Chapter 3

Finite Fields

3.1 Construction

Definition 3.1. A *field* F is a set closed under two operations $+$, $\times$ such that

(i) $(F, +)$ is an abelian group with identity 0;

(ii) $(F\backslash\{0\}, \times)$ is an abelian group with identity 1;

(iii) For all $x, y, z \in F$,

$$x(y+z) = xy + xz, \quad (x+y)z = xz + yz.$$

Example 3.2. Examples of fields:

$$\begin{array}{lcl} \mathbf{R} & = & \text{the real numbers;} \\ \mathbf{Q} & = & \text{the rational numbers;} \\ \mathbf{C} & = & \text{the complex numbers;} \\ \mathbf{Z}_p = \mathbf{F}_p & = & \text{the integers modulo the prime } p. \end{array}$$

Lemma 3.3. (i) *A field has no zero divisors.*

(ii) *If the positive integer n is composite, $\mathbf{Z}_n$ is not a field.*

Proof (i) If $m_1m_2 = 0$ with $m_1, m_2 \neq 0$, then $m_1^{-1}m_1m_2 = 0$ and so $m_2 = 0$, a contradiction.

(ii) Suppose $n = m_1m_2$ with $m_1 > 1, m_1 > 1$. Then, in $\mathbf{Z}_n$, it follows that $m_1m_2 = 0$, again a contradiction by (i). □

Lemma 3.4. *If p is a prime, then $\mathbf{Z}_p$ is a field.*

Proof If $1 \leq n < p$, then $n \neq 0$ in $\mathbf{Z}_p$. So there exist $a, b \in \mathbf{Z}$ such that

$$an + bp = 1.$$

In $\mathbf{Z}_p$, it follows that $an = 1$ and $n^{-1} = a$. □

Example 3.5. (i) $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5, \mathbf{Z}_7$ are fields;

(ii) $\mathbf{Z}_4$, $\mathbf{Z}_6$ are not fields.

In $\mathbf{Z}_4$, $2 \times 2 = 4 = 0$. In $\mathbf{Z}_6$, $2 \times 3 = 6 = 0$.

Definition 3.6. In any field F, the smallest positive integer p such that

$$\underbrace{1+1+\cdots+1}_{p}=0$$

is the *characteristic.*

If there is no such integer, then F has *characteristic zero.*

Lemma 3.7. *In a finite field F,*

(i) *the characteristic p is a prime;*

(ii) *F is a vector space over $\mathbf{F}_p$.*

Proof (i) If $p=p_1p_2$ with $1<p_i<p$, then $p_1p_2\,1=0$, whence $p_2\,1=0$, a contradiction.

(ii) This follows from the axioms of a vector space. $\square$

Theorem 3.8. *If a finite field F has $|F|=q$, then $q=p^h$ with p a prime and $h\in\mathbf{N}$.*

Proof Let $\{\alpha_1,\ldots,\alpha_h\}$ be a basis for F over $\mathbf{F}_p$. Then, if $x\in F$, there exist unique $t_1,\ldots,t_h\in\mathbf{F}_p$ such that

$$x=t_1\alpha_1+t_2\alpha_2+\cdots+t_h\alpha_h.$$

As there are p choices for each t_i, so $|F|=p^h$. $\square$

Theorem 3.9. *Any two fields of the same order q are isomorphic; that is, if F_1, F_2 are fields with $|F_1|=|F_2|=q$, then there exists a bijection*

$$\theta: F_1\rightarrow F_2$$

with $\theta(x+y)=\theta(x)+\theta(y)$, $\theta(x\,y)=\theta(x)\,\theta(y)$ for all $x,y\in F_1$.

Notation 3.10. If $|F|=q$, write $F=\mathbf{F}_q$ or $F=\mathrm{GF}(q)$; here GF stands for *Galois field.*

Definition 3.11. A *ring* (= commutative ring with 1) is a set with two operations $+,\times$ satisfying all the axioms of a field except perhaps the existence of a multiplicative inverse for all non-zero elements.

Example 3.12. (i) $\mathbf{Z}$, the integers;

(ii)
$$\begin{aligned} F[X] &= \{a_0+a_1\,X+\cdots+a_n\,X^n \mid a_i\in F;\ n\in\mathbf{N}\cup\{0\}\} \\ &= \text{ring of polynomials over } F \text{ in the indeterminate } X. \end{aligned}$$

Definition 3.13. The polynomial $f(X)$ in $F[X]$ is *irreducible* if $f=f_1\,f_2$ with $f_1,\ f_2\in F[X]$ implies that either f_1 or f_2 is a constant.

