1
Fields

In this chapter the basic algebraic objects of a group, a ring and a field are defined. It is shown that a finite field has q elements, where q is a prime power, and that there is a unique field with q elements. We define an automorphism of a field and introduce the associated trace and norm functions. Some lemmas related to these functions are proven in the case that the field is finite. Finally, some additional results on fields are proven which will be needed in the subsequent chapters.

1.1 Rings and fields

A *group* G is a set with a binary operation $\circ$ which is associative ($(a \circ b) \circ c = a \circ (b \circ c)$), has an identity element e ($a \circ e = e \circ a = a$) and for which every element of G has an inverse (for all a, there is a b such that $a \circ b = b \circ a = e$). A group is *abelian* if the binary operation is commutative ($a \circ b = b \circ a$).

A *commutative ring* R is a set with two binary operations, addition and multiplication, such that it is an abelian group with respect to addition with identity element 0, and multiplication is commutative, associative and distributive ($a(b + c) = ab + ac$) and has an identity element 1.

The set of integers $\mathbb{Z}$ is an example of a commutative ring.

An *ideal* $\mathfrak{a}$ of a ring R is an additive subgroup with the property that $ra \in \mathfrak{a}$ for all $r \in R$ and $a \in \mathfrak{a}$. For example, the multiples of an element $r \in R$ form an ideal, which is denoted by (r).

A *coset* of $\mathfrak{a}$ is a set $r + \mathfrak{a} = \{r + a \mid a \in \mathfrak{a}\}$, for some $r \in R$. The set of cosets, denoted $R/\mathfrak{a}$ form a ring called the *quotient ring*, where addition and multiplication is defined by

$$r + \mathfrak{a} + s + \mathfrak{a} = r + s + \mathfrak{a},$$

and

$$(r+\mathfrak{a})(s+\mathfrak{a}) = rs+\mathfrak{a},$$

respectively.

Let n be a positive integer. The set $n\mathbb{Z}$ of integers that are multiples of n is an ideal of the ring $\mathbb{Z}$.

An ideal of R is *maximal* if it is not contained in a larger ideal other than R.

Let p be a prime number. The set $p\mathbb{Z} = \{n \in \mathbb{Z} \mid p \text{ divides } n\}$ is an example of a maximal ideal.

A *field* is a commutative ring in which every non-zero element has a multiplicative inverse. In other words, for all $a \neq 0$, there is a b such that $ab = 1$.

Theorem 1.1 *If $\mathfrak{a}$ is a maximal ideal of a commutative ring R then $R/\mathfrak{a}$ is a field.*

Proof We have to show that $x+\mathfrak{a}$ has a multiplicative inverse for all $x \in R$, $x \notin \mathfrak{a}$.

Let $\mathcal{B} = \{a+rx \mid a \in \mathfrak{a},\ r \in R\}$. Then $\mathcal{B}$ is an additive subgroup and has the property that $rb \in \mathcal{B}$ for all $r \in R$ and $b \in \mathcal{B}$. Hence, B is an ideal and it also strictly contains $\mathfrak{a}$. Since $\mathfrak{a}$ is maximal, $\mathcal{B} = R$ and so $1 \in \mathcal{B}$. Therefore, there is an $a \in \mathfrak{a}$ and $y \in R$ such that $a+yx = 1$. Then

$$(x+\mathfrak{a})(y+\mathfrak{a}) = xy+\mathfrak{a} = 1-a+\mathfrak{a} = 1+\mathfrak{a},$$

so $x+\mathfrak{a}$ has a multiplicative inverse. □

Theorem 1.1 implies that for p prime, $\mathbb{Z}/p\mathbb{Z}$ is a field. This field has p elements and is denoted $\mathbb{F}_p$.

Let $\mathbb{F}$ be a field and let f be an irreducible polynomial in $\mathbb{F}[X]$. Then (f) is a maximal ideal and so by Theorem 1.1, $\mathbb{F}/(f)$ is a field.

If $\mathbb{F} = \mathbb{F}_p$ and f has degree h then $\mathbb{F}[X]/(f)$ is a field with p^h elements.

