MATH4302

Combinatorial Designs

Supplementary notes on groups, fields and vector spaces

2021

Contents

There are many textbooks which cover the material in these notes, for example see [1, 2, 3, 4]. These are not intended to be comprehensive notes. They serve only to summarise many of the basic properties of groups, fields and vector spaces that are needed for this course.

Chapter 1

Groups

A **group** $G = (G, *)$ consists of a set G of elements on which a binary operation $a * b$ is defined such that the following group axioms are satisfied.
Group Axioms:

G1. For any $a, b \in G$, $a * b \in G$.

G2. For any $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

G3. There exists an element e, called the identity, in G such that $a * e = e * a = a$ for each $a \in G$.

G4. For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

The **order** of a group $\mathcal{G} = (G, *)$ is $|G|$. A group which also satisfies

G5. For any $a, b \in G$, $a * b = b * a$

is called an **abelian** group. The axioms G1, G2, G3, G4 and G5 say that G is closed, associative, has an identity, has inverses, and is commutative (or abelian) respectively. The binary operation for a group is often either addition $a + b$ in which case we have an **additive group** or multiplication ab in which case we have a **multiplicative group**.

For each positive integer n, the integers modulo n form an abelian group under addition. This group is denoted by $(\mathbb{Z}_n, +)$ and is called the **cyclic group of order n**. Note that a cyclic group of order n can also be written multiplicatively as follows. The elements of the group are $x^0 = 1, x^1 = x, x^2, x^3, \ldots, x^{n-1}$ and multiplication is defined by $x^i x^j = x^{i+j}$ with $x^n = 1$. The exponents behave like the integers modulo n. Written this way, the group is called the cyclic group of order n generated by x.

The integers modulo n under multiplication do not form a group, as 0 has no inverse. However, when n is prime $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is an abelian group. When n is not prime, $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is not a group. For example, in $\mathbb{Z}_6$ the element 2 has no multiplicative inverse. In general, $a \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$, which explains why $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is a group if and only if n is prime.

A **subgroup** of a group G is a subset of G which is itself a group (using the same binary operation). The notation $H \leq G$ is used to indicate that H is a subgroup of G. If $H \leq G$ then for each $g \in G$, $gH = \{gh : h \in H\}$ is called a **left coset** of H in G. Similarly $Hg = \{hg : h \in H\}$ is called a **right coset** of H in G. Note that $g_1 \in g_2H$ if and only if $g_1H = g_2H$. It is easy to show that the set of all left (respectively right) cosets of H in G partitions G into parts of cardinality $|H|$. The following theorem, known as Lagrange's Theorem, is a direct consequence of this.

Theorem 1.1. If G is finite and $H \leq G$, then $|H|$ divides $|G|$.

A subgroup H of a group G is a **normal subgroup** if $gH = Hg$ for all $g \in G$, equivalently if the left and right cosets of H in G coincide. For the most part, we will be dealing with abelian groups, and every subgroup of an abelian group is a normal subgroup.

Definition 1.2. Let H be a normal subgroup of G. The set of all cosets of H in G is denoted by G/H and forms a group, called the **quotient group**, under the operation $(Hg_1)(Hg_2) = H(g_1g_2)$. □

For any element g in a finite multiplicative group G, there exists a smallest integer n such that $g^n = 1$. To see this, observe that if $g^s = g^t$ with $s < t$ then $g^s \cdot (g^{-1})^s = g^t \cdot (g^{-1})^s$ and so we have $g^{t-s} = 1$. This integer n is called the **order** (in G) of the element g. It is easy to check that for any element g of order n in a group G, $\{1, g, g^2, \ldots, g^{n-1}\}$ is a subgroup of G. This subgroup is called the **subgroup generated by** g and is denoted by $\langle g \rangle$. It is isomorphic to the cyclic group $\mathbb{Z}_n$. Note that by Theorem 1.1, the order of any element of a finite group divides the order of the group itself.