Example 3.14. The polynomial X^2+1 is irreducible over $\mathbf{R}$ but reducible over $\mathbf{C}$.

Lemma 3.15 (Remainder Theorem)**.** *Over a field F, the linear polynomial $X-\alpha$ divides $f(X)$ if and only if $f(\alpha)=0$.*

Proof First,

$$f(X) = (X - \alpha)g(X) + R$$

with $R \in F$. Put $X = \alpha$; then $R = f(\alpha)$. So $R = 0$ if and only if $f(\alpha) = 0$. □

Example 3.16. (i) If $F = \mathbf{F}_2$, then $X^2 + 1$ is reducible but $X^2 + X + 1$ is irreducible, since 1 is a zero of the first but $0, 1$ are not zeros of the second.

(ii) If $F = \mathbf{F}_3$, then $X^2 - X + 1$ is reducible but $X^2 - X - 1$ is irreducible, since -1 is a zero of the first but $0, 1, -1$ are not zeros of the second.

(iii) If $F = \mathbf{F}_5$, then $X^2 + X - 1$ is reducible but $X^2 - X + 1$ is irreducible, since 2 is a zero of the first but $0, 1, -1, 2, -2$ are not zeros of the second.

Example 3.17. Construction of a field of order p^2

First,

$$\mathbf{C} = \mathbf{R}[X]/(X^2 + 1) = \{x + y\,i \mid x, y \in \mathbf{R};\ i^2 + 1 = 0\}.$$

Similarly, let $X^2 - bX - c$ be irreducible over $\mathbf{F}_p$. Write

$$\alpha^2 - b\alpha - c = 0.$$

Then

$$\begin{aligned} \mathbf{F}_{p^2} = \mathrm{GF}(p^2) &= \mathbf{F}_p[X]/(X^2 - bX - c) \\ &= \{a_0 + a_1\alpha \mid a_i \in \mathbf{F}_p;\ \alpha^2 = b\alpha + c\} \end{aligned}$$

Example 3.18. (i) To construct $\mathbf{F}_4$, take $X^2 + X + 1$, which is irreducible over $\mathbf{F}_2$, and let $\omega^2 + \omega + 1 = 0$. Then

$$\mathbf{F}_4 = \{a + b\omega \mid a, b \in \mathbf{F}_2\} = \{0, 1, \omega, 1 + \omega = \omega^2\}.$$

(ii) To construct $\mathbf{F}_9$, take $X^2 - X - 1$, which is irreducible over $\mathbf{F}_3 = \{0, 1, -1 = 2\}$, and let $\tau^2 - \tau - 1 = 0$. Then

$$\mathbf{F}_9 = \{a + b\tau \mid a, b \in \mathbf{F}_3;\ \tau^2 = \tau + 1\} = \{0, \pm 1, \pm\tau, \pm 1 \pm \tau\}.$$

Alternatively, take $X^2 + 1$, which is also irreducible over $\mathbf{F}_3$ and let $\iota^2 + 1 = 0$. Then

$$\mathbf{F}_9 = \{a + b\iota \mid a, b \in \mathbf{F}_3;\ \iota^2 = -1\} = \{0, \pm 1, \pm\iota, \pm 1 \pm \iota\}.$$

Example 3.19. Construction of $\mathbf{F}_q$ with $q = p^h$

Let $f(X) = X^h - b_{h-1}X^{h-1} - \cdots - b_1 X - b_0$ and let $f(\alpha) = 0$, where $f \in \mathbf{F}_p[X]$ and irreducible. Then

$$\mathbf{F}_q = \{a_0 + a_1\alpha + \cdots + a_{h-1}\alpha^{h-1} \mid a_i \in \mathbf{F}_p;\ f(\alpha) = 0\}$$

is a field of order $q = p^h$.

Theorem 3.20. *Let $q = p^h$. The field $\mathbf{F}_q$ has the following properties.*

(i) $(x + y)^p = x^p + y^p$ *for all* $x, y \in \mathbf{F}_q$.

(ii) $t^q = t$ *for all* $t \in \mathbf{F}_q$.

(iii) *There exists* $\alpha \in \mathbf{F}_q$ *such that*

$$\mathbf{F}_q = \{0, 1, \alpha, \ldots, \alpha^{q-2} \mid \alpha^{q-1} = 1\}.$$

(iv) *Under multiplication,* $\mathbf{F}_q \setminus \{0\}$ *is a cyclic group of order* $q-1$:

$$\mathbf{F}_q \cong \mathbf{Z}_{q-1}.$$

(v) *Under addition,*

$$\mathbf{F}_q \cong \underbrace{\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p}_{h}.$$

(vi) *If* F_1, F_2 *are finite fields such that* $F_1 \subset F_2$, *then* $|F_1|$ *divides* $|F_2|$.

