

# Chapter 1

## Abstract Algebra

In these notes we will give an informal account of some necessary background in abstract algebra; in particular, we will address unique factorization domains and the construction of finite fields.

### 1.1 Unique Factorization Domains

Let us briefly recapitulate some basic results from algebra. A ring (for us, a ring is always commutative and has a unit element 1) is called a domain if it has no zero divisors, that is, if  $ab = 0$  for  $a, b \in R$  implies that  $a = 0$  or  $b = 0$ . For example,  $\mathbb{Z}/6\mathbb{Z}$  is not an integral domain because  $2 \cdot 3 = 0$ , but  $2 \neq 0$  and  $3 \neq 0$  in this ring. Domains  $R$  have the cancellation property: if  $ab = ac$  for  $a, b, c \in R \setminus \{0\}$ , then  $b = c$ ; this can be proved by constructing the field of quotients and then multiplying through by  $a^{-1}$ . Rings with zero divisors do not have the cancellation property: for example,  $3 \cdot 2 = 3 \cdot 4 = 0$ , but  $2 \neq 4$  in  $\mathbb{Z}/6\mathbb{Z}$ .

Now let  $R$  be a domain. We say that  $b \mid a$  for elements  $a, b \in R$  if there is a  $c \in R$  such that  $a = bc$ . Elements dividing 1 are called units and form a group  $R^\times$ , the unit group of  $R$ . A simple observation is that if  $a \mid b$  and  $b \mid a$ , then  $a = bu$  for some unit  $u$ : in fact,  $a \mid b$  implies  $b = ac$  for some  $c \in R$ , and  $b \mid a$  shows  $a = bd$  for some  $d \in R$ . Thus  $a = bd = acd$

An element  $p \in R \setminus R^\times$  is called

- irreducible if every factorization  $p = ab$  in  $R$  is trivial, that is, if  $p = ab$  implies that  $a$  or  $b$  is a unit;
- prime if it has the property that, whenever  $p \mid ab$  divides a product, it divides one of the factors:  $p \mid a$  or  $p \mid b$ .

It is easy to see that primes are always irreducible: in fact, if a prime  $p$  has the factorization  $p = ab$ , then  $p \mid ab$ ; since  $p$  is prime, it divides one of the factors, say  $a$ ; but then we have  $p \mid a$ , i.e.  $a = pc$  for some  $c \in R$ . Thus  $a = pc = abc$ , and from the cancellation law we conclude that  $bc = 1$ , hence  $b$  is a unit and any factorization of  $p$  is trivial.

The converse, namely that irreducibles are prime, is not true in general, but it holds for unique factorization domains (UFDs). These are domains in which every nonunit has a factorization into primes that is unique up to units and the order of the factors.

It is known that any Euclidean ring is a UFD; a Euclidean ring is a ring with a Euclidean algorithm, that is, a function  $f : R \rightarrow \mathbb{N}$  with the property that

- $f(a) = 0$  if and only if  $a = 0$ ;
- for any pair  $a, b \in R \setminus \{0\}$ , there is a  $q \in R$  such that  $f(a - bq) < f(b)$ .

The standard examples of Euclidean rings are  $\mathbb{Z}$ , where  $f$  can be taken to be the absolute value (although there exist other possible choices as well), and the polynomial ring  $K[X]$  in one variable over a field  $K$ , where  $f$  is the function  $f(r) = 2^{\deg r}$  for polynomials  $r \in K[X]$ .

From what we have seen above, any irreducible element in  $K[X]$  is prime; for example,  $X - 4$  and  $X^2 + 1$  are primes in  $\mathbb{Q}(X)$  (what about  $\mathbb{C}[X]$ ?).