For example, in Table 1.1, we have the addition and multiplication table of $\mathbb{F}_2[X]/(X^2+X+1)$, a finite field with four elements, and in Table 1.2 and Table 1.3, we have the addition and multiplication table of $\mathbb{F}_3[X]/(X^2+1)$, a finite field with nine elements.

Let $\mathbb{F}'$ also denote a field.

An *isomorphism* is a bijection σ from $\mathbb{F}$ to $\mathbb{F}'$ which preserves addition and multiplication. In other words, $\sigma(x+y) = \sigma(x)+\sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$. If there exists such an isomorphism then we say that $\mathbb{F}$ is *isomorphic* to $\mathbb{F}'$.

Theorem 1.2 *If $\mathbb{F}$ is a finite field with q elements then $a^q = a$, for all $a \in \mathbb{F}$.*

Table 1.1 *The addition and multiplication table for the field* $\mathbb{F}_2[X]/(X^2+X+1)$

$+$	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

$.$	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	$1+X$	1
$1+X$	0	$1+X$	1	X

Proof Suppose that $a \neq 0$. The set $A = \{xa \mid x \in \mathbb{F} \setminus \{0\}\}$ is the set of all non-zero elements of $\mathbb{F}$. The product of all the elements in A is a^{q-1} times the product of all non-zero elements of $\mathbb{F}$. However, A is the set of all non-zero elements of $\mathbb{F}$, so the product of all its elements is the product of all non-zero elements of $\mathbb{F}$. Hence, $a^{q-1} = 1$. □

The *splitting field* of a polynomial g in $\mathbb{F}[X]$ is the smallest field containing $\mathbb{F}$ in which g factorises into linear factors.

Theorem 1.3 *The splitting field of a polynomial is unique up to isomorphism.*

Proof This will be proved in Appendix B.2. □

Theorem 1.4 *A finite field $\mathbb{F}$ with $q = p^h$ elements is the splitting field of the polynomial $X^q - X$ and is unique up to isomorphsim. Thus,*

$$X^q - X = \prod_{a \in \mathbb{F}_q} (X - a),$$

and in particular the product of the non-zero elements of $\mathbb{F}$ is -1.

Proof By Theorem 1.2, a finite field with $q = p^h$ elements is the splitting field of the polynomial $X^q - X$, an element of $\mathbb{F}_p[X]$. □

We have already seen that $\mathbb{F}_p[X]/(f)$, where f is an irreducible polynomial of $\mathbb{F}_p[X]$ of degree h, is a field with $q = p^h$ elements. So we have the following theorem.

Theorem 1.5 *The unique field with q elements is isomorphic to $\mathbb{F}_p[X]/(f)$, where f is an irreducible polynomial of $\mathbb{F}_p[X]$ of degree h.*

We we will denote this field by $\mathbb{F}_q$.

The *characteristic* $\mathrm{char}(\mathbb{F})$ of a field $\mathbb{F}$ is the smallest integer n such that $1 + \cdots + 1 = 0$, where the sum has n terms. If no such n exists then we define $\mathrm{char}(\mathbb{F})$ to be zero.

Table 1.2 *The addition table for the field* $\mathbb{F}_3[X]/(X^2+1)$

$+$	0	1	2	X	$1+X$	$2+X$	$2X$	$1+2X$	$2+2X$
0	0	1	2	X	$1+X$	$2+X$	$2X$	$1+2X$	$2+2X$
1	1	2	0	$1+X$	$2+X$	X	$1+2X$	$2+2X$	$2X$
2	2	0	1	$2+X$	X	$1+X$	$2+2X$	$2X$	$1+2X$
X	X	$1+X$	$2+X$	$2X$	$1+2X$	$2+2X$	0	1	2
$1+X$	$1+X$	$2+X$	X	$1+2X$	$2+2X$	$2X$	1	2	0
$2+X$	$2+X$	X	$1+X$	$2+2X$	$2X$	$1+2X$	2	0	1
$2X$	$2X$	$1+2X$	$2+2X$	0	1	2	X	$1+X$	$2+X$
$1+2X$	$1+2X$	$2+2X$	$2X$	1	2	0	$1+X$	$2+X$	X
$2+2X$	$2+2X$	$2X$	$1+2X$	2	0	1	$2+X$	X	$1+X$