Chapter 2

Polynomials

Let F be a field (see Chapter 3). A **polynomial** (in one variable) over F is a sequence $(a_0, a_1, a_2, ...)$ of elements of F with the property that there exists a non-negative integer n such that $a_i = 0$ for all $i > n$. The set of all such polynomials is denoted by $F[x]$ where x is the variable (or indeterminate). A polynomial is usually written in the form

$$\sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

The elements of the sequence $(a_0, a_1, a_2, \ldots)$ are called the **coefficients** of the polynomial and n is its **degree** (except that if $n = 0$ and $a_0 = 0$, then the degree is $-\infty$). A polynomial in $F[x]$ is often called a **polynomial over F**. Addition and multiplication of polynomials is defined in the usual way (with all operations being carried out in F). That is,

$$a(x) + b(x) = \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=1}^{\infty} (a_i + b_i) x_i$$

and

$$a(x) \cdot b(x) = \sum_{i=0}^{\infty} a_i x^i \cdot \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (\sum_{j=0}^{i} a_j b_{i-j}) x^i.$$

A proof of the following theorem can be found in [2].

Theorem 2.1. If F is a field and $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x) \neq 0$, then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $a(x) = b(x) \cdot q(x) + r(x)$ where $0 \leq \deg(r(x)) < \deg(b(x))$ or $r(x) = 0$.

For polynomials $a(x)$ and $b(x)$ in $F[x]$, we say that $b(x)$ **divides** $a(x)$ if there is a polynomial $q(x) \in F[x]$ such that $a(x) = b(x) \cdot q(x)$. Moreover, for polynomials $a(x), b(x), f(x) \in F[x]$, we say that $a(x)$ and $b(x)$ are **equivalent modulo $f(x)$**, denoted $a(x) \equiv b(x) \pmod{f(x)}$, if and only if $f(x)$ divides $a(x) - b(x)$.

Given an element $\alpha \in F$ and a polynomial $a(x) = \sum_{i=0}^{\infty} a_i x^i$ in $F[x]$, $a(\alpha)$ is defined to be $\sum_{i=0}^{\infty} a_i \alpha^i$ (with operations being carried out in F). An element $\alpha \in F$ is a **root** of a polynomial $f(x)$ in $F[x]$ if $f(\alpha) = 0$.

Theorem 2.2. If F is a field and $a(x) \in F[x]$, then the element $\alpha \in F$ is a root of $a(x)$ if and only if $x - \alpha$ divides $a(x)$.

Proof If $x - \alpha$ divides $a(x)$ then $a(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$ and it follows that $a(\alpha) = (\alpha - \alpha) \cdot q(\alpha) = 0$. Thus α is a root. Conversely, suppose α is a root of $a(x)$, that is $a(\alpha) = 0$. By Theorem 2.1 (with $b(x) = x - \alpha$), there exist polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $a(x) = (x - \alpha)q(x) + r(x)$ where $\deg(r(x)) = 0$ or $r(x) = 0$. In either case $r(x)$ is a constant. Thus, $0 = a(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r(\alpha) = r(\alpha) = r(x)$ and so we see that $x - \alpha$ divides $a(x)$. □

Definition 2.3. A polynomial $f(x)$ of degree at least 1 is **irreducible** over a finite field F if it cannot be written as a product of two polynomials each of degree less than $f(x)$. □

A proof of the following theorem can be found in [3].

Theorem 2.4. For any prime p and any integer n, there exists an irreducible polynomial of degree n over the finite field $(\mathbb{Z}_p, +, \cdot)$.

The following theorem gives a fundamental property of irreducible polynomials. A proof can be found in [2]. Note the similarity between the property of irreducible polynomials given in the theorem and the property that a prime p divides a product ab of integers if and only if p divides a or p divides b.

Theorem 2.5. If $f(x)$, $a(x)$ and $b(x)$ are polynomials over a field F, $f(x)$ is irreducible, and $f(x)$ divides $a(x)b(x)$, then either $f(x)$ divides $a(x)$ or $f(x)$ divides $b(x)$.

Theorem 2.6. If F is a field, then any non-zero polynomial of degree $n \geq 0$ in $F[x]$ has at most n roots in F.