The reason we have inserted this section on UFDs is that we will need the following result below:

**Proposition 1.1.1.** *Let  $R$  be a UFD. If  $a, b, m$  are nonzero elements of  $R$  such that  $a \mid m$  and  $b \mid m$ , and if  $\gcd(a, b) = 1$ , then  $ab \mid m$ .*

*Proof.* Just look at the prime factorizations: we know  $m = ac$  for some  $c$ , and that  $b \mid m = ac$ . Since the prime factors of  $b$  do not occur in the prime factorization of  $a$ , they must all occur in the prime factorization of  $c$ , which implies  $b \mid c$  and therefore  $m = abd$ , that is,  $ab \mid m$ .  $\square$

For Euclidean domains  $R$  there is a simpler proof using only the fact that if  $\gcd(a, b) = d$ , then there are  $r, s \in R$  with  $d = ar + bs$  (Bezout's Lemma). Now assume that  $m = ac = bd$ , and write  $ar + bs = 1$  ( $a$  and  $b$  are coprime). Then  $bd = mr = arc = (1 - bs)c = c - bsc$ , which immediately implies that  $b \mid c$ , and we are done.

## 1.2 Finite Fields

The simplest finite fields are the residue class rings  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  for primes  $p$ . Its elements can be represented by  $\{0, 1, \dots, p-1\}$ , and the field operations are addition and multiplication modulo  $p$ .

Are there any other fields?

### 1.2.1 Some Abstract Algebra

Assume that  $\mathbb{F}_q$  is a finite field with  $q$  elements. The order of an element divides the order of a group; applying this to the additive group  $(\mathbb{F}_q, +)$  with  $q$  elements we find that  $q \cdot 1 = 1 + \dots + 1 = 0$ . This allows us to define the characteristic of a finite field as the smallest integer  $m > 0$  such that  $m \cdot 1 = 0$ .

We claim that the characteristic  $p$  of a finite field is prime. In fact, assume that  $p = ab$  for integers  $a, b > 1$ . Then  $0 = ab$  implies that  $a = 0$  or  $b = 0$  since fields do not have zero divisors.

Now let  $\mathbb{F}_q$  be a finite field with characteristic  $p$ . We claim that  $\mathbb{F}_q$  contains  $\mathbb{F}_p$  as a subfield. In fact, consider the smallest subfield  $F$  of  $\mathbb{F}_q$  containing 1. This field clearly contains  $0, 1, 1 + 1, \dots, (p - 1) \cdot 1$ . Since these elements form a field, we have  $\mathbb{F}_p \subseteq \mathbb{F}_q$ .

Next we claim that if  $\mathbb{F}_q$  is a field with characteristic  $p$ , then  $q = p^n$  is a power of  $p$ . This follows from the following observation:

**Lemma 1.2.1.** *Assume that  $K \subseteq L$  are fields. Then  $L$  is a  $K$ -vector space.*

*Proof.* This is trivial: we have to check that  $L$  is an additive group, and that we can multiply the 'vectors' in  $L$  by 'scalars' in  $K$ , which we obviously can, and of course all the axioms are satisfied.  $\square$

Thus  $\mathbb{F}_q$  is an  $\mathbb{F}_p$ -vector space. Let  $x_1, \dots, x_n$  denote a basis of  $\mathbb{F}_q$  over  $\mathbb{F}_p$ . Then every element in  $\mathbb{F}_q$  can be written uniquely as a linear combination of the  $x_j$  with coefficients from  $\mathbb{F}_p$ . This implies that  $\#\mathbb{F}_q = p^n$ :

**Proposition 1.2.2.** *If  $\mathbb{F}_q$  is a finite field with characteristic  $p$ , then  $q = p^n$  for some  $n \geq 1$ .*

Now let us show that there is a field  $\mathbb{F}_4$  with four elements. Since every field contains 0 and 1, let us write  $\mathbb{F}_4 = \{0, 1, x, y\}$  and see whether we can define addition and multiplication in such a way that  $\mathbb{F}_4$  becomes a field. Clearly  $\mathbb{F}_4$  has characteristic 2, hence  $1 + 1 = x + x = y + y = 0$ .