Table 1.3 *The multiplication table for the field* $\mathbb{F}_3[X]/(X^2+1)$

$.$	0	1	2	X	$1+X$	$2+X$	$2X$	$1+2X$	$2+2X$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	X	$1+X$	$2+X$	$2X$	$1+2X$	$2+2X$
2	0	2	1	$2X$	$2+2X$	$1+2X$	X	$2+X$	$1+X$
X	0	X	$2X$	2	$2+X$	$2+2X$	1	$1+X$	$1+2X$
$1+X$	0	$1+X$	$2+2X$	$2+X$	$2X$	1	$1+2X$	2	X
$2+X$	0	$2+X$	$1+2X$	$2+2X$	1	X	$1+X$	$2X$	2
$2X$	0	$2X$	X	1	$1+2X$	$1+X$	2	$2+2X$	$2+X$
$1+2X$	0	$1+2X$	$2+X$	$1+X$	2	$2X$	$2+2X$	X	1
$2+2X$	0	$2+2X$	$1+X$	$1+2X$	X	2	$2+X$	1	$2X$

Lemma 1.6 *If* $\mathrm{char}(\mathbb{F}) \neq 0$ *then* $\mathrm{char}(\mathbb{F}) = p$ *for some prime* p.

Proof Since $(1 + \cdots + 1)(1 + \cdots + 1) = 1 + \cdots + 1$, if the first sum has $m \geqslant 2$ terms and the second has $k \geqslant 2$ terms then the sum on the right-hand side has mk terms. If $mk = n$, the characteristic of $\mathbb{F}$, then the right-hand side is zero. Hence, one of the sums on the left-hand side is zero, a contradiction since n is minimal. Therefore, $n = p$ for some prime p. □

Note that the proof of the following theorem uses Theorem 2.2, which we have yet to prove. There is no anomaly here, since we will not use any of the following results to prove Theorem 2.2. The proof is included here for convenience, since this is the natural time to state the theorem.

Theorem 1.7 *A field* $\mathbb{F}$ *with* q *elements has characteristic* p *for some prime* p *and* $q = p^h$.

Proof It is clear a finite field must have finite characteristic, so it has characteristic p for some prime p by Lemma 1.6. The element 1 generates (additively) the elements of $\mathbb{F}_p$, so the field $\mathbb{F}$ contains $\mathbb{F}_p$. It is a vector space over $\mathbb{F}_p$, so by Theorem 2.2 there is a basis $B = \{e_1, \ldots, e_h\}$ for which every element of $\mathbb{F}$ can be written in a unique way as a linear combination of elements of B. Hence, $\mathbb{F}$ contains p^h elements for some positive integer h. □

Lemma 1.8 *For all* $i \in \mathbb{N}$, *the sum*

$$\sum_{a \in \mathbb{F}_q} a^i,$$

is zero if i *is not a multiple of* $q - 1$ *and* -1 *if* i *is a multiple of* $q - 1$.

Proof This is similar to the proof of Theorem 1.2. For $x \in \mathbb{F}_q \setminus \{0\}$,

$$\sum_{a \in \mathbb{F}_q} a^i = \sum_{a \in \mathbb{F}_q} (xa)^i = x^i \sum_{a \in \mathbb{F}_q} a^i.$$

If $i < q-1$ then there is an $x \in \mathbb{F}_q \setminus \{0\}$ such that $x^i \neq 1$. Hence, $\sum_{a \in \mathbb{F}_q} a^i = 0$.

If $i = q - 1$ then by Theorem 1.2, $a^{q-1} = 1$ for all non-zero $a \in \mathbb{F}_q$, so $\sum_{a \in \mathbb{F}_q} a^i = q - 1 = -1$.

If $i = j(q - 1) + k$, where $0 < k \leqslant q - 1$ then $\sum_{a \in \mathbb{F}_q} a^i = \sum_{a \in \mathbb{F}_q} a^k$, from which the lemma follows. □

1.2 Field automorphisms

An *automorphism* of a field $\mathbb{F}$ is an isomorphism from a field $\mathbb{F}$ to itself. The set of all automorphisms forms a group where we define the binary operation on the set to be composition.