(vii) *The automorphism group of* $\mathbf{F}_q$ *is*

$$\mathrm{Aut}(\mathbf{F}_q) = \{1, \varphi, \ldots, \varphi^{h-1}\} \cong \mathbf{Z}_h,$$

where $\varphi(x) = x^p$, $\varphi^i(x) = x^{p^i}$.

Definition 3.21. If α is as in Theorem 3.20 (iii), it is *primitive*. The irreducible polynomial over $\mathbf{F}_p$ that α satisfies is also *primitive*.

Note 3.22. A primitive element in $\mathbf{F}_q$ has *order* $q-1$, where the order of x is the smallest positive integer n such that $x^n = 1$. The order n divides $q-1$ for any $x \in \mathbf{F}_q \setminus \{0\}$.

Corollary 3.23.

$$\prod t = -1,$$

where the product is taken over all $t \in \mathbf{F}_q \setminus \{0\}$.

3.2 Irreducible polynomials

Theorem 3.24. $X^{p^n} - X$ *is the product of all monic irreducible* f *in* $\mathbf{F}_p[X]$ *such that deg* f *divides* n.

Let N_d be the number of polynomials over $\mathbf{F}_p$ which are monic and irreducible of degree d.

Corollary 3.25. $p^n = \sum_{d|n} dN_d$.

Definition 3.26 (The Möbius function)**.** If the integer $m = p_1^{r_1} \cdots p_k^{r_k}$, then

$$\mu(m) = \begin{cases} 1 & \text{if } r_1 = r_2 = \ldots = r_k = 0, \\ 0 & \text{if } r_i > 1 \text{ for some } i, \\ (-1)^k & \text{if } r_1 = r_2 = \cdots = r_k = 1. \end{cases}$$

If f is a function $\mathbf{N} \to \mathbf{Z}$ such that

$$g(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

Corollary 3.27. $N_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$

Proof Put $g(n) = p^n,\ f(n) = nN_n$. □

Corollary 3.28. *If $N(n, q)$ is the number of irreducible monic polynomials of degree n over $\mathbf{F}_q$, then*

$$N(n, q) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Corollary 3.29. $N(n, q) > 0$.

Proof

$$N(n, q) > \frac{1}{n}(q^n - q^{n-1} \ldots - q) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q - 1}\right) > 0.$$

□

Hence $\mathbf{F}_{p^h}$ can be constructed from an irreducible polynomial of degree h and such a polynomial always divides $X^{p^h} - X$.

Example 3.30. Construct $\mathbf{F}_8$ over $\mathbf{F}_2$

$$\begin{aligned} X^8 + X &= X(X^7 + 1) \\ &= X(X + 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1) \\ &= X(X + 1)(X^3 + X^2 + 1)(X^3 + X + 1). \end{aligned}$$

Using $X^3 + X^2 + 1$, let $\epsilon^3 + \epsilon^2 + 1 = 0$. Then

$$\mathbf{F}_8 = \{0, 1, \epsilon, \epsilon^2, \epsilon^3, \epsilon^4, \epsilon^5, \epsilon^6 \mid \epsilon^7 = 1\}.$$

Note that $\epsilon^6 + \epsilon^4 + 1 = 0,\ \epsilon^5 + \epsilon + 1 = 0$. Hence, for example,

$$\begin{aligned} &\epsilon + \epsilon^3 = \epsilon(1 + \epsilon^2) = \epsilon.\epsilon^3 = \epsilon^4; \\ &\epsilon^2 + \epsilon^6 = \epsilon^2(1 + \epsilon^4) = \epsilon^2.\epsilon^6 = \epsilon^8 = \epsilon. \end{aligned}$$

3.3 Applications

3.3.1 Old ISBN numbers, also known as ISBN-10

Example 3.31. $\mathbf{F}_{11}$

x	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10
x	1	2	3	4	5	−5	−4	−3	−2	−1
x^{-1}	1	−5	4	3	−2	2	−3	−4	5	−1

Example 3.32. Examples of old International Standard Book Numbers

$$0 - 19 - 853537 - 6$$
$$0 - 19 - 850295 - 8$$

Here, 0 indicates the language, namely English; 19 is the publisher, Oxford University Press; 850295 is the book number; and 8 is the check digit.