Proof The proof is by induction on n. If $n = 0$ then the result is trivial since the polynomial has no roots. So assume that any polynomial of degree n in $F[x]$ has at most n roots and consider a polynomial $a(x) \in F[x]$ of degree $n + 1$. If $a(x)$ has no roots then we are finished so we can assume it has a root α. Thus, by Theorem 2.2 we have $a(x) = (x - \alpha) \cdot q(x)$ for some $q(x) \in F[x]$. Now, if $\beta \neq \alpha$ is a root of $a(x)$ then $(\beta - \alpha) \cdot q(\beta) = 0$. Since $\beta - \alpha$ is non-zero, it has a multiplicative inverse in F and so $q(\beta) = 0$ and we see that β is also a root of $q(x)$. However, it is clear that $\deg(q(x)) = n$ and so by the induction hypothesis, $q(x)$ has at most n roots. Thus, $a(x)$ has at most $n + 1$ roots and the proof follows by induction. □

Chapter 3

Fields

A **field** $F = (F, +, \cdot)$ consists of a set F of elements on which two binary operations addition $a + b$ and multiplication ab are defined such that the following field axioms are satisfied.
Field Axioms:

A1. For any $a, b \in F$, $a + b \in F$.

A2. For any $a, b, c \in F$, $(a + b) + c = a + (b + c)$.

A3. There exists an element 0, called the additive identity, in F such that $a + 0 = 0 + a = a$ for each $a \in F$.

A4. For each $a \in F$, there exists an element $-a \in F$, called the additive inverse of a, such that $a + (-a) = (-a) + a = 0$.

A5. For any $a, b \in F$, $a + b = b + a$.

M1. For any $a, b \in F$, $ab \in F$.

M2. For any $a, b, c \in F$, $(ab)c = a(bc)$.

M3. There exists an element 1, called the multiplicative identity, in F such that $1a = a1 = a$ for each $a \in F$.

M4. For each $a \in F \setminus \{0\}$, there exists an element $a^{-1} \in F$, called the multiplicative inverse of a, such that $aa^{-1} = a^{-1}a = 1$.

M5. For any $a, b \in F$, $ab = ba$.

D. For any $a, b, c \in F$, $a(b + c) = ab + ac$.

The **order** of a field $F = (F, +, \cdot)$ is $|F|$. Notice that if $F = (F, +, \cdot)$ is a field then $(F, +)$ and $(F \setminus \{0\}, \cdot)$ are abelian groups. The group $(F, +)$ is called the **additive group** of F, and $(F \setminus \{0\}, \cdot)$ is called the **multiplicative group** of F. The rational numbers, the real numbers and the complex numbers, with the usual addition and multiplication, are each examples of fields. The integers do not form a field as only 1 and -1 have multiplicative inverses.

Example 3.1. If p is prime then $(\mathbb{Z}_p, +, \cdot)$ is a field. □

Consider $(\mathbb{Z}_n, +, \cdot)$. It is easy to verify that $(\mathbb{Z}_n, +, \cdot)$ satisfies all of the field axioms except possibly M4. Moreover, one can verify that axiom M4 is satisfied if and only if n is prime. So $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if n is prime. When $n = p$ is prime, the notation $\mathbb{F}_p$ or $\mathrm{GF}(p)$ is used to denote this field; the **Galois Field** of order p. The fact that $(\mathbb{Z}_n, +, \cdot)$ satisfies M4 if and only if n is prime can be verified by recalling that $a \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$. Alternatively, the following argument can be used.

Firstly, if n is not prime then it is clear that there exists a $b \in \mathbb{Z}_n \setminus \{0, 1\}$ such that b divides n. Clearly b has no multiplicative inverse. Conversely, let p be prime, let $a \in \mathbb{Z}_p \setminus \{0\}$, and consider the elements $a, 2a, 3a, \ldots, (p-1)a$ of $\mathbb{Z}_p$. These must be the $p-1$ distinct non-zero elements of $\mathbb{Z}_p$. For if $ra = sa \pmod p$ for distinct $r, s \in \mathbb{Z}_p \setminus \{0\}$, then $a(r-s) = 0 \pmod p$. That is p divides $a(r-s)$ which means p divides a or p divides $r-s$, both of which are contradictions. The first because a is a non-zero element of $\mathbb{Z}_p$ and the second because r and s are distinct modulo p. Similarly, if $ra = 0 \pmod p$ then p divides ra which implies p divides r or p divides a, both of which are contradictions. So since $a, 2a, 3a, \ldots, (p-1)a$ are the $p-1$ non-zero elements of $\mathbb{Z}_p$, one of $a, 2a, 3a, \ldots, (p-1)a$ is 1. But if $ta = 1$ then t is the multiplicative inverse of a and so we see that axiom M4 is satisfied.

