

Lecture Notes for Math 696  
Coding Theory

Michael E. O'Sullivan  
mosulliv@math.sdsu.edu  
[www-rohan.sdsu.edu/~mosulliv](http://www-rohan.sdsu.edu/~mosulliv)

January 19, 2006

# Introduction

## Introduction

Since the birth of the subject roughly 50 years ago, coding theory has grown enormously and has become enriched by its relationship with many areas of mathematics. There are a number of excellent books on coding theory, but the challenge to write my own notes and cover the topics in the manner that made most sense to me proved irresistible. Here in this first installment we will cover the algebraic preliminaries: polynomial rings and finite fields being the essential topics. A later set of notes will cover Reed-Solomon codes and decoding by the Berlekamp-Massey algorithm. I hope to add some sections expanding beyond Reed-Solomon codes later in the semester.

I hope you will enjoy these notes, and enjoy being part of this project of mine to put them together. Please be patient with the typos and various problems that are certain to be encountered. Although I have revised and reread a number of times, there will still be mistakes. Please also inform me of any problems whether they be mundane errors, stylistic confusion or (heaven forbid) mathematical errors.

I will use the following notation.

- The positive integers:  $\mathbb{N}$ .
- The nonnegative integers:  $\mathbb{N}_0$ .
- The integers greater than or equal to  $a$ :  $\mathbb{N}_a$ .
- All integers:  $\mathbb{Z}$ .
- The integers modulo  $n$ :  $\mathbb{Z}/n$ .
- The rationals:  $\mathbb{Q}$ .
- The real numbers:  $\mathbb{R}$ .
- The complex numbers:  $\mathbb{C}$ .
- The finite field of  $q$  elements:  $\mathbb{F}_q$ .

# Chapter 1

## Commutative Rings and Finite Fields

### 1.1 Review of Properties of the Integers

In this section we will review the main theorems that lead to the unique factorization of integers. We will establish analogous results for polynomials over a field in a later section. Proofs are sometimes omitted or are briefly sketched in this section. I recommend Chapter 3 of Rosen's book [7] for a more detailed treatment of this material.

**Theorem 1.1.1 (Division).** *Given integers  $a, b$  with  $b > 0$  there exist unique integers  $q, r$  such that*

- 1)  $a = bq + r$ , and
- 2)  $0 \leq r < b$ .

PROOF: Consider the set  $S = \{a - bk : k \in \mathbb{Z}\}$ . By the well ordering property of the natural numbers, there exists a smallest nonnegative integer in  $S$ . Call it  $r$  and let  $r = a - bq$ . Then  $q$  and  $r$  satisfy item 1). Furthermore  $r$  must be less than  $b$ , for otherwise  $r - b = a - b(q + 1)$  would be in  $S$  and less than  $r$ , contradicting the choice of  $r$ . So item 2) is satisfied. For uniqueness, suppose that  $q'$  and  $r'$  also satisfy items 1) and 2). Taking the difference of the two equations from 1), we get  $r - r' = b(q' - q)$ . From 2),  $|r - r'| < b$ , but  $|b(q' - q)| \geq b$  when it is nonzero. Thus we must have  $q = q'$  and  $r = r'$ .

□

**Definition 1.1.2.** Let  $a$  and  $b$  be integers, not both equal to 0. The *greatest common divisor* of  $a$  and  $b$ , denoted  $\gcd(a, b)$ , is the largest positive integer dividing both  $a$  and  $b$ . If the gcd is 1 we say  $a$  and  $b$  are *coprime*.

**Theorem 1.1.3.** *Given integers  $a, b$ , not both 0, the greatest common divisor of  $a$  and  $b$  may be written as a linear combination of  $a$  and  $b$ .*

PROOF: (Sketch) Choose the smallest positive element of  $\{ra + sb : r, s \in \mathbb{Z}\}$ , call it  $d$ . It is clear that any common divisor of  $a$  and  $b$  divides  $d$ . Show that the remainder when

either  $a$  or  $b$  is divided by  $d$  must be 0, otherwise the definition of  $d$  is violated. Thus  $d$  must be  $\gcd(a, b)$ .  $\square$

The preceding result simply says that the gcd of two integers can be written as a linear combination of the two. The next result—2000 years old—describes how to compute the gcd.

**Theorem 1.1.4.** *The Euclidean algorithm may be used to find the greatest common divisor of two integers, and to find the linear combination that gives the greatest common divisor.*

In Section 1.6, there is a matrix version of the Euclidean algorithm which computes the linear combination that gives the gcd. It is very similar to a matrix version of the Berlekamp-Massey algorithm for decoding Reed-Solomon codes that we will see in a later Chapter.

**Definition 1.1.5.** A nonzero integer  $p$  is *irreducible* when any factorization  $p = ab$  is trivial: either  $a$  or  $b$  is  $\pm 1$ . A nonzero integer  $p$  is *prime* whenever  $p$  divides  $ab$  implies that  $p$  divides either  $a$  or  $b$ .

In a first course in number theory one normally defines a prime as we have defined an irreducible. The reason for the switch here is to conform with the modern usage in commutative algebra. Notice that a prime number, or an irreducible, may be negative.

If you look for the following theorem in a number theory book it will say: “Suppose  $p$  is prime, then if  $p$  divides  $ab$  either  $p$  divides  $a$  or  $p$  divides  $b$ .”

**Theorem 1.1.6.** *Let  $p \in \mathbb{Z}$  be irreducible. Then  $p$  is prime. The converse is also true, so  $p$  is irreducible if and only if it is prime.*

PROOF: Suppose  $p$  is irreducible and  $p|ab$ . If  $p \nmid a$  then  $\gcd(p, a) = 1$ , so there are integers  $r$  and  $s$  such that  $pr + as = 1$ . Multiplying by  $b$  we have  $prb + asb = b$ . Now  $p$  divides the left hand side, so  $p|b$ .

For the reverse implication, suppose  $p$  is prime and  $p = ab$ . Without loss of generality, we may assume  $p|a$ , say  $a = pk$ . Then  $p = pkb$ , hence  $p(1 - kb) = 0$ . Since  $p$  is nonzero  $1 - kb = 0$ . But then  $b$  is  $\pm 1$ .  $\square$

Now we have unique factorization!

**Theorem 1.1.7.** *Given any nonzero  $n \in \mathbb{Z}$  there is a unique way to write  $n$  as a product*

$$n = u \prod_{i=1}^r p_i$$

where  $r \in \mathbb{N}_0$ , the  $p_i$  are positive primes with  $p_i \leq p_{i+1}$ , and  $u = \pm 1$ .

PROOF: Clearly  $u = -1$  for negative integers and  $u = 1$  for positive integers, and it is sufficient to prove the result for positive integers. We first show existence of a prime factorization by induction. For  $n = 1$  the result is trivial,  $r$  must be zero. Assuming that any integer less than  $n$  has a unique prime factorization, consider  $n$ . If  $n$  is prime then  $n = 1n$  is a prime factorization. If  $n$  is composite then  $n = ab$  for  $a, b < n$ . The product of the prime factorizations for  $a$  and  $b$  gives one for  $n$ .

For uniqueness of the factorization, suppose that  $n$  has two factorizations  $n = p_1 p_2 \cdots p_r$ , and  $n = q_1 q_2 \cdots q_s$  with the  $p_i$  and  $q_j$  in increasing order. By the previous theorem  $p_1 | q_j$  for some  $j$ . But since  $q_j$  is a positive irreducible,  $p_1 = q_j$ . Since the  $q_j$  are in increasing order,  $q_1 \leq p_1$ . Similarly one shows that  $p_1 \leq q_1$ . So, in fact  $p_1 = q_1$ . Thus we have  $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$ . This integer is smaller than  $n$  so is factor-able in a unique way. Thus  $r = s$  and  $p_i = q_i$ .  $\square$

We sometimes consolidate multiple factors of a given prime to write

$$n = u \prod_{i=1}^r p_i^{a_i}$$

with the  $a_i$  positive integers and  $p_i < p_{i+1}$ .

Another important concept from number theory is modular arithmetic. I will skip the definition of  $\mathbb{Z}/n$  and the justification for the arithmetic in  $\mathbb{Z}/n$ , which you can read elsewhere [7, §4.1]. The main result we need is:

**Theorem 1.1.8.** *Let  $p$  be a prime number. Then every nonzero element of  $\mathbb{Z}/p$  has a multiplicative inverse.*

PROOF: Let  $a$  be an integer whose congruence class is nonzero mod  $p$ . Then  $a$  is not divisible by  $p$ , so in fact it must be coprime to  $p$ . By Theorem 1.1.3 there exist  $r$  and  $s$  such that  $ar + ps = 1$ . This means that  $ar \equiv 1 \pmod{p}$ , as was to be shown.  $\square$

### Exercises 1.1.9.

1. Solve the linear equations.
  - (a)  $3x + 7 \equiv 5 \pmod{17}$
  - (b)  $3x + 7 \equiv 5 \pmod{15}$
  - (c)  $3x + 7 \equiv 4 \pmod{15}$
  
2. Use the quadratic formula, or completing the square, to find solution(s) if they exist to
  - (a)  $2x^2 + 7x + 5 \equiv 0 \pmod{17}$ .
  - (b)  $3x^2 + 16x + 4 \equiv 0 \pmod{17}$
  - (c)  $5x^2 + 7x + 14 \equiv 0 \pmod{19}$
  
3. Use Maple to find solutions if they exist to
  - (a)  $7x^4 + 3x^2 + x + 15 \equiv 0 \pmod{17}$ .
  - (b)  $7x^4 + 2x^2 + x + 15 \equiv 0 \pmod{19}$ .
  