Lemma 1.9 *The map $\sigma(a) = a^p$ is an automorphism of $\mathbb{F}_q$, where $q = p^h$ for some prime p.*

Proof By Theorem 1.7, $\mathrm{char}(\mathbb{F}_q) = p$, so

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b).$$

Clearly $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$ and $\sigma(1) = 1$. □

For any automorphism σ, we often write a^σ in place of $\sigma(a)$ when it is a more convenient notation.

The automorphism $\sigma(a) = a^p$ generates a group of automorphisms of $\mathbb{F}_q$,

$$\{id, \sigma, \sigma^2, \ldots, \sigma^{h-1}\}.$$

Note that $a^{\sigma^h} = a^{p^h} = a^q = a$, so $\sigma^h = id$, where id is the identity map.

Let σ be an automorphism of a field $\mathbb{F}$. The set of elements of $\mathbb{F}$ fixed by σ is denoted by $\mathrm{Fix}(\sigma)$.

Lemma 1.10 $\mathrm{Fix}(\sigma)$ *is a subfield of* $\mathbb{F}$.

Proof It is immediate that $\mathrm{Fix}(\sigma)$ is closed under addition and multiplication and contains 1, so it is a commutative ring. Moreover, if $x \in \mathrm{Fix}(\sigma)$,

$$1 = \sigma(1) = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1}) = x\sigma(x^{-1}).$$

Hence, $\sigma(x^{-1}) = x^{-1}$ and every element of $\mathrm{Fix}(\sigma)$ has a multiplicative inverse, so it is a field. □

The *order* of an automorphism σ is the smallest integer r such that $\sigma^r = id$.

The *trace function* of an automorphism σ is defined as

$$\mathrm{Tr}_\sigma(x) = x + x^\sigma + \cdots + x^{\sigma^{r-1}}.$$

Lemma 1.11 *The trace function is an additive surjective map from $\mathbb{F}$ to* $\mathrm{Fix}(\sigma)$.

Proof For all $x \in \mathbb{F}$,

$$\mathrm{Tr}_\sigma(x)^\sigma = (x + x^\sigma + \cdots + x^{\sigma^{r-1}})^\sigma = x^\sigma + \cdots + x^{\sigma^{r-1}} + x^{\sigma^r} = \mathrm{Tr}_\sigma(x),$$

so $\mathrm{Tr}_\sigma(x) \in \mathrm{Fix}(\sigma)$.

Since σ is additive,

$$\mathrm{Tr}_\sigma(x+y) = \mathrm{Tr}_\sigma(x) + \mathrm{Tr}_\sigma(y),$$

so Tr_σ is an additive map.

If $\lambda \in \mathrm{Fix}(\sigma)$ then $\mathrm{Tr}_\sigma(\lambda x) = \lambda \mathrm{Tr}_\sigma(x)$, so the trace function is surjective. □

The following lemma applies to finite fields.

Lemma 1.12 *Suppose that* $\mathrm{Fix}(\sigma) = \mathbb{F}_q$ *and that* $\mathbb{F} = \mathbb{F}_{q^h}$. *For all* $a \in \mathbb{F}_q$,

$$\mathrm{Tr}_\sigma(x) = a,$$

has precisely q^{h-1} *solutions.*

Proof For $a \in \mathbb{F}_q$,

$$\mathrm{Tr}_\sigma(x) = x + x^q + \ldots + x^{q^{h-1}} = a$$

has at most q^{h-1} solutions, since we can consider $\mathrm{Tr}_\sigma(x) - a$ as a polynomial in x of degree q^{h-1}. Since, $\mathrm{Tr}_\sigma(x) \in \mathrm{Fix}(\sigma) = \mathbb{F}_q$, for all $x \in \mathbb{F}_{q^h}$ and there are q elements in $\mathbb{F}_q$, there must be exactly q^{h-1} solutions for each of the elements $a \in \mathbb{F}_q$. □

The *norm function* of an automorphism σ is defined as

$$\mathrm{Norm}_\sigma(x) = xx^\sigma \cdots x^{\sigma^{r-1}}.$$

Lemma 1.13 *The norm function is a multiplicative map from* $\mathbb{F}$ *to* $\mathrm{Fix}(\sigma)$.