Definition 3.33.

$$x_1 x_2 \cdots x_{10}$$

is an old ISBN number if

(i) each of the first nine digits is in {0,1,...,9};

(ii) the last digit may also be X;

(iii)
$$\sum_{i=1}^{10} i x_i = 0$$
in $\mathbf{F}_{11}$.

For example,

$$\begin{array}{c|ccccccccccccccc} x_i & 0 & 1 & 9 & 8 & 5 & 3 & 5 & 9 & 2 & 9 & & & & \\ i & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & & & & \\ \hline ix_i & 0 & 2 & 5 & -1 & 3 & -4 & 2 & -5 & -4 & 2 & = & 14-14 & = & 0 \end{array}$$

Theorem 3.34. (i) *An old ISBN number* $x_1 x_2 \cdots x_{10}$ *has*

$$x_{10} = \sum_{i=1}^{9} i x_i \quad \textit{in } \mathbf{F}_{11}.$$

(ii) *The old ISBN code* detects (a) *a single error or* (b) *a double error created by interchanging two digits.*

(iii) *The old ISBN code* **corrects** *an error in a given place.*

Proof (i) In $\mathbf{F}_{11}$, $10 = -1$. So

$$0 = \sum_1^{10} i x_i = \sum_1^{9} i x_i + 10 x_{10} = \sum_1^{9} i x_i - x_{10}.$$

Hence $x_{10} = \sum\limits_1^9 i x_i$.

(ii) If $y_j = x_j + t$ is received for x_j with $t \neq 0$, but $y_i = x_i$ for $i \neq j$, then

$$\sum i y_i = \sum i x_i + tj = tj \neq 0$$

in $\mathbf{F}_{11}$.

(iii) If the number is $x_1 x_2 \cdots x \cdots x_{10}$ with x in the j-th place, then

$$jx + \sum_{i \neq j} i x_i = 0,$$
$$x = -j^{-1} \sum_{i \neq j} i x_i.$$

□

3.3.2 New ISBN numbers, also known as ISBN-13

Example 3.35. Examples of new International Standard Book Numbers:

$$978 - 0 - 691 - 09679 - 7$$
$$978 - 0 - 8218 - 4306 - 2$$

In the first of these, 978 is always present; 0 indicates the language, namely English; 691 is the publisher Princeton University Press; 09679 is the book number; and 7 is the check digit. In the second, 8218 is the American Mathematical Society.

Definition 3.36.

$$x_1 x_2 \cdots x_{13}$$

is a new ISBN number if

(i) each digit is in {0,1,...,9};

(iii)

$$x_1 + 3x_2 + x_3 + 3x_4 + \cdots + x_{11} + 3x_{12} + x_{13} = 0$$

in $\mathbf{Z}_{10}$.

For example,

x_i	9	7	8	0	6	9	1	0	9	6	7	9	7		
c_i	1	3	1	3	1	3	1	3	1	3	1	3	1		
$c_i x_i$	9	21	8	0	6	27	1	0	9	18	7	27	7		
=	9	1	8	0	6	7	1	0	9	8	7	7	7	=	70

Theorem 3.37. (i) *A new ISBN number $x_1 x_2 \cdots x_{13}$ has*

$$x_{13} = -\sum_{i=1}^{12} c_i x_i \quad \textit{in } \mathbf{Z}_{10},$$

where $c_i = 1$ for i odd and $c_i = 3$ for i even.

(ii) *The new ISBN code* **corrects** *an error in a given place.*

3.3.3 The Codabar system

Example 3.38. 4929 5316 9048 9053 is a valid 16-digit credit card number:

4929 is Barclaycard; the next 11 digits form the identifying number; the last digit is a check digit.

Definition 3.39. In general,

$$x = x_1 x_2 \cdots x_{15} x_{16}$$

is a *codabar number* if, with $c = 2121212121212121$,

$$c \cdot x + t \equiv 0 \pmod{10}$$

where t is the number of x_i in odd positions i with $x_i \geq 5$.

In the example, $t = 4$ as only positions $5, 9, 13, 15$ fulfil this condition. Hence,

$$\begin{array}{r|llllllllllllllll}
x & 4 & 9 & 2 & 9 & 5 & 3 & 1 & 6 & 9 & 0 & 4 & 8 & 9 & 0 & 5 & 3 \\
c & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\
x_i c_i & 8 & 9 & 4 & 9 & 0 & 3 & 2 & 6 & 8 & 0 & 8 & 8 & 8 & 0 & 0 & 3 = 76
\end{array}$$

Now, $76 + 4 = 80 \equiv 0 \pmod{10}$.

Note 3.40. As in Theorem 3.34, the codabar system corrects an error in a given place.