4. Give an example of a quartic polynomial with three distinct roots modulo 17.

## 1.2 Commutative Rings and Ideals

The fundamental algebraic properties of the integers can be generalized to define a ring. Many of the notions of divisibility generalize as well. We give the formal definitions here and construct several examples.

**Definition 1.2.1.** A *ring* is a set  $R$  with two binary operations—addition,  $+$ , and multiplication,  $*$ —such that

- both operations are commutative,
- both operations are associative,
- both operations have an identity (0 for  $+$  and 1 for  $*$ ),
- there is an additive inverse for each element of  $R$ , and
- multiplication distributes over addition.

A *field* is a ring with the extra property that there is a multiplicative inverse for each nonzero element.

**Remark 1.2.2.** Strictly speaking, the definition above is for a commutative ring with identity. Since that is a mouthful, and we will only use commutative rings with identity, I opt for a four letter term. Some authors allow fields to have noncommutative multiplication. Others call such a structure a skew field or division ring. We always assume multiplication is commutative.

**Definition 1.2.3.** Let  $R$  be a ring. An element  $a \in R$  is called a *unit* if there is a multiplicative inverse for  $a$ . It is called a *zero-divisor* if it is nonzero itself and there is some nonzero  $b \in R$  such that  $a * b = 0$ .

Elements  $a, b \in R$  are called *associates* if there is a unit  $u \in R$  such that  $a = ub$ .

Here are some quick exercises:

1. The zero element, 0, is unique.
2. For any  $a \in R$ ,  $0 * a = 0$
3. The unity element, 1, is unique.
4. The inverse of an element (additive or multiplicative) is unique.
5. Every nonzero element of a field is a unit.
6. No element can be both a zero-divisor and a unit.

Of particular interest are rings with no zero-divisors.

**Definition 1.2.4.** A ring  $R$  is called an *integral domain* if it has no zero-divisors.

**Definition 1.2.5.** Let  $A$  and  $R$  be rings. A *homomorphism* from  $A$  to  $R$  is a function  $f$  that preserves the operations of  $A$  and  $R$ . That is,  $f(0_A) = 0_R$ ,  $f(1_A) = 1_R$ , and for  $a, b \in A$ ,  $f(a +_A b) = f(a) +_R f(b)$ , and  $f(a *_A b) = f(a) *_R f(b)$ .

An isomorphism is a homomorphism that is also a bijection of sets.

I used  $+_A$  and  $+_R$  to emphasize that the two operations take place in different rings. Normally we won't be so fussy since the context makes it clear. The more general ring theoretic approach does not require a homomorphism to satisfy  $f(1_A) = 1_R$ , but from a commutative algebra viewpoint it is natural to do so. The reader should verify that the inverse function of an isomorphism is a homomorphism, and therefore an isomorphism.

### Some Examples

The first ring that you should know about is the ring of integers,  $\mathbb{Z}$ . It is actually first in a very precise sense. There exists exactly one ring homomorphism from  $\mathbb{Z}$  to any other ring,  $R$ . It is defined by  $1_{\mathbb{Z}} \rightarrow 1_R$ . There is also a "last ring." It is the ring with just one element  $0 = 1$ . Check that it is a ring and that every ring has a unique map to the zero ring.

We will not develop the general theory of rings, but it is worth illustrating three standard methods to construct new rings from old:

1. form a ring of fractions by "adjoining inverses" of some elements,
2. form a "quotient ring" modulo some element (or elements)
3. form a "polynomial ring" in an indeterminate.

We will not use the first method again, but the other two will be very important. The following two examples illustrate the first two methods for the integers.

**Example 1.2.6.** If we adjoin to  $\mathbb{Z}$  the inverse of each nonzero integer we get the rational numbers:  $\mathbb{Q} = \{a/b : a \in \mathbb{Z}, b \in \mathbb{N}, (a, b) = 1\}$ . More formally, one defines an equivalence relation on the set of all fractions  $a/b$  with  $b$  nonzero:  $a/b$  is congruent to  $c/d$  whenever  $ad = bc$ . Then  $\mathbb{Q}$  is the set of equivalence classes.

There are numerous rings sandwiched between  $\mathbb{Z}$  and  $\mathbb{Q}$  that are very important in number theory. They are constructed by inverting only certain integers. Here are two examples. In the first we invert 2, in the second we invert all primes except 2.

Let  $2^{-1}\mathbb{Z}$  include the set of elements of  $\mathbb{Q}$  that can be expressed as  $a/b$  with  $b$  a power of 2. So  $2^{-1}\mathbb{Z} = \mathbb{Z} \cup \{a/2^i : a \text{ odd}, i \in \mathbb{N}\}$ . You should check that  $2^{-1}\mathbb{Z}$  is closed under addition and multiplication, and that it is a ring. This ring is called the localization of  $\mathbb{Z}$  away from 2.

Let  $P$  be the set of odd positive primes. Let  $P^{-1}\mathbb{Z}$  include the inverses of the odd primes, so  $P^{-1}\mathbb{Z} = \{a/b : a \in \mathbb{Z}, b \in \mathbb{N}, b \text{ odd}, \gcd(a, b) = 1\}$ . You should check that  $P^{-1}\mathbb{Z}$  is closed under addition and multiplication, and that it is a ring. This ring is called the localization of  $\mathbb{Z}$  at 2.

The localizations of  $\mathbb{Z}$  are all of the form  $P^{-1}\mathbb{Z}$  where  $P$  is a subset of the set of positive primes. The elements of  $P^{-1}\mathbb{Z}$  are uniquely represented in the form  $a/b$  with  $a \in \mathbb{Z}$ ,  $b$  divisible only by primes in  $P$ , and  $\gcd(a, b) = 1$ .

**Example 1.2.7.** You should already be familiar with the next standard family of examples, the integers modulo  $n$ , also called the quotient of  $\mathbb{Z}$  by  $n$ , which we will denote  $\mathbb{Z}/n$ .

Suppose that the greatest common divisor  $d$  of  $a$  and  $n$  satisfies  $1 < d < n$ . Let  $b = n/d$ . Then neither  $a$  nor  $b$  is congruent to  $0 \pmod n$ , but  $ab \equiv 0 \pmod n$ . So  $a$  and  $b$  are both zero divisors. On the other hand, if  $(a, n) = 1$  then there exist integers  $r$  and  $s$  such that  $ra + sn = 1$ . Since  $ra \equiv 1 \pmod n$ , we see that  $r$  is the multiplicative inverse of  $a$  in  $\mathbb{Z}/n$ . Thus we have shown that any nonzero element of  $\mathbb{Z}/n$  is either a unit or a zero divisor.

**Exercises 1.2.8.**

1. Prove the cancellation law for integral domains. If  $a, b, c$  are elements of an integral domain with  $a \neq 0$  and  $ab = ac$  then  $b = c$ .
2. Show that  $\mathbb{Z}/p$  is a field if and only if  $p$  is prime.
3. Show that the set of units in a ring forms a group under multiplication.

**Polynomial Rings**

We next want to introduce polynomial rings over a given ring  $R$ . This is actually a bit tricky. You can find an interesting discussion in [3, p.81]. We will give an informal definition and refer to [3, Appendix G] for one way to formally define polynomials. See also [4, pp. 248-]

**Definition 1.2.9.** Let  $R$  be a ring and let  $x$  be an indeterminate. For any  $n \in \mathbb{Z}$  and  $a_0, a_1, \dots, a_n \in R$  with  $a_n \neq 0$ , we will call an expression of the form  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  a *polynomial in  $x$  over  $R$* . The *leading term* is  $a_nx^n$ , the *leading coefficient* is  $a_n$  and the *degree* is  $n$ . The *coefficient of  $x^k$*  is  $a_k$ , for  $k \leq n$  and  $0$  for  $k > n$ . The polynomial is *monic* if the leading coefficient is  $1$ . The *polynomial ring in  $x$  over  $R$* , denoted  $R[x]$  is the set of all such polynomials (along with  $0$ ). We will sometimes write a general element as  $f(x) = \sum_i a_i x^i$  with the understanding that the sum is from  $0$  to  $\infty$  and that  $f_i = 0$  for all  $i > \deg f(x)$ . The element  $0 \in R[x]$  is then  $\sum_i 0x^i$ . It is convenient to define  $\deg 0 = -\infty$ . Addition in  $R[x]$  is defined componentwise and multiplication is defined by

$$f(x) * g(x) = \sum_k x^k \sum_{i=0}^k a_i b_{k-i}$$

where  $f(x) = \sum_i a_i x^i$  and  $g(x) = \sum_j b_j x^j$ .