Proof For all $x \in \mathbb{F}$,

$$\mathrm{Norm}_\sigma(x)^\sigma = (xx^\sigma \cdots x^{\sigma^{r-1}})^\sigma = x^\sigma \cdots x^{\sigma^{r-1}} x^{\sigma^r} = \mathrm{Norm}_\sigma(x),$$

so $\mathrm{Norm}_\sigma(x) \in \mathrm{Fix}(\sigma)$.

Since σ is multiplicative,

$$\mathrm{Norm}_\sigma(xy) = \mathrm{Norm}_\sigma(x)\mathrm{Norm}_\sigma(y),$$

so Norm_σ is a multiplicative map. □

The following lemma applies to finite fields.

Lemma 1.14 *Suppose that* $\mathrm{Fix}(\sigma) = \mathbb{F}_q$ *and that* $\mathbb{F} = \mathbb{F}_{q^h}$. *For all non-zero* $a \in \mathbb{F}_q$,

$$\mathrm{Norm}_\sigma(x) = a,$$

has precisely $(q^h - 1)/(q-1)$ *solutions.*

Proof For $a \in \mathbb{F}_q$, $a \neq 0$,

$$\mathrm{Norm}_\sigma(x) = x^{1+q+\cdots+q^{h-1}} = a$$

has at most

$$1 + q + \cdots + q^{h-1} = (q^h - 1)/(q - 1)$$

solutions, since we can consider $\mathrm{Norm}_\sigma(x) - a$ as a polynomial in x of degree $(q^h - 1)/(q - 1)$. Since $\mathrm{Norm}_\sigma(x) = 0$ has only one solution, there must be exactly $(q^h - 1)/(q - 1)$ solutions for each of the $q - 1$ non-zero elements of $a \in \mathbb{F}_q$. □

We shall use the following lemmas in the classification of quadratic forms.

Lemma 1.15 *Suppose q is even and let σ be the automorphism of $\mathbb{F}_q$ defined by $\sigma(a) = a^2$. If $\mathrm{Tr}_\sigma(a^{-1}) = 1$ then the polynomial $X^2 + aX + 1$ is irreducible in $\mathbb{F}_q[X]$.*

Proof If X^2+aX+1 is reducible then there is an $x \in \mathbb{F}_q$ such that $x^2+ax+1 = 0$. Therefore $a^{-2}x^2 + a^{-1}x + a^{-2} = 0$. Applying the trace function and using the fact that the characteristic is two, we conclude that

$$\mathrm{Tr}_\sigma(a^{-2}) = \mathrm{Tr}_\sigma(a^{-1})^2 = 0.$$ □

Lemma 1.16 *Suppose q is odd and let S be the set of non-zero squares and let N be the set of non-squares. Then $|S| = |N| = (q - 1)/2$, for any $\eta \in N$,*

$$N = \{\eta x \mid x \in S\}$$

and the product of any two elements of N is an element of S.

Proof By definition,

$$S = \{x \in \mathbb{F}_q \mid x = y^2 \text{ for some } y \in \mathbb{F}_q \setminus \{0\}\}.$$

Since $y \mapsto y^2$ is a two-to-one mapping, the set S has $(q - 1)/2$ elements. Note that S is multiplicative, in other words, if $x, z \in S$ then $xz \in S$.

Let $\eta \in N$. Since $\eta \notin S$, it follows that $\eta x \notin S$ for all $x \in S$, so

$$N = \{\eta x \mid x \in S\}.$$

The product of two elements of N is $\eta x \eta z = \eta^2 xz$ for some $x, z \in S$, which is an element of S. □

1.3 The multiplicative group of a finite field

The *order* of an element a of a group G with identity element e is the smallest integer r such that $a^r = e$ (where the binary operation of G is written multiplicatively).

A group G is *cyclic* if it is generated by a single element. In other words, there is an element of G of order $|G|$.