We observe that Fermat's Little Theorem, which states that $a^{p-1} = 1 \pmod p$ for any prime p and any non-zero integer a, is an easy consequence of the above argument. Since we have $\{a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, \ldots, p-1\}$, obviously we have

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1).$$

Multiplying both sides by $1^{-1} \cdot 2^{-1} \cdot \ldots \cdot (p-1)^{-1}$ we obtain $a^{p-1} = 1 \pmod p$.

Although $(\mathbb{Z}_n, +, \cdot)$ is not a field when n is not prime, there do exist finite fields of non-prime order. We now show how to construct a finite field of order q for any prime power $q = p^n$ (p prime and $n > 1$). Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_p$. The elements of our field of order p^n will be the equivalence or residue classes modulo $f(x)$ of the polynomials over $\mathbb{F}_p$, and addition and multiplication will be defined in the usual way. For polynomials over a field F, the analogue of a prime is an irreducible polynomial, so we are looking at an analogue of $\mathbb{F}_p = (\mathbb{Z}_p, +, \cdot)$.

By Theorem 2.1, if $a(x)$ is any polynomial of degree at least n then we can write

$$a(x) = f(x)q(x) + r(x)$$

where $r(x)$ has degree at most $n-1$. So $a(x) \equiv r(x) \pmod{f(x)}$ and we see that every polynomial over $\mathbb{F}_p$ is equivalent to a polynomial of degree less than n over $\mathbb{F}_p$. Hence we may take polynomials of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$$

where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_p$ as representatives of our residue classes. Clearly, if $a(x)$ and $b(x)$ are distinct polynomials of degree less than n over $\mathbb{F}_p$ then $a(x)$ and $b(x)$ are not equivalent modulo $f(x)$. So we have p^n distinct residue classes.

It is straightforward to verify that these residue classes together with the usual operations of addition and multiplication of polynomials satisfy all of the field axioms except possibly Axiom M4.

We now check that it too is satisfied. Let $q = p^n$ and let $u_0, u_1, u_2, \ldots, u_{q-1}$ be our q residue class representatives with $u_0 = 0$ and $u_1 = 1$. Now let $k \neq 0$ and consider $u_k u_1, u_k u_2, \ldots, u_k u_{q-1}$. Firstly, it is clear that $u_k u_i$ is non-zero for $i = 1, 2, \ldots, q-1$. For if $u_k u_i \equiv 0 \pmod{f(x)}$ then $f(x)$ divides u_k or $f(x)$ divides u_i, neither of which is possible. We now show that $u_k u_1, u_k u_2, \ldots, u_k u_{q-1}$ are in $q-1$ distinct residue classes. Suppose for a contradiction that $u_k u_i \equiv u_k u_j \pmod{f(x)}$ for some $i \neq j$. That is, $f(x)$ divides $u_k(u_i - u_j)$ and from the irreducibility of $f(x)$ this implies $f(x)$ divides u_k or $u_i \equiv u_j \pmod{f(x)}$, neither of which is possible. Hence $u_k u_1, u_k u_2, \ldots, u_k u_{q-1}$ are indeed the $q-1$ distinct non-zero residue classes. In particular, one of $u_k u_1, u_k u_2, \ldots, u_k u_{q-1}$ is 1 and so we see that u_k has a multiplicative inverse. Hence Axiom M4 holds, and we have a field of order $q = p^n$.

Definition 3.2. Let $q = p^n$ where p is prime and $n \geq 1$ is an integer. The finite field of order q consisting of the residue classes of polynomials modulo an irreducible polynomial of degree n over $\mathbb{F}_p$ is denoted by $\mathbb{F}_q$ (or sometimes GF(q)). □

Example 3.3. Construction of $\mathbb{F}_9$. Let $p = 3$ and $n = 2$ so that $p^n = 9$. The elements of the field $\mathbb{F}_9$ are

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2.$$

In this example we take $f(x) = x^2 + x + 2$ as our irreducible polynomial. The addition and multiplication tables for the field are shown below.