The following proposition summarizes the basic results. Proofs are left to the reader or the references.

**Proposition 1.2.10.** *Let  $R$  be a ring.*

1.  $R[x]$  is a commutative ring with identity elements  $0$  for  $+$  and  $1x^0$  for  $*$ .
2. The polynomials of degree  $0$  form a subring isomorphic to  $R$ .

3.  $\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$  with equality if  $\deg f(x) \neq \deg g(x)$ .

Some funny things can happen when the ring  $R$  has zero divisors. For example in  $\mathbb{Z}/4[x]$ , the product of  $2x$  and  $2x$  is 0. We will avoid this nuisance by only using polynomial rings over an integral domain.

**Proposition 1.2.11.** *If  $R$  is an integral domain then so is  $R[x]$  and the degree of the product of two polynomials is the sum of the degrees,  $\deg(f(x) * g(x)) = \deg f(x) + \deg g(x)$ .*

We can now add to our store of examples. We have the polynomial ring  $\mathbb{Z}[x]$ . Letting  $y$  be another indeterminate we may form  $\mathbb{Z}[x][y]$ , which we usually write  $\mathbb{Z}[x, y]$ . Inductively, polynomial rings in several variables are constructed. We can also form polynomial rings over the rings constructed from  $\mathbb{Z}$  earlier,  $\mathbb{Z}/n[x]$ , and  $P^{-1}\mathbb{Z}[x]$ . We now give two more examples illustrating “adjoining inverses” and “forming quotients” from the ring  $\mathbb{Q}[x]$ .

**Example 1.2.12.** If we adjoin to  $\mathbb{Q}[x]$  the inverse of each nonzero polynomial, we get the field of rational polynomials, denoted  $\mathbb{Q}(x)$ . Formally one defines an equivalence relation on the set of all fractions  $a(x)/b(x)$  with  $b(x)$  nonzero:  $a(x)/b(x)$  is congruent to  $c(x)/d(x)$  whenever  $a(x)d(x) = b(x)c(x)$ . Then  $\mathbb{Q}(x)$  is the set of equivalence classes.

**Example 1.2.13.** In number theory you may have seen the Gaussian integers,  $\mathbb{Z}[i]$ , where  $i^2 = -1$ . The Gaussian numbers are formed by taking the quotient of  $\mathbb{Q}[x]$  by the polynomial  $x^2 + 1$ . The process for constructing  $\mathbb{Q}[i] = \mathbb{Q}[x]/(x^2 + 1)$  is entirely analogous to the formation of  $\mathbb{Z}/n$ , as we shall see in Section 1.3. The Gaussian integers form a subring of the Gaussian numbers.

## Ideals

**Definition 1.2.14.** An *ideal* of a ring  $R$  is a subset  $I \subset R$  which is closed under addition and closed under multiplication by an arbitrary element of  $R$ :

$$a + b \in I \quad \text{if } a, b \in I \quad (1.1)$$

$$ar \in I \quad \text{if } a \in I \text{ and } r \in R \quad (1.2)$$

You can prove this one.

**Proposition 1.2.15.** *If an ideal  $I$  of  $R$  contains a unit, then  $I = R$ .*

**Proposition 1.2.16.** *Let  $R$  be a ring. For an  $a_1, a_2, \dots, a_n \in R$ , the set  $I = \{r_1a_1 + r_2a_2 + \dots + r_na_n : r_i \in R\}$  is an ideal of  $R$ .*

PROOF: Clearly the sum of  $r_1a_1 + r_2a_2 + \dots + r_na_n$  and  $s_1a_1 + s_2a_2 + \dots + s_na_n$  is in  $I$  and the product of  $r$  with  $r_1a_1 + r_2a_2 + \dots + r_na_n$  is in  $I$ .  $\square$

The ideal  $I$  is *principal* if there exists some  $a \in I$  such that  $I = \{ar : r \in R\}$ . We say  $I$  is *generated by*  $a_1, a_2, \dots, a_s$  if  $I = \{r_1a_1 + r_2a_2 + \dots + r_sa_s : r_i \in R\}$ . We write  $I = \langle a_1, a_2, \dots, a_s \rangle$ .

**Example 1.2.17.** The principal ideals of  $\mathbb{Z}$  are multiples of a particular integer.

- (2) is the set of even numbers.
- (3) is the set of multiples of 3.
- (1) is all integers.
- (0) is the ideal containing only 0.

**Proposition 1.2.18.** *Every ideal in  $\mathbb{Z}$  is principal.*

PROOF: Let  $I$  be an ideal of  $\mathbb{Z}$ . If  $I = \{0\}$ , there is nothing to prove. Otherwise, let  $a$  be the smallest positive integer in  $I$ . Let  $b$  be any other nonzero element of  $I$ . Then by the properties of ideals, any linear combination of  $a$  and  $b$  is in  $I$ . Therefore  $\gcd(a, b) \in I$ . But the gcd of  $a$  and  $b$  is positive and less than or equal to  $a$ . Since  $a$  is the smallest positive element of  $I$ , we must have  $\gcd(a, b) = a$ . In other words an arbitrary element of  $I$  is divisible by  $a$ , so  $I = \langle a \rangle$  is principal.  $\square$

It should be clear that the principal ideals of  $\mathbb{Z}$  are in one correspondence with the nonnegative integers. One simply takes the least positive element of a nonzero ideal, or 0 for the zero ideal.

**Definition 1.2.19.** An ideal  $I$  in  $R$  is *prime* when  $ab \in I$  implies that either  $a \in I$  or  $b \in I$ . An ideal  $I$  is *maximal* if the only ideal properly containing  $I$  is  $R$ .

In any integral domain, the zero ideal is prime. This follows directly from the definition of integral domain,  $ab = 0$  implies  $a = 0$  or  $b = 0$ .

Let  $I$  be a nonzero ideal in the integers, and let  $d$  be its positive generator. If  $d$  is not prime, say  $d = ab$ , then  $I$  is not a prime ideal since  $ab \in I$ , but  $a, b \notin I$ . If  $d$  is prime then  $ab \in I$  implies that  $d|ab$ , and by primality of  $d$ , either  $d|a$  or  $d|b$ . Thus either  $a$  or  $b$  is in  $I$ , and  $I$  is prime. We conclude that for the integers an ideal is prime if and only if its generator is either 0 or a prime integer. Clearly the nonzero prime ideals are also maximal.

**Exercises 1.2.20.**

1. Identify all the ideals in  $2^{-1}\mathbb{Z}$ . Identify all the ideals in  $P^{-1}\mathbb{Z}$  for an arbitrary set of positive primes  $P$ . Which ideals are prime?
2. Suppose  $R, S$  are subrings of a ring  $T$ . Show that  $R \cap S$  is also a subring of  $T$ . Give an example to show that  $R \cup S$  may not be a ring.
3. Let  $R$  be a subring of a ring  $S$ . Let  $I$  be an ideal in  $S$ . Show that  $I \cap R$  is an ideal in  $R$ . Show that when  $I$  is prime so is  $I \cap R$ .
4. An element  $a$  in a ring  $R$  is *nilpotent* when  $a^t = 0$  for some positive integer  $t$ .
  - (a) Prove that the set of nilpotent elements in  $R$  forms an ideal in  $R$ . This ideal is called the *nilradical* of  $R$ .
  - (b) Find the nilradical of  $\mathbb{Z}/8$ , of  $\mathbb{Z}/12$ , and of  $\mathbb{Z}/30$ .
  - (c) Find the nilradical of  $\mathbb{Z}/n$  using the unique factorization of  $n$ .

5. An element  $e$  in a ring  $R$  is *idempotent* when  $e^2 = e$ .
- (a) If  $e$  is an idempotent in  $R$  prove that the principal ideal  $Re$  with the operations inherited from  $R$  has the structure of a ring, with identity  $e$ .
  - (b) Prove that  $(1 - e)$  is also an idempotent in  $R$ .
  - (c) Prove that every element in  $R$  may be uniquely expressed as the sum of an element in  $Re$  and an element in  $R(1 - e)$ .
  - (d) Find the idempotents in  $\mathbb{Z}/12$  and comment on the decomposition above.
  - (e) Find the idempotents in  $\mathbb{Z}/30$  and comment on the decomposition above.

### Divisibility, and Prime and Irreducible Elements in Integral Domains

The first step in analyzing many mathematical objects is to understand the elements that can't be broken down effectively. In this section we examine divisibility in this context. Some of the material here may be studied in general rings, but we gain simplicity by focusing on integral domains.

**Definition 1.2.21.** Let  $R$  be an integral domain and let  $r, s \in R$ . We say  $r$  divides  $s$  if there is some  $a \in R$  such that  $ra = s$ .

The units in  $R$  are those elements which divide 1. One can show, in the usual manner, that divides is transitive. If  $a$  and  $b$  are associates then each divides the other and any number divisible by  $a$  is also divisible by  $b$ .

**Definition 1.2.22.** A non-unit  $p \in R$  is called *irreducible* when any factorization is trivial in the sense that  $p = a * b$ , implies either  $a$  or  $b$  is a unit. A non-unit  $p \in R$  is *prime* when  $p$  divides  $ab$ , implies that either  $p$  divides  $a$  or  $p$  divides  $b$ .