Now we claim that  $x + 1 = y$ . In fact, we cannot have  $x + 1 = 0$ ,  $x + 1 = 1$  or  $x + 1 = x$  since this would imply  $x = 1$ ,  $x = 0$  or  $x = y$ , respectively. We also observe that  $y + 1 = x + 1 + 1 = x$ . This takes care of addition.

Now  $x^2 \neq 0$  and  $x^2 \neq x$  since this would imply  $x = 0$  or  $x = 1$ . If  $x^2 = 1$ , then  $x(x + 1) = x^2 + x = x + 1$ , hence  $x = 1$ : contradiction. Thus we must have  $x^2 = y$ . This shows that  $xy = x(x + 1) = x^2 + x = x + y = 1$  and  $y^2 = (x + 1)^2 = x^2 + 1 = y + 1 = x$ .

Thus if  $\mathbb{F}_4$  can be made into a field, then addition and multiplication tables must look like this:

$$\begin{array}{c|cccc} + & 0 & 1 & x & y \\ \hline 0 & 0 & 1 & x & y \\ 1 & 1 & 0 & y & x \\ x & x & y & 0 & 1 \\ y & y & x & 1 & 0 \end{array} \quad \begin{array}{c|cccc} \cdot & 0 & 1 & x & y \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & x & y \\ x & 0 & x & y & 1 \\ y & 0 & y & 1 & x \end{array}$$

It remains to check associativity and distributivity.

Of course we don't want to construct fields like this; we need something better (and something more abstract).

The following construction provides us with fields  $\mathbb{F}_q$  ( $q = p^2$ ):

**Proposition 1.2.3.** *Let  $F$  be a field, and let  $m \in F^\times \setminus \mathbb{F}^{\times 2}$  be a nonsquare. Then  $K = F(\sqrt{m}) = \{a+b\sqrt{m} : a, b \in F\}$  is a field, containing  $F = \{a+0\sqrt{m} : a \in F\}$  as a subfield. If  $F = \mathbb{F}_p$ , then  $K = \mathbb{F}_{p^2}$ .*

*Proof.* The definition of addition and multiplication is clear: we put  $(a+b\sqrt{m}) + (c+d\sqrt{m}) = (a+c) + (b+d)\sqrt{m}$  and  $(a+b\sqrt{m})(c+d\sqrt{m}) = (ac+bdm) + (ad+bc)\sqrt{m}$ . The neutral element of addition is  $0 = 0 + 0\sqrt{m}$ , the neutral element of multiplication is  $1 = 1 + 0\sqrt{m}$ . If  $a + b\sqrt{m} \neq 0$ , then its multiplicative inverse is  $\frac{1}{a+b\sqrt{m}} = \frac{a-b\sqrt{m}}{a^2-mb^2} = \frac{a}{a^2-mb^2} - \frac{b}{a^2-mb^2}\sqrt{m}$ , which is an element of  $L$  since  $a^2 - mb^2 \neq 0$ . In fact,  $a^2 - mb^2 = 0$  with  $b \neq 0$  implies  $m = (a/b)^2$ , contradicting our assumption that  $m$  be a nonsquare.  $\square$

Thus in order to construct a field with 9 elements, pick the nonsquare  $-1 = 2 \in \mathbb{F}_3$  and form

$$\mathbb{F}_9 = \{a + bi : a, b \in \mathbb{F}_3\},$$

where  $i$  is an element with  $i^2 = -1$ . What are the  $\mathbb{F}_9$ -rational points on the unit circle  $\mathcal{C} : X^2 + Y^2 = 1$ ? We still have the four points  $(\pm 1, 0)$ ,  $(0, \pm 1)$  from  $\mathbb{F}_3$ , but there are more: clearly  $(\pm i, \pm i)$  are on the unit circle since  $i^2 + i^2 = -2 = 1$ . In fact, these are all points as the standard parametrization of the unit circle shows.

## 1.2.2 More Abstract Algebra

For constructing fields with  $p^n$  elements, the above ad-hoc method is not really suited. Let us therefore give an equivalent construction that works for general  $n$ .