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	$2x+1$	1	$x+1$	$x+2$	$2x+2$	2
$x+1$	0	$x+1$	$2x+2$	1	$x+2$	$2x$	2	x	$2x+1$
$x+2$	0	$x+2$	$2x+2$	$x+1$	$2x$	2	$2x+2$	1	x
$2x$	0	$2x$	x	$x+2$	2	$2x+2$	$2x+1$	$x+1$	1
$2x+1$	0	$2x+1$	$x+2$	$2x+2$	x	1	$x+1$	2	$2x$
$2x+2$	0	$2x+2$	$x+1$	2	$2x+1$	x	1	$2x$	$x+2$

We illustrate how this multiplication table is constructed with the example of $(x+2)(2x+1)$. Using ordinary polynomial multiplication and reducing the coefficients modulo 3 we obtain $(x+2)(2x+1) = 2x^2+5x+2 = 2x^2+2x+2$. But since we are working modulo $f(x) = x^2+x+2$, we have $x^2+x+2 = 0$ which implies $x^2 = -x-2 = 2x+1$ and $2x^2 = x+2$. Hence, $(x+2)(2x+1) = (x+2)+2x+2 = 1$. □

The following theorem says that the fields constructed above are the only finite fields. There is a proof in [1].

Theorem 3.4. There exists a finite field of order q if and only if q is a prime power (that is, $q = p^\alpha$ for some prime p and some positive integer α). Moreover, for each prime power q, the only (up to isomorphism) finite field of order q is $\mathbb{F}_q$.

Theorem 3.5. The additive group of $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{Z}_p^n$.

Proof Clearly, $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \mapsto (a_0, a_1, \ldots, a_{n-1})$ is an isomorphism. □

It turns out that the multiplicative group of $\mathbb{F}_q$ is $\mathbb{Z}_{q-1}$, but to prove this we first need a result on the **Euler totient function** $\phi(n)$. This is defined for any positive integer n to be the number of positive integers less than or equal to n which are relatively prime to n. That is

$$\phi(n) = |\{x : 1 \le x \le n, \gcd(x,n) = 1\}|.$$

The value of $\phi(n)$ for $n \le 20$ is given in the following table.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Lemma 3.6.

$$\sum_{d|n} \phi(d) = n$$

Proof First note that the number of elements of order n in the cyclic group $\mathbb{Z}_n$ is $\phi(n)$. Let d be a divisor of n. Then $\mathbb{Z}_n$ has exactly one subgroup of order d, namely the subgroup generated by n/d. Let X_d be the subset of elements of order d in the subgroup of order d. So $|X_d| = \phi(d)$. But X_d contains all the elements of $\mathbb{Z}_n$ that have order d. So since each element of $\mathbb{Z}_n$ has order d for some divisor d of n, it follows that

$$\sum_{d|n} \phi(d) = n.$$

□

Theorem 3.7. The multiplicative group of non-zero elements of a finite field of order q is the cyclic group of order $q-1$.

Proof Let F be a field of order q, let d be the order of some element $\alpha \in F \setminus \{0\}$, and let $\langle\alpha\rangle$ be the subgroup of $F \setminus \{0\}$ generated by α (so $|\langle\alpha\rangle| = d$). Now, the order of each element in $\langle\alpha\rangle$ divides d and so $x^d = 1$ for all $x \in \langle\alpha\rangle$. That is, each of the d elements of $\langle\alpha\rangle$ is a root of the polynomial $x^d - 1$. By Theorem 2.6 this polynomial has at most d roots in F, and so we see that the elements of $\langle\alpha\rangle$ are all the roots of the polynomial $x^d - 1$. In particular, there are no more elements of order d other than those in $\langle\alpha\rangle$. This means that the number of elements of order d in $(F \setminus \{0\}, \cdot)$ is either 0 or $\phi(d)$.