There is a subtle difference between the two definitions. Note first of all that the usual definition of a prime integer corresponds to the definition for irreducible above, not the one for prime. Fortunately, as we showed in Section 1.1, the two notions coincide for the integers.

**Proposition 1.2.23.** *Suppose  $r$  and  $s$  are associates in a ring  $R$ . If  $r$  is either prime or irreducible then so is  $s$ .*

PROOF: Let  $r = us$  with  $u$  a unit. Suppose  $r$  is irreducible and that  $s = ab$ . Then  $r = uab$ . Since  $r$  is irreducible, one of  $ua$  or  $b$  must be a unit. If  $ua$  is a unit so is  $a$ . Thus one of  $a$  and  $b$  must be a unit. Therefore  $s$  is irreducible.

Suppose that  $r$  is prime and that  $s$  divides  $ab$ . Since  $r$  and  $s$  are associates,  $r$  also divides  $ab$ . But then  $r$  must divide one of  $a$  or  $b$ , say  $a$ . Since  $r$  and  $s$  are associates,  $s$  must divide  $a$  also. Thus  $s$  is prime.  $\square$

**Theorem 1.2.24.** *In any integral domain  $R$ , any prime element is irreducible.*

PROOF: Let  $p$  be a prime element of  $R$  and suppose that  $p = ab$ . We wish to show that either  $a$  or  $b$  is a unit. Since  $p$  is prime we know that  $p$  either divides  $a$  or  $b$ . Suppose

that it divides  $a$ , so  $a = pr$ . Then  $p = prb$ , so  $p(1 - rb) = 0$ . Since  $R$  is an integral domain,  $1 - rb = 0$ . This shows that  $b$  has an inverse, namely  $r$ .  $\square$

The converse is not always true! An example can be found in  $\mathbb{Z}[\sqrt{-5}]$  where  $1 + \sqrt{-5}$ ,  $2$ , and  $3$  are all irreducible but not prime, [7, p. 105]. Since  $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , we have  $2 \cdot 3 \in \langle 1 + \sqrt{-5} \rangle$  but it can be shown that  $2 \notin \langle 1 + \sqrt{-5} \rangle$ .

**Example 1.2.25.** The irreducible elements of  $\mathbb{Z}_2$  are the ordinary odd prime integers (and their associates). For example,  $3$  is irreducible, for if  $3 = (a/2^i) * (b/2^j)$  then  $3 = ab/2^{i+j}$ . But since  $a$  and  $b$  are odd (we may assume the original factors were in lowest terms) we must have  $i + j = 0$  and  $ab = 3$ . Consequently, one of  $a$  or  $b$  is  $\pm 1$ . But then one of  $a/2^i$  or  $b/2^j$  is a unit in  $\mathbb{Z}_2$ .

Since the only irreducibles of  $\mathbb{Z}_2$  are the primes of  $\mathbb{Z}$  not equal to  $2$  (and associates), we say that  $\mathbb{Z}_2$  is  $\mathbb{Z}$  localized away from  $2$ .

The only irreducible element of  $\mathbb{Z}_{(2)}$  is  $2$ . It is clear that the odd prime integers are not irreducible in  $\mathbb{Z}_{(2)}$  since they are in fact units! Since  $2$  is the only prime of  $\mathbb{Z}$  that remains prime in  $\mathbb{Z}_{(2)}$  we say that  $\mathbb{Z}_{(2)}$  is  $\mathbb{Z}$  localized at  $2$ .

### 1.3 Polynomials over a field

In Section 1.2, we discussed the basics of commutative rings. We defined what we mean by a field and we introduced polynomial rings. In this section we will show that the polynomial ring over a field  $F$  behaves very much like the integers. In particular, we establish unique factorization and show that  $F[x]/p(x)$  is a field when  $p(x)$  is irreducible.

**Lemma 1.3.1.** *Let  $a(x)$ , of degree  $r$ , and  $b(x)$ , of degree  $s$ , be two polynomials over a field  $F$ . Suppose  $r \geq s$ . Then*

$$\deg \left( a(x) - \frac{a_r}{b_s} x^{r-s} b(x) \right) < r$$

PROOF: Exercise.  $\square$

**Theorem 1.3.2 (Division).** *Given polynomials  $a(x), b(x) \in F[x]$  with  $b(x) \neq 0$  there exist unique polynomials  $q(x), r(x)$  such that*

1)  $a(x) = b(x)q(x) + r(x)$ , and

2)  $\deg r(x) < \deg b(x)$ .

PROOF: For existence, consider the set  $S = \{a(x) - b(x)k(x) : k(x) \in F[x]\}$ . Let  $r(x) = a(x) - b(x)q(x)$  be a monic polynomial of smallest degree in  $S$ . Then  $q(x)$  and  $r(x)$  satisfy item 1). Using the lemma above, one can show that if  $\deg r(x) \geq \deg b(x)$  a polynomial of lower degree than  $r(x)$  would be in  $S$ , contradicting the choice of  $r(x)$ . Thus item 2) is satisfied.

For uniqueness, suppose that  $a(x) = b(x)q(x) + r(x)$  with  $\deg r(x) < \deg b(x)$ . Suppose also that  $a(x) = b(x)q'(x) + r'(x)$  with  $\deg r'(x) < \deg b(x)$ . Taking the difference of the two equations,  $0 = b(x)(q(x) - q'(x)) + r(x) - r'(x)$ . Then  $r'(x) - r(x) = b(x)(q(x) - q'(x))$ . The degree of the left hand side is strictly less than  $\deg b(x)$ , but the right hand side has

degree at least  $\deg b(x)$  unless it is zero. Therefore both sides must be zero and we have  $q(x) = q'(x)$  and  $r(x) = r'(x)$ .  $\square$

We say a polynomial  $d(x)$  *divides*  $f(x)$  when the remainder of  $f(x)$  upon division by  $d(x)$  is 0. We write  $d(x)|f(x)$ . Divisibility satisfies the following properties.

**Proposition 1.3.3.** *Let  $a(x), b(x), c(x) \in F[x]$ .*

- *If  $a(x)|b(x)$  and  $a(x)|c(x)$  then  $a(x)|(r(x)b(x) + s(x)c(x))$  for any  $r(x), s(x) \in F[x]$ .*
- *If  $a(x)|b(x)$  and  $b(x)|c(x)$  then  $a(x)|c(x)$ .*

PROOF: Exercise.  $\square$

**Theorem 1.3.4.** *Let  $a(x), b(x) \in F[x]$  with not both equal to zero. The set  $I = \{r(x)a(x) + s(x)b(x) : r(x), s(x) \in F[x]\}$  has a unique monic polynomial of minimal degree. This polynomial is also the unique monic polynomial of maximal degree that divides both  $a(x)$  and  $b(x)$ .*

PROOF: Let  $n$  be the minimal degree of the nonzero polynomials in  $I$ . There is a monic polynomial of degree  $n$  in  $I$ , since we can multiply any polynomial in  $I$  by the inverse of its leading term to get a monic polynomial that is also in  $I$ . Suppose that there were two distinct monic polynomials  $f(x)$  and  $g(x) \in I$  of degree  $n$ . Then  $f(x) - g(x)$  is in  $I$ , and of degree less than  $n$ . This contradicts the definition of  $n$ . Thus there can only be one monic polynomial of minimal degree in  $I$ . Let it be  $d(x) = h(x)a(x) + k(x)b(x)$ .

By Proposition 1.3.3, any common divisor of  $a(x)$  and  $b(x)$  also divides any element of  $I$ , in particular  $d(x)$ . If we can show that  $d(x)$  divides both  $a(x)$  and  $b(x)$  then it must have maximal degree among all divisors of  $a(x)$  and  $b(x)$  as claimed. It must also be the unique common divisor of that degree since a monic polynomial can divide another monic polynomial of the same degree only if the two are equal.

From the Division Theorem, there are unique  $q(x)$  and  $r(x)$  such that

1.  $a(x) = d(x)q(x) + r(x)$ , and
2.  $\deg r(x) < \deg d(x)$ .

Substituting for  $d(x)$  we get

$$\begin{aligned} r(x) &= a(x) - d(x)q(x) \\ &= a(x) - [h(x)a(x) + k(x)b(x)]q(x) \\ &= [1 - q(x)h(x)]a(x) - (q(x)k(x))b(x) \end{aligned}$$

If  $r(x)$  were not 0, then we would have a contradiction to our choice of  $d(x)$  as the lowest degree element of  $I$ . Thus  $d(x)$  divides  $a(x)$ , and, by a similar argument,  $d(x)$  divides  $b(x)$ .  $\square$

The uniqueness in the proposition allows us to make the following definition of the greatest common divisor. It also says that the gcd of two polynomials can be written as a linear combination of the two. The subsequent theorem says that the Euclidean

algorithm can be extended to polynomials. In Section 1.6, there is a matrix version of the Euclidean algorithm which computes the linear combination that gives the gcd. It is very similar to a matrix version of the Berlekamp-Massey algorithm for decoding Reed-Solomon codes.

