite.)

Exercise A.4. Assume K is an infinite field. Using Exercise A.3, solve a slightly simplified version of Exercise A.5 with the modification that S is any set so that $|S| > |K|$ (so that there is no intermediate set T in the picture). Therefore, the addition of T is only needed to deal with finite fields.

Exercise A.5 (Difficult exercise)**.** Use Zorn's lemma to show an algebraic closure of a field K exists as follows: Let T be an infinite set with $|T| > |K|$ and let S be a set with $|S| > |T|$.

(1) Consider the partially ordered set

$$R := \{(L, \phi) : L \text{ is an algebraic extension of } K \text{ and } \phi : L \hookrightarrow S \text{ is a subset }\}$$

Check that one can define a partial ordering on R by declaring $(L_1, \phi_1) \leq (L_2, \phi_2)$ if $i : L_1 \to L_2$ is an algebraic extension, and $\phi_2 \circ i = \phi_1$.

(2) Use Zorn's lemma, Lemma A.1, to show that R has a maximal element, call it (M, ϕ).

(3) Show that M is algebraically closed by showing that if $i : M \to N$ is any algebraic extension then there is a map $\psi : N \to S$ with $\psi \circ i(x) = \phi(x)$. *Hint:* Use that $|N| \leq |M| \leq |T| < S$ and $|S - M| = |S| > |N - M|$.

Exercise A.6. Suppose we have an algebraic extension $K \subset L$ and $K \subset \overline{K}$ with $\overline{K}$ algebraically closed. Show that there is a map of extensions $L \to \overline{K}$ in the following steps:

(1) Consider the partially ordered set I of pairs (M, ϕ) with $K \subset M \subset L$ and $\phi : M \to \overline{K}$ a map of fields. Check that the relation

$$(M_1, \phi_1) \leq (M_2, \phi_2)$$

if $M_1 \subset M_2$ and $\phi_2|_{M_1} = \phi_1$ defines a partial ordering on such pairs (M, ϕ).

(2) Show that any totally ordered subset $I' \subset I$ corresponding to a collection $\{(M_i, \phi_i)\}_{i \in I'}$ has a maximum element given by taking $(\cup_i M_i, \cup_i \phi_i)$, with $\cup_i \phi_i$ interpreted suitably.

(3) Using Zorn's lemma obtain a maximal element (M, ϕ) of I.

(4) Verify that the maximum element (M, ϕ) has $M = L$ and conclude there is a map $L \to \overline{K}$ *Hint:* Suppose $L \neq M$. Then there is some $x \in L - M$. Show that x satisfies some minimal polynomial over L. Deduce there is a map $M(x) \to \overline{K}$ restricting to the given map $\phi : M \to \overline{K}$, and hence (M, ϕ) was not maximal.

Exercise A.7. Prove Theorem 4.9(2) using Exercise A.6 as follows:

(1) Show that for any two algebraic closures $\overline{K}_1, \overline{K}_2$ of the same field K there is an injective map between $\phi : \overline{K}_1 \to \overline{K}_2$.

(2) Show that the injective map ϕ is an algebraic extension.

(3) Conclude that the map produced $\overline{K}_1 \to \overline{K}_2$ is an isomorphism from the definition of algebraic closure.

APPENDIX B. BASICS OF RINGS

In this appendix, we review some basic definitions relating to rings. Recall our definition of a (commutative) ring (with unit), Definition 2.1. We repeat this now for your convenience.

Definition B.1. A **commutative ring with unit** is a set R together with two operations $(+, \cdot)$ satisfying the following properties:

(1) Associativity: $a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(2) Commutativity: $a + b = b + a, a \cdot b = b \cdot a$
(3) Additive identity: there exists $0 \in R$ so that $a + 0 = a$
(4) Multiplicative identity: there exists $1 \neq 0 \in R$ so that $1 \cdot a = a$
(5) Additive inverses: For every $a \in R$, there is a additive inverse, denoted $-a$ satisfying $a + (-a) = 0$
(6) Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

For us, all rings will be commutative rings with unit, and so we will simply refer to them as rings from now on. We now recall some elementary properties of rings. Many of these follow directly from the analogous properties for groups.

Exercise B.2. Verify, directly from the definition that every ring has a unique 0 and 1. Show that for any $a \in R$, a has a unique additive inverse, and so the name $-a$ is justified.

Definition B.3. A **map** of rings $f : R \to S$ is a map of sets such that $f(1_R) = 1_S, f(0_R) = 0_S, f(a +_R b) = f(a) +_S f(b)$ and $f(a \cdot_R b) = f(a) \cdot_S f(b)$. where the subscripts denote the identity, multiplication, and addition in the corresponding ring.

Definition B.4. A ring map $f : R \to S$ is **injective** if $f(a) = f(b) \implies a = b$. It is **surjective** if for every $s \in S$ there is some $r \in R$ with $f(r) = s$. It is **bijective** (also known as an **isomorphism**) if it is both injective and surjective. If $f : R \to S$ is bijective, we write $R \simeq S$.

Exercise B.5. Show that a ring map $f : R \to S$ is injective if and only if $f^{-1}(0_S) = 0_R$.

Exercise B.6. Show that a ring map $f : R \to S$ is bijective if and only if there is a ring map $f^{-1} : S \to R$ so that $f^{-1} \circ f = \mathrm{id}_R, f \circ f^{-1} = \mathrm{id}_S$. *Hint:* Show that a map is bijective if and only if there is a unique element of R mapping to any given element of S. Use this to define an inverse map.

B.1. **Quotients.** The following will not be needed in this course. Indeed, we will construct particular quotient rings in this course, but these quotients will all be of the form $K[x]/(f)$ for K a field, a situation which is much more concrete than the general case developed below. We encourage you to skip the following, but we include it for completeness.

Definition B.7. An **ideal** I of R is a subset $I \subset R$ so that

(1) $0_R \in I$.
(2) For any $r \in I$ we also have $-s \in I$.
(3) If $a, b \in I$ then $a + b \in I$.
(4) If $r \in R$ and $a \in I$ then $a \cdot_R b \in I$.

Definition B.8. Let $I \subset R$ be a subring. Construct the **quotient** R/I as the set of all elements $a \in R$ modulo the equivalence relation $a \sim b$ if there is some $c \in I$ with $a = b + c$. The equivalence class of a is called the **coset of** a and the coset is notated $a + I$.

Exercise B.9. Verify that the relation $\sim$ as defined in Definition B.8 is indeed an equivalence relation.

Exercise B.10. Show that if $I \subset R$ is an ideal then R/I is again a ring. (Under our definition, this includes verifying that the quotient is commutative and has a unit).

REFERENCES