Let $\psi(d)$ denote the number of elements of order d in $(F \setminus \{0\}, \cdot)$ and for a contradiction suppose $(F \setminus \{0\}, \cdot)$ is not the cyclic group. Then there is no element of order $q - 1$ and it follows that

$$\sum_{d|q-1} \psi(d) < \sum_{d|q-1} \phi(d).$$

But by Lemma 3.6, this implies

$$\sum_{d|n} \psi(d) < q - 1$$

and so we have less than $q - 1$ elements. This is a contradiction and we conclude that $(F \setminus \{0\}, \cdot)$ is the cyclic group. □

An element $\omega \in F$ such that $\{\omega^i : i = 0, 1, \ldots, q-2\}$ is the set of all non-zero elements of a finite field F of order q is called a **primitive element**. Theorem 3.7 guarantees that every finite field has a primitive element. It can be shown that for any prime power q and any positive integer n, there exists an irreducible polynomial (in the variable x) of degree n over $\mathbb{F}_q$ such that x is a primitive element of $\mathbb{F}_{q^n}$. Such a polynomial is called a **primitive polynomial**. Note that the term primitive polynomial is used to mean something different in Ring Theory. The polynomial $x^4 + x^3 + x^2 + x + 1$ is an irreducible polynomial of degree 4 over $\mathbb{F}_2$, but it is not a primitive polynomial.

The following tables give a primitive polynomial of degree n over $\mathbb{F}_p$ for various small values of p and n.

n	Primitive polynomial of degree n over $\mathbb{F}_2$
1	$x + 1$
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$

n	Primitive polynomial of degree n over $\mathbb{F}_3$
1	$x + 1$
2	$x^2 + x + 2$
3	$x^3 + 2x + 1$
4	$x^4 + x + 2$
5	$x^5 + 2x + 1$
6	$x^6 + x + 2$

n	Primitive polynomial of degree n over $\mathbb{F}_5$
1	$x + 2$
2	$x^2 + x + 2$
3	$x^3 + 3x + 2$
4	$x^4 + x^2 + 2x + 2$

n	Primitive polynomial of degree n over $\mathbb{F}_7$
1	$x + 2$
2	$x^2 + x + 3$
3	$x^3 + 3x + 2$
4	$x^4 + x^2 + 3x + 5$

A **subfield** of a field $F = (F, +, \cdot)$ is a subset of F which is itself a field (using the same binary operations). Proofs of the following theorem can be found in [1] and [4].

Theorem 3.8. For each divisor m of n, $\mathbb{F}_{p^n}$ has a unique subfield of order p^m consisting of the elements satisfying the equation $z^{p^m} = z$. Furthermore, these are the only subfields of $\mathbb{F}_{p^n}$.

We prove the second part of the theorem only. Suppose that t is the order of a subfield of $\mathbb{F}_{p^n}$. Then t must divide p^n (as the order of the subfield's additive group divides the order of $\mathbb{F}_{p^n}$'s additive group) so $t = p^m$ for some m. But we also have that $p^m - 1$ divides $p^n - 1$ (as the order of the subfield's multiplicative group divides the order of $\mathbb{F}_{p^n}$'s multiplicative group). Let $n = bm + r$ with $0 \leq r \leq m-1$. Since p^m-1 divides $p^{bm}-1$ (as $p^{bm}-1 = (p^m)^b-1 = (p^m-1)((p^m)^{b-1}+(p^m)^{b-2}+\cdots+1)$) we have $p^m - 1$ divides $p^r(p^{bm} - 1) = p^{bm+r} - p^r = p^n - p^r$. Combining this with the fact that $p^m - 1$ divides $p^n - 1$ we see that $p^m - 1$ divides $(p^n - 1) - (p^n - p^r) = p^r - 1$. Since $r \leq m$ we have $r = 0$ and m divides n.

Definition 3.9. Let p be an odd prime, let $q = p^m$ for some integer $m \geq 1$, and let ω be a primitive element of $\mathbb{F}_q$. The **quadratic residues** or **squares** in $\mathbb{F}_q$ are the elements $1, \omega^2, \omega^4, \ldots, \omega^{q-3}$. □

Theorem 3.10. Let p be an odd prime, let $q = p^m$ for some integer $m \geq 1$, and let ω be a primitive element of $\mathbb{F}_q$. Then

- when $q \equiv 1 \pmod{4}$, x is a square if and only if $-x$ is a square, and
- when $q \equiv 3 \pmod{4}