**Definition 1.3.5.** Let  $a(x)$  and  $b(x)$  be two polynomials over a field  $F$ , not both equal to 0. The *greatest common divisor* of  $a$  and  $b$ , denoted  $\gcd(a(x), b(x))$ , is the largest degree monic polynomial dividing both  $a(x)$  and  $b(x)$ . If the gcd is 1 we say  $a(x)$  and  $b(x)$  are *coprime*.

**Theorem 1.3.6.** *The Euclidean algorithm may be used to find the greatest common divisor of two polynomials, and to find the combination that gives the greatest common divisor.*

**Definition 1.3.7.** A positive polynomial  $p(x) \in \mathbb{F}[x]$  is *irreducible* if for any factorization  $p(x) = a(x)b(x)$  either  $a(x)$  or  $b(x)$  is an element of  $F$ . A polynomial  $p(x)$  is *prime* if whenever  $p(x)$  divides  $a(x)b(x)$ ,  $p(x)$  divides either  $a(x)$  or  $b(x)$ .

Theorem 1.2.24 showed that any prime element of an integral domain is irreducible. As with the integers, the converse is true in the polynomial ring over a field.

**Theorem 1.3.8.** *Let  $p(x) \in F[x]$  be irreducible. Then  $p(x)$  is prime.*

PROOF: Suppose  $p(x)$  is irreducible and  $p(x)|a(x)b(x)$ . Suppose that  $p(x) \nmid a(x)$ . Then  $\gcd(p(x), a(x)) = 1$ , so there are polynomials  $r(x)$  and  $s(x)$  such that  $p(x)r(x) + a(x)s(x) = 1$ . Multiplying by  $b(x)$  we have  $p(x)r(x)b(x) + a(x)s(x)b(x) = b(x)$ . Now  $p(x)$  divides the left hand side, so  $p(x)|b(x)$ .  $\square$

Now we have unique factorization!

**Theorem 1.3.9.** *Given any nonzero  $f(x) \in F[x]$  there exists an element  $\alpha \in F$ , a nonnegative integer  $r$ , and for each  $i = 1, \dots, r$ , distinct monic irreducibles  $p_i(x)$  and integers  $a_i > 0$  such that*

$$f(x) = \alpha \prod_{i=1}^r p_i(x)^{a_i}$$

*The element  $\alpha$  and the integer  $r$  are unique and the polynomials and their powers are unique, up to reordering.*

PROOF: For polynomials of degree 0—that is, nonzero elements of  $F$ —unique factorization is clear since the number of polynomials,  $r$ , must be zero (Proposition 1.2.11). Suppose that all polynomials of degree less than  $n$  have a unique factorization as described in the statement of the theorem. Suppose that  $f(x)$  has degree  $n$ . If  $f(x)$  is irreducible with leading coefficient  $a_n$  then  $a_n(f(x)/a_n)$  is a factorization as required. If  $f(x) = a(x)b(x)$  with both  $a(x)$  and  $b(x)$  having positive degree, then both  $a(x)$  and  $b(x)$  have degree less than  $n$  and so each has a factorization as a product of monic irreducibles. Then  $a(x)b(x)$  also has a factorization as a product of monic irreducibles.

For uniqueness of the factorization, Suppose that  $f(x)$  has two factorizations

$$\alpha p_1(x)^{a_1} p_2(x)^{a_2} \cdots p_r(x)^{a_r} = f(x) = \beta q_1(x)^{b_1} q_2(x)^{b_2} \cdots q_s(x)^{b_s}$$

By the previous theorem  $p_1(x)|q_k(x)$  for some  $k$ . By rearranging the  $q_j$  we may assume  $k = 1$ . Since  $q_1$  is monic and irreducible we must have  $p_1(x) = q_1(x)$ . By the cancellation law in an integral domain we have

$$\alpha p_1(x)^{a_1-1} p_2(x)^{a_2} \cdots p_r(x)^{a_r} = \beta q_1(x)^{b_1-1} q_2(x)^{b_2} \cdots q_s(x)^{b_s}$$

This polynomial product has degree less than  $n$  so it can be factored in a unique way. Thus  $r = s$  and after reordering  $p_i = q_i$  and  $a_i = b_i$ .  $\square$

**Corollary 1.3.10.** *If  $p_1(x), p_2(x), \dots, p_r(x)$  are distinct monic irreducible polynomials dividing  $f(x)$  then  $\prod_{i=1}^r p_i(x)$  divides  $f(x)$ .*

Since the product of two polynomials over  $F$  has degree equal to the sum of the degrees of the factors we get the following.

**Corollary 1.3.11.** *Let  $f(x)$  have the factorization in the Theorem. Then  $\deg f(x) = \sum_{i=1}^r a_i \deg p_i(x)$ .*

### Roots of Polynomials

Another consequence of unique factorization is that, as we prove below, a polynomial of degree  $d$  has at most  $d$  roots.

**Definition 1.3.12.** Let  $f(x) \in F[x]$  and let  $f(x) = \sum_{i=1}^n a_i x^i$  with  $a_i \in F$ . For  $\beta \in F$  we define  $f(x)$  *evaluated at  $\beta$* , written  $f(\beta)$ , to be  $\sum_{i=1}^n a_i \beta^i$ . This is an element of  $F$ . We say that  $\beta$  is a *root* of  $f(x)$  if  $f(\beta) = 0$ .

We leave it as an exercise to check that the evaluation of  $f(x)+g(x)$  at  $\beta$  is  $f(\beta)+g(\beta)$  and that the evaluation of  $f(x)g(x)$  at  $\beta$  is  $f(\beta)g(\beta)$ .

From the division theorem we see that finding a root of  $f(x)$  corresponds to finding a factor of  $f$ .

**Proposition 1.3.13.** *Let  $f(x) \in F[x]$  and let  $\beta \in F$ . Then  $\beta$  is a root of  $f(x)$  if and only if  $(x - \beta)$  is a factor of  $f(x)$ .*

PROOF: Using the division theorem the remainder when  $f(x)$  is divided by  $x - \beta$  has degree 0 and is therefore an element of  $F$ . Thus  $f(x) = q(x)(x - \beta) + r$  with  $r \in F$ . Evaluating at  $\beta$ ,  $f(\beta) = q(\beta)(\beta - \beta) + r = r$ . Thus  $\beta$  is a root of  $f(x)$  if and only if  $r = 0$ . That is,  $x - \beta$  divides  $f(x)$ .  $\square$

**Proposition 1.3.14.** *If  $\deg f(x) = d$  then  $f(x)$  has at most  $d$  distinct roots.*

PROOF: Each root gives a factor of  $f(x)$ , so  $n$  distinct roots give  $n$  distinct linear factors of  $f(x)$ . By unique factorization the product of these roots, which has degree  $n$ , divides  $f(x)$ . Thus  $n \leq d$ .  $\square$

**Example 1.3.15.** Suppose that  $F$  is the field  $\mathbb{Z}/p$ . Fermat's little theorem says that  $1, 2, 3, \dots, p-1$  are all roots of  $x^{p-1} - 1$ . Therefore the unique factorization of  $x^{p-1} - 1$  is  $(x-1)(x-2)\cdots(x-(p-1))$ .

## Congruence Modulo a Polynomial

We now extend the concept of modular arithmetic to polynomial rings. The first thing to do is to establish an equivalence relation on  $F[x]$  for each  $p(x) \in F[x]$ . Next one shows that arithmetic is well defined. I will just state the results. The proofs are exact analogues of those for integers.

**Definition 1.3.16.** Let  $p(x) \in F[x]$  with  $F$  a field. We say  $f(x), g(x)$  are *congruent modulo  $p(x)$* , written  $f(x) \equiv g(x) \pmod{p(x)}$ , if  $p(x)$  divides  $f(x) - g(x)$ .

We leave the following two important propositions as an exercise. The proofs follow with little change from the proofs for the analogous results for  $\mathbb{Z}/n$ .

**Proposition 1.3.17.** *Congruence modulo  $p(x)$  is an equivalence relation.*

**Proposition 1.3.18.** *If  $f(x) \equiv g(x) \pmod{p(x)}$  and  $a(x) \equiv b(x) \pmod{p(x)}$  then*

- $a(x) + f(x) \equiv b(x) + g(x) \pmod{p(x)}$ .
- $a(x)f(x) \equiv b(x)g(x) \pmod{p(x)}$ .

**Definition 1.3.19.** The two propositions show that there are two well defined operations on the set of equivalence classes of  $f[x]$  modulo  $p(x)$ , and it is easy to verify that the ring properties hold. We denote by  $F[x]/p(x)$  ring of polynomials modulo  $p(x)$ .