Euler's *totient function* $\phi(d)$ is defined as the number of integers e, for which $1 \leqslant e \leqslant d-1$ and $\gcd(d, e) = 1$.

Lemma 1.17 *The non-zero elements of $\mathbb{F}_q$ form a multiplicative cyclic group.*

Proof Let $a \in \mathbb{F}_q$, $a \neq 0$. By Lemma 1.2, $a^{q-1} = 1$.

Let $N(d)$ be the number of elements of $\mathbb{F}_q^*$ of order d. There are at most d roots of the polynomial

$$X^d - 1.$$

If a is an element of order d then the roots of this polynomial are $\{1, a, \ldots, a^{d-1}\}$. The element a^e has order d if and only if $\gcd(d, e) = 1$. So $N(d) = 0$ or $N(d) = \phi(d)$.

Euler's formula states

$$\sum_{d|q-1} \phi(d) = q - 1,$$

so we have

$$\sum_{d|q-1} N(d) = q - 1 = \sum_{d|q-1} \phi(d) \geqslant \sum_{d|q-1} N(d).$$

Therefore, we have equality throughout and $N(q-1) = \phi(q-1) \neq 0$. Hence, the set of non-zero elements of $\mathbb{F}_q$ has an element of order $q-1$ and so is cyclic. □

Lemma 1.18 *If $\gcd(e, q-1) = 1$ then the equation $x^e = 1$ has no solutions in $\mathbb{F}_q \setminus \{1\}$.*

Proof A solution to the equation $x^e = 1$ generates a multiplicative subgroup $\{x, x^2, \ldots, x^{e'}\}$, for some e' dividing e. The multiplicative group of $\mathbb{F}_q$ has $q-1$ elements, so e' divides $q-1$. Since $\gcd(e, q-1) = 1$, $e' = 1$ and $x = 1$. □

1.4 Exercises

Exercise 1 Prove that a group has a unique identity element and that each element has a unique inverse.

Exercise 2 Calculate the multiplication table of the field with eight elements, $\mathbb{F}_2[X]/(X^3+X+1)$.

Exercise 3 Show that complex conjugation of the field of complex numbers is an automorphism. Deduce the fixed field of this automorphism and prove that the associated norm function is not surjective onto the fixed field.

Exercise 4 Deduce the tower of subfields of $\mathbb{F}_{p^{12}}$, by considering $\mathrm{Fix}(\sigma)$, where σ is an automorphism of $\mathbb{F}_{p^{12}}$.

Exercise 5 Show that X^2+1 and X^2-X-1 are both irreducible in $\mathbb{F}_3[X]$. Find the isomorphism from $\mathbb{F}_3[X]/(X^2+1)$ to $\mathbb{F}_3[X]/(X^2-X-1)$.

An irreducible polynomial $f \in \mathbb{F}_p[X]$ is *primitive* if it has a root of order p^h-1 in $\mathbb{F}_{p^h}$, where h is the degree of f. An element of $\mathbb{F}_{p^h}$ of order p^h-1 is called a *primitive element*.

Exercise 6 Find a primitive irreducible polynomial and a non-primitive irreducible polynomial of degree two in $\mathbb{F}_3[X]$.

Exercise 7 Let q be odd. Prove that the polynomial

$$X^{(q-1)/2}-1$$

factorises in $\mathbb{F}_q[X]$ and that its roots are the non-zero squares in $\mathbb{F}_q$ and that the polynomial

$$X^{(q-1)/2}+1$$

also factorises in $\mathbb{F}_q[X]$ and that its roots are the non-squares in $\mathbb{F}_q$.

Exercise 8 Let p be an odd prime. Let

$$f(X)=\frac{X^{p+1}-1}{X-1}-2 \in \mathbb{F}_p[X].$$

(i) Prove by induction that if z is a root of f then

$$z^{p^i}=\frac{(i+1)z-i}{iz-(i-1)}.$$

(ii) Show that $z \notin \mathbb{F}_p$, but $z \in \mathbb{F}_{p^p}$.
(iii) Prove that f is irreducible in $\mathbb{F}_p[X]$.