To this end we have to look at the ring  $\mathbb{F}_p[X]$  of polynomials in  $X$  with coefficients from  $\mathbb{F}_p$  (note that the coefficients are from  $\mathbb{F}_p$ , but the exponents are not:  $X^2 = X \cdot X$  even in  $\mathbb{F}_2$ . Thus you are allowed to reduce the coefficients modulo  $p$ , but not the exponents!). Let  $m$  be a nonsquare in  $\mathbb{F}_p$ ; the multiples of the polynomial  $X^2 - m$  form an ideal  $I = (X^2 - \sqrt{m})$  in  $\mathbb{F}_p[X]$ , hence the quotient  $\mathbb{F}_p[X]/(X^2 - m)$  is a ring. Here is how you compute in this ring.

First observe that you are working modulo  $X^2 - m$ ; this means that  $X^2 - m \equiv 0 \pmod{I}$  in  $\mathbb{F}_p[X]/I$ . In particular, we have  $X^3 \equiv mX \pmod{I}$ ,  $X^4 \equiv m^2 \pmod{I}$ , etc. Thus every polynomial in  $\mathbb{F}_p[X]$  can be reduced modulo  $I$  to a polynomial of degree  $\leq 1$  just by replacing every  $X^2$  by  $m$ .

Now consider the map  $\phi : \mathbb{F}_p(\sqrt{m}) \rightarrow \mathbb{F}_p[X]/I$  defined by  $\phi(a + b\sqrt{m}) = a + bX \pmod{I}$ . We claim that  $\phi$  is an isomorphism. Clearly  $\phi$  is surjective. Moreover,  $\ker \phi$  consists of all  $a + b\sqrt{m}$  for which  $a + bX \in I$ . But the only multiple of  $X^2 - m$  of degree  $< 2$  is 0, hence  $a = b = 0$ , and thus  $\phi$  is injective. It is also clear that  $\phi$  is a homomorphism: we have

$$\begin{aligned} \phi((a + b\sqrt{m})(c + d\sqrt{m})) &= \phi((ac + bdm) + (ad + bc)\sqrt{m}) \\ &= (ac + bdm) + (ad + bc)X + I, \end{aligned}$$

and

$$\begin{aligned}\phi((a + b\sqrt{m})\phi(c + d\sqrt{m})) &= (a + bX + I)(c + dX + I) \\ &= ac + (ad + bc)X + bdX^2 + I \\ &= (ac + bdm) + (ad + bc)X + I.\end{aligned}$$

The corresponding property for addition is even simpler.

Thus instead of adjoining a square root of  $m$  to  $\mathbb{F}_p$  we might as well form  $\mathbb{F}_p[X]/(X^2 - m)$ . Observe that  $m$  is a nonsquare if and only if  $X^2 - m$  is irreducible in  $\mathbb{F}_p$ .

Now we can (almost) construct fields with  $p^n$  elements: just pick an irreducible polynomial  $f \in \mathbb{F}_p[X]$  and let  $K = \mathbb{F}_p[X]/(f)$ . This is a field with  $p^n$  elements; the only axiom that might be problematic to check is the existence of inverses. Assume that  $g + (f) \neq 0$ . Then  $f \nmid g$ , and since  $f$  is irreducible and  $\mathbb{F}_p[X]$  is a unique factorization domain, we have  $\gcd(f, g) = 1$ . Since  $\mathbb{F}_p[X]$  is Euclidean, there exist polynomials  $r, s \in \mathbb{F}_p[X]$  such that  $rf + sg = 1$ . But then  $(s + (f))$  is the inverse of  $g + (f)$  since  $sg \equiv 1 \pmod{f}$ .

This approach allows us to construct  $\mathbb{F}_4$  without technicalities: the polynomial  $f(X) = X^2 + X + 1$  is irreducible in  $\mathbb{F}_2$ , and we have  $\mathbb{F}_4 = \mathbb{F}_2[X]/(f)$ . Put  $x = X + (f)$  and  $y = x + 1$ . Then  $x^2 = X^2 + (f) = X + 1 + (f) = y$  exactly as before.