**Proposition 1.3.20.** *The set of polynomials of degree less than  $\deg p(x)$  form a complete system of residues modulo  $p(x)$ .*

PROOF: Let  $p(x)$  have degree  $d$ . If two unequal polynomials have degree less than  $d$  then their difference cannot be divisible by  $p(x)$ , so they are incongruent mod  $p(x)$ . Clearly, every polynomial is equivalent to its remainder when divided by  $p(x)$ , and the remainder has degree less than  $d$ . Thus each element in  $F[x]$  is equivalent to exactly one polynomial of degree less than  $d$ .  $\square$

From the proposition, a complete system of representatives for  $F[x]/p(x)$  is  $\{a_0 + a_1x + \cdots + a_{d-1}x^{d-1} : a_i \in F\}$  where  $\deg p(x)$ . The addition of these polynomials is done component-wise. Multiplication by an element of  $F$  is also component-wise. Consequently,  $F[x]/p(x)$  is a vector space of dimension  $d$  over  $F$ . Our next theorem concerns the multiplicative structure of  $F[x]/p(x)$  when  $p(x)$  is irreducible.

**Theorem 1.3.21.** *Let  $p(x)$  be an irreducible polynomial over a field  $F$ . Then  $F[x]/p(x)$  is a field.*

PROOF: Let  $a(x)$  be a polynomial whose congruence class is nonzero mod  $p(x)$ . Then  $a(x)$  is not divisible by  $p(x)$ , so in fact it must be coprime to  $p(x)$ . Then by Theorem 1.3.4 there exist  $r(x)$  and  $s(x)$  such that  $a(x)r(x) + p(x)s(x) = 1$ . This means that  $a(x)r(x) \equiv 1 \pmod{p(x)}$ . Consequently  $a(x)$  is a unit mod  $p(x)$ , and  $F[x]/p(x)$  is a field.  $\square$

**Definition 1.3.22.** A *subfield* of a field  $K$  is a subset  $F$  which contains  $0_K$  and  $1_K$  and is a field under the operations of  $K$ ,  $+_K$  and  $*_K$ . We also say that  $K$  is an *extension* of  $F$ .

If  $\alpha \in K$  we define  $F[\alpha]$  to be the smallest subfield of  $K$  containing  $F$  and  $\alpha$ . (It is the intersection of all subfields of  $K$  containing  $F$  and  $\alpha$ ).

For  $\alpha \in K$  consider all polynomials  $f(x) \in F[x]$  that have  $\alpha$  as a root. If this set is nonempty, we define the *minimal polynomial* of  $\alpha$  over  $F$  to be the monic polynomial  $M(x) \in F[x]$  of smallest degree such that  $M(\alpha) = 0$ .

The minimal polynomial is indeed unique, for if two monic polynomials have the same degree and both have  $\alpha$  as a root then their difference also has  $\alpha$  as a root and is of lower degree. Some multiple of this difference would be monic (and have  $\alpha$  as a root) contradicting the minimal degree of the minimal polynomial.

**Lemma 1.3.23.** *Let  $F$  be a subfield of a field  $K$ . Suppose  $\alpha \in K$  has minimal polynomial  $M(x)$  over  $F$ .*

1)  $M(x)$  is irreducible.

2) If  $\alpha$  is a root of  $f(x) \in F[x]$  then  $M(x)$  divides  $f(x)$ .

PROOF: Exercise. Use the division theorem for item 2). □

I won't prove this but I will prove a simpler version in the context of finite fields.

**Theorem 1.3.24.** *Let  $F$  be a subfield of  $K$ . Suppose that  $\alpha \in K$  has minimal polynomial  $M(x)$ . Then  $F[x]/M(x)$  is isomorphic to  $F[\alpha]$  under the map taking the conjugate class of  $x$  to  $\alpha$ .*

**Exercises 1.3.25.**

1. Find the greatest common divisor and express it as a combination of the given polynomials.
  - (a)  $a(x) = x^3 + 2x^2 + 2x + 1$  and  $b(x) = x^2 + 2x + 1$  over  $\mathbb{Z}/3$ .
  - (b)  $f(x) = x^2 + 2$  and  $g(x) = x^3 + x^2 + x + 2$  over  $\mathbb{Z}/3$ .
  - (c)  $f(x) = 4x^2 + 9x$  and  $g(x) = x^3 + 6x^2 + 6x + 2$  over  $\mathbb{Z}/11$
2. Write your own implementation of the Euclidean algorithm in Maple or Magma.
3. Prove Lemma 1.3.23.
4. Let  $f(x) \in F[x]$  with  $f(x) = x^n + \cdots + a_1x + a_0$ . Let  $\bar{x}$  be the equivalence class of  $x$  in  $F[x]/f(x)$ . Show that  $\bar{x}^n + \cdots + a_1\bar{x} + a_0$  is the 0 element of  $F[x]/f(x)$ .
5. What is  $\mathbb{R}[x]/(x^2 + 1)$ ? Can you find any other extensions of the reals?
6. Describe the arithmetic for  $\mathbb{Q}[x]/(x^2 + 1)$ . Construct other extensions of  $\mathbb{Q}$  of degree 2. Give an example of an extension of degree 3. Does  $x^3 + 1$  work?
7. Find an irreducible polynomial of degree 2, one of degree 3, and one of degree 4 over  $\mathbb{F}_2$ . For each, find a system of representatives for  $\mathbb{F}_2[x]/p(x)$ .
8. Find a polynomial of degree 4 over  $\mathbb{F}_2$  which has no roots but is not irreducible.

## 1.4 Finite Fields: Structure

The last section ended with the result that for a field  $F$  and irreducible polynomial  $p(x)$  over  $F$ ,  $F[x]/p(x)$  is a field. We will be working with polynomials over this new field, so it will be useful to have simpler notation. We will use a Greek letter, say  $\alpha$ , to denote the equivalence class of  $x$ . Notice that by an exercise in 1.3.25,  $\alpha$  may be considered a root of  $p(x)$ . The field will then be identified as  $F[\alpha]$  where  $p(\alpha) = 0$ . In coding, we are primarily interested in finite fields, for example  $\mathbb{Z}/p$ . The main result of this section is that for each prime power  $q = p^n$ , there is a unique field (up to isomorphism) with  $p^n$  elements. We denote this field  $\mathbb{F}_q$ . In particular, for a prime  $p$ , we use  $\mathbb{F}_p$  instead of  $\mathbb{Z}/p$ .

This section is devoted to proving the following theorem which we will do in stages.

**Theorem 1.4.1.** *Let  $F$  be a field with a finite number of elements.*

- 1)  $F$  has  $p^n$  elements where  $p$  is a prime.
- 2) There is an element  $\alpha \in F$  whose powers  $\alpha^1, \alpha^2, \dots, \alpha^{p^n-1} = 1$  give all the nonzero elements of  $F$ .
- 3)  $F$  is isomorphic to  $\mathbb{F}_p[x]/P(x)$  for some irreducible polynomial  $P(x)$  over  $\mathbb{F}_p$ .

For any prime  $p$  and any positive integer  $n$ ,

- 4) There exists a field with  $p^n$  elements.
- 5) Any two fields with  $p^n$  elements are isomorphic.

As a first step we prove

**Proposition 1.4.2.** *A finite field is a vector space over  $\mathbb{F}_p$  for some prime  $p$ . Consequently, the number of elements of  $F$  is a power of  $p$ .*

PROOF: Suppose that  $F$  is a finite field. Consider the additive subgroup generated by 1, i.e.  $1, 1+1, 1+1+1$ . Let  $m$  be the smallest positive integer such that the sum of  $m$  1's is 0. If  $m$  were composite,  $m = ab$ , then we would have

$$0 = \underbrace{1 + 1 + 1 + \cdots + 1 + 1}_{m \text{ terms}} = \underbrace{(1 + 1 + \cdots + 1)}_{a \text{ terms}} \underbrace{(1 + 1 + \cdots + 1)}_{b \text{ terms}}$$

The two factors on the right would then be zero-divisors, contradicting the assumption that  $F$  is a field. Thus  $m$  is in fact a prime, which we will now call  $p$ . We may think of  $F$  as containing a copy of  $\mathbb{F}_p$ . From the field axioms we see immediately that  $F$  is a vector space over  $\mathbb{F}_p$ . If its dimension over  $\mathbb{F}_p$  is  $n$  then  $F$  must have  $p^n$  elements. Thus any field has a prime power number of elements.  $\square$

**Definition 1.4.3.** The prime  $p$  in the theorem is called the *characteristic* of the field.

Suppose that  $q = p^n$  is the number of elements in  $F$ . By the field axioms, the set of nonzero elements of  $F$  is a group under multiplication. This group is denoted  $\mathbb{F}^*$ . Recall that the *order* of an element  $\alpha$  in a group  $G$  is the smallest positive integer  $r$  such that  $\alpha^r$  is the identity, or infinity, if no such  $r$  exists. As an exercise, review the following properties:

**Lemma 1.4.4.** Let  $\alpha$  be an element of order  $r$  in a group  $G$ .

- 1)  $\alpha^i = \alpha^j$  iff  $i \equiv j \pmod{r}$ .
- 2) The order of  $\alpha^i$  is  $r/d$  where  $d = \gcd(i, r)$ .
- 3) Let  $\beta \in G$  have order  $s$ , coprime to  $r$ . Then  $\text{ord}(\alpha\beta) = rs$ .

Now we can establish item 2) of the Theorem.

**Proposition 1.4.5.** The multiplicative group of a finite field is cyclic.

PROOF: Let  $F$  have  $p^n$  elements and let the prime factorization of  $p^n - 1$  be  $\prod_{i=1}^r q_i^{a_i}$ . We will show that for each  $i = 1 \dots, r$  there is an element  $b_i \in \mathbb{F}^*$  of order  $q_i^{a_i}$ . By Lemma 1.4.4, the order of  $b = \prod_{i=1}^r b_i$  is  $\prod_{i=1}^r q_i^{a_i} = p^n - 1$ . Thus  $b$  generates the multiplicative group of  $F$ .

Let  $q^a \mid (p^n - 1)$  and let  $t = (p^n - 1)/q^a$  and consider the set  $S = \{\alpha^t : \alpha \in \mathbb{F}^*\}$ . For any  $\beta \in S$  the polynomial  $x^t - \beta$  has at most  $t$  roots so there can be at most  $t$  elements of  $F$  whose  $t$ th power is  $\beta$ . Therefore the cardinality of  $S$  is at least  $(p^n - 1)/t = q^a$ . On the other hand, everything in  $S$  is a root of  $x^{q^a} - 1$  since

$$(\alpha^t)^{q^a} = \alpha^{p^n - 1} = 1$$

There can be only  $q^a$  roots of  $x^{q^a} - 1$ , so  $S$  has at most  $q^a$  elements. This shows  $|S| = q^a$ . Similarly, at most  $q^{a-1}$  of the elements in  $S$  can be roots of  $x^{q^{a-1}} - 1$  so there must be at least  $q^a - q^{a-1}$  elements of  $S$  whose order in  $F$  is  $q^a$ . This was what we wanted to show. □

**Definition 1.4.6.** An element of a finite field whose powers generate the nonzero elements of the field is called *primitive*.

The theorem says that every finite field has a primitive element. Furthermore, from the lemma, if  $\alpha$  is primitive in a field of  $p^n$  elements then  $\alpha^k$  is also primitive whenever  $k$  is coprime to  $p^n - 1$ . Thus there are  $\phi(p^n - 1)$  primitive elements, where  $\phi$  is the Euler totient function ( $\phi(n)$  is the number of positive integers less than  $n$  and coprime to  $n$ ).

**Corollary 1.4.7.** If  $F$  is a field with  $p^n$  elements then

$$x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha) \quad \text{and,}$$

$$x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}^*} (x - \alpha)$$

According to the following definition, the corollary shows that a field  $F$  of order  $p^n$  is a splitting field for  $x^{p^n - 1} - 1$  and for  $x^{p^n} - x$  over  $\mathbb{F}_p$ .

**Definition 1.4.8.** Let  $F$  be a field and let  $f(x) \in F[x]$ . A *splitting field* for  $f(x)$  is a field  $K$  containing  $F$  such that

- $f(x)$  factors into linear factors in  $K[x]$ .

- Every element of  $K$  can be written as a polynomial in the roots of  $f(x)$ .

To prove item 3) of the Theorem we need to use the minimal polynomial of a primitive element (see Definition 1.3.22).

**Proposition 1.4.9.** *Let  $F$  be a finite field of  $p^n$  elements. Let  $\beta$  be any primitive element of  $F$  and let  $M(x)$  be its minimal polynomial over  $\mathbb{F}_p$ . Then  $F$  is isomorphic to  $\mathbb{F}_p[x]/M(x)$ . In particular  $\deg M(x) = n$ .*

PROOF: Let  $M(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0$  with  $a_i \in \mathbb{F}_p$ . We will show that  $1, \beta, \dots, \beta^{r-1}$  is a basis for  $F$  over  $\mathbb{F}_p$ . We first observe that  $1, \beta, \dots, \beta^{r-1}$  must be linearly independent over  $\mathbb{F}_p$ . Suppose on the contrary that some nontrivial linear combination is 0,  $b_{r-1}\beta^{r-1} + \cdots + b_1\beta + b_0 = 0$ . Let  $k$  be the largest positive integer such that  $b_k \neq 0$ . Then

$$\beta^k + \frac{b_{k-1}}{b_k} \cdots + \frac{b_1}{b_k} \beta + \frac{b_0}{b_k} = 0$$

This shows that  $\beta$  is a root of a polynomial over  $\mathbb{F}_p$  of degree less than  $\deg M(x)$ , contradicting the minimality of  $M(x)$ .

Next we show that any power of  $\beta$  can be written as a linear combination of  $1, \beta, \beta^2, \dots, \beta^{r-1}$ . This is true trivially for  $\beta^i$  for  $i = 0, \dots, r-1$ . Assume that for some  $k \geq r$ , each  $\beta^i$  for  $i < k$  can be written as a linear combination as stated. Since  $M(\beta) = 0$ ,  $\beta^r = -a_{r-1}\beta^{r-1} - \cdots - a_1\beta - a_0$ . Multiplying by  $\beta^{k-r}$  we can write  $\beta^k$  as a linear combination of lower powers of  $\beta$ . By the induction hypothesis these are all linear combinations of  $1, \beta, \dots, \beta^{r-1}$ , so  $\beta^k$  is also. Since every nonzero element of  $F$  is a power of  $\beta$ , we have shown that  $1, \beta, \dots, \beta^{r-1}$  span  $F$  as claimed.

Since  $F$  has  $p^n$  elements  $r = n$ . Furthermore the arithmetic on  $F$  is completely determined by its structure as a vector space and  $\beta^n = -a_{n-1}\beta^{n-1} - \cdots - a_1\beta - a_0$ . This is exactly the same structure that  $\mathbb{F}_p[x]/M(x)$  has. In other words the map from  $\mathbb{F}_p[x]/M(x)$  to  $F$  taking the class of  $x$  to  $\beta$  is an isomorphism.  $\square$

We can now prove existence and uniqueness for fields of prime power order. We will need the ‘‘Freshman’s dream’’:

**Proposition 1.4.10.** *Let  $\alpha, \beta$  be elements of a field of characteristic  $p$ . Then  $(\alpha + \beta)^p = \alpha^p + \beta^p$ .*

PROOF: Expand  $(\alpha + \beta)^p$  using the binomial theorem and we get terms like

$$\binom{p}{k} \alpha^k \beta^{p-k}$$

The binomial coefficient really means 1 added to itself  $\binom{p}{k}$  times. Since  $p$  divides the binomial coefficient when  $1 < k < p$  the coefficient is 0 unless  $k = 0$  or  $k = p$ . That gives the result.  $\square$

**Proposition 1.4.11.** *For any prime power there exists a unique field of that order.*

PROOF: Uniqueness: Let  $F$  and  $F'$  be two fields with  $p^n$  elements. Let  $\alpha$  be a primitive element in  $F$  and let  $M(x)$  be its minimal polynomial over  $\mathbb{F}_p$ . Since  $\alpha$  is a root of

$x^{p^n} - x$ , Lemma 1.3.23 says that  $M(x)$  divides  $x^{p^n} - x$ . By Corollary 1.4.7,  $x^{p^n} - x$  factors into distinct linear factors in both  $F$  and  $F'$  so there must be a root of  $M(x)$  in  $F'$ . By Proposition 1.4.9, both  $F$  and  $F'$  are isomorphic to  $\mathbb{F}_p[x]/M(x)$  so they are isomorphic to each other.

Existence: By successively factoring  $x^{p^n} - x$  and adjoining roots of a nonlinear irreducible factor, we can, after a finite number of steps, arrive at a field in which  $x^{p^n} - x$  factors completely. I claim that the roots of  $x^{p^n} - x$  form a field, which by Proposition 1.3.14 must have  $p^n$  elements.

We need to show that the sum of two roots is a root, that the additive inverse of a root is a root, that the product of two roots is a root and that the multiplicative inverse of a root is a root. These are all trivial except for the case of the sum of two roots, which can be proved using the “Freshman’s dream.”  $\square$

The following example shows that there are many ways to construct a given field.

**Example 1.4.12.** Let  $p = 3$ . We can construct the field  $\mathbb{F}_{3^2}$  by adjoining to  $\mathbb{F}_3$  a root  $\alpha$  of the irreducible polynomial  $x^2 + 2x + 2$ . You can check by hand that  $\alpha$  is primitive in this field. If we had used  $x^2 + 1$ , which is also irreducible, we would still get a field with 9 elements. But the root of  $x^2 + 1$  will only have order 4 since  $\alpha^{-1} = -1$  implies  $\alpha^4 = 1$ .

**Definition 1.4.13.** Let  $F$  be a finite field and let  $p(x)$  be a polynomial over  $F$ . If  $p(x)$  is irreducible and the class of  $x$  is primitive in  $F[x]/p(x)$ , then we say  $p(x)$  is a *primitive polynomial*.

**Example 1.4.14.** We can construct  $\mathbb{F}_{3^6}$  by adjoining to the field of the previous example a root  $\beta$  of the primitive polynomial (verified using Magma)  $x^3 + \alpha x^2 + \alpha x + \alpha^3$  over  $\mathbb{F}_{3^2}$ . Elements of  $\mathbb{F}_{3^6}$  are uniquely represented as polynomials in  $\alpha$  and  $\beta$  whose degree in  $\alpha$  is at most 1, and whose degree in  $\beta$  is at most 2.

We could also construct  $\mathbb{F}_{3^6}$  by first constructing  $\mathbb{F}_{3^3}$  by adjoining a root  $\alpha'$  of the primitive polynomial  $x^3 + 2x + 1$  and then adjoining a root  $\beta'$  of the primitive polynomial (verified using Magma)  $x^2 + x + (\alpha')^7$  over  $\mathbb{F}_{3^3}$ .

Finally we could construct  $\mathbb{F}_{3^6}$  directly by adjoining a root of the primitive polynomial  $x^6 + 2x^4 + x^2 + 2x + 2$ .

In each of these fields you can find a root of any one of the polynomials, and thereby define isomorphisms between the fields.

#### Exercises 1.4.15.

1. Construct  $\mathbb{F}_{2^6}$  in three ways:
  - a) by constructing  $\mathbb{F}_4$  using an irreducible polynomial of degree 2 over  $\mathbb{F}_2$  and then by constructing  $\mathbb{F}_{64}$  using an irreducible polynomial of degree 3 over  $\mathbb{F}_4$ .
  - b) by constructing  $\mathbb{F}_8$  using an irreducible polynomial of degree 3 over  $\mathbb{F}_2$  and then by constructing  $\mathbb{F}_{64}$  using an irreducible polynomial of degree 2 over  $\mathbb{F}_8$ .
  - c) by using an irreducible polynomial of degree 6 over  $\mathbb{F}_2$ .
 Give isomorphisms between the three representations.
2. Construct  $\mathbb{F}_{81}$  in two ways. You may notice that  $x^2 + 2x + 1$  and  $x^2 + x + 2$  are both irreducible over  $\mathbb{F}_3$ . Can you construct  $\mathbb{F}_{81}$  by using one of these polynomials and then the other?

3. Factor  $x^{80} - 1$  over  $\mathbb{F}_3$  and explain the relationship between the factors and the elements of  $\mathbb{F}_{81}$ . Factor  $x^{80} - 1$  over  $\mathbb{F}_9$  and explain the relationship between the factors and the elements of  $\mathbb{F}_{81}$ .
4. Factor  $x^{15} - 1$  over  $\mathbb{F}_2$ . Construct  $\mathbb{F}_{16}$  in three ways as a degree 4 extension of  $\mathbb{F}_2$  and show isomorphisms between the three representations.
5. Make a table showing the possible orders and the number of elements of each order for  $\mathbb{F}_{64}$ ,  $\mathbb{F}_{128}$ , and  $\mathbb{F}_{256}$ .
6. Prove that if  $r|n$  then  $\mathbb{F}_{q^r}$  is a subfield of  $\mathbb{F}_{q^n}$ .
7. Let  $n = 6$ . Find all irreducible polynomials over  $\mathbb{F}_2$  of deg  $d$  where  $d|n$ . Find the product of these polynomials.
8. For a given prime  $p$ , let  $I(d)$  be the set of irreducible polynomials of degree  $d$  over  $\mathbb{F}_p$ . Show that for  $n > 0$ ,

$$\prod_{d|n} \prod_{f \in I(d)} f = x^n - 1$$

9. Show that for any  $\alpha \in \mathbb{F}_q$ ,

$$1 + \alpha + \alpha^2 + \alpha^3 + \dots + \alpha^{q-2} = \begin{cases} 1 & \text{if } \alpha = 0 \\ -1 & \text{if } \alpha = 1 \\ 0 & \text{otherwise} \end{cases}$$

## 1.5 The Frobenius Map

**Definition 1.5.1.** The *Frobenius map* on  $\mathbb{F}_{p^n}$  is the map  $\phi : \alpha \rightarrow \alpha^p$ .

**Theorem 1.5.2.** *The Frobenius map satisfies the following*

- 1) *It is an automorphism of  $\mathbb{F}_{p^n}$ .*
- 2) *The set of elements which are fixed by the Frobenius map is exactly  $\mathbb{F}_p$ .*
- 3) *If  $\alpha \in \mathbb{F}_{p^n}$  has minimal polynomial  $M(x)$  over  $\mathbb{F}_p$  then  $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$  are the roots of  $M(x)$  where  $d = \deg M(x)$ .*
- 4) *For  $d|n$  the set of elements fixed by  $\phi^d$  is  $\mathbb{F}_{p^d}$ .*

**Corollary 1.5.3.** *For any  $\alpha \in \mathbb{F}_{p^n}$ ,  $\sum_{i=0}^{n-1} \phi^i(\alpha)$  and  $\prod_{i=0}^{n-1} \phi^i(\alpha)$  are elements of  $\mathbb{F}_p$*

**Definition 1.5.4.** The *trace map* from  $\mathbb{F}_{p^n}$  to  $\mathbb{F}_p$  is  $\text{Tr}(\alpha) = \sum_{i=0}^{n-1} \phi^i(\alpha)$  The *norm map* from  $\mathbb{F}_{p^n}$  to  $\mathbb{F}_p$  is

$$N(\alpha) = \prod_{i=0}^{n-1} \phi^i(\alpha)$$

## 1.6 The Euclidean Algorithm

Let  $a, b$  be integers with  $b > 0$ . The following algorithm computes the greatest common divisor of  $a$  and  $b$ .

**Input:** Nonzero integers  $a, b$ .

**Output:** The (positive) greatest common divisor of  $a$  and  $b$ .

**Algorithm:** Define inductively  $r_i$  for  $i \geq 0$  and  $q_i$  for  $i \geq 1$ :

$$\begin{aligned} r_0 &= a \\ r_1 &= b \end{aligned}$$

While  $r_i \neq 0$ , let  $r_{i+1}, q_i$  be the remainder and quotient when  $r_{i-1}$  is divided by  $r_i$ ,

$$\begin{aligned} r_{i+1} &= q_i r_i - r_{i-1} \\ 0 &\leq r_{i+1} < r_i \end{aligned}$$

Output  $r_{i-1}$  when  $r_i = 0$ .

**Theorem 1.6.1.** *The algorithm above terminates after a finite number of steps. If  $n$  is the smallest integer such that  $r_{n+1} = 0$  then  $r_n$  is the greatest common divisor of  $a$  and  $b$ .*

*The number of steps  $n$  is at most  $1 + \log b / (\log(1 + \sqrt{5}) - 1)$ , where  $\log$  is base 2.*

PROOF: See Rosen [7]. □

We now consider a matrix version of the Euclidean algorithm that produces the linear combination of  $a$  and  $b$  that gives the gcd.

**Input:** Nonzero integers  $a, b$ .

**Output:** Integers  $d, r, s$ , such that  $d = \gcd(a, b)$  and  $d = ra + bs$ .

**Algorithm:** Define inductively 2-vectors,  $R^{(i)}$ , and  $2 \times 2$  matrices  $T^{(i)}$  for  $i \geq 0$ :

$$\begin{aligned} R^{(0)} &= \begin{bmatrix} b \\ a \end{bmatrix} \\ T^{(0)} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

While  $r_i \neq 0$ , define  $q_i = \lfloor R_2^{(i-1)} / R_1^{(i-1)} \rfloor$

$$\begin{aligned} Q^{(i)} &= \begin{bmatrix} -q_i & 1 \\ 1 & 0 \end{bmatrix} \\ R^{(i)} &= Q^{(i)} R^{(i-1)} \\ T^{(i)} &= Q^{(i)} T^{(i-1)} \end{aligned}$$

**Theorem 1.6.2.** *The matrix  $R^{(i)}$  keeps track of the usual remainders.*

$$R^{(i)} = \begin{bmatrix} r_{i+1} \\ r_i \end{bmatrix}$$

*The matrix  $T^{(k)}$  is the product of the  $Q^{(i)}$ ,*

$$T^{(k)} = \prod_{i=1}^k Q^{(i)}$$

*If the algorithm terminates after  $n$  steps then*

$$\begin{bmatrix} r_{n+1} \\ r_n \end{bmatrix} = T^{(n)} \begin{bmatrix} b \\ a \end{bmatrix}$$

*so the bottom row of  $T^{(n)}$  gives a linear combination of  $a$  and  $b$  that produces the gcd,  $r_n$ .*

**Exercises 1.6.3.**

1. Write a procedure implementing the matrix version of the Euclidean algorithm. Do it first for integers, then for polynomials over  $\mathbb{Q}$ , then generalize to polynomials over finite fields.

# Bibliography

- [1] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, 1983.
- [2] R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 2003.
- [3] T. W. Hungerford, *Abstract Algebra: An Introduction*, 2nd ed., Saunders Harcourt Publishing, 1997.
- [4] J. A. Gallian, *Contemporary Abstract Algebra* 3rd ed., D. C. Heath and Co., 1994.
- [5] S. Lang, *Algebra* 2nd ed., Addison-Wesley, 1984.
- [6] S. Lin, D. J. Costello *Error Control Coding, 2nd Ed.*, Prentice Hall, 2004.
- [7] K. Rosen, *Elementary Number Theory and Its Applications* 4th ed. Addison Wesley Longman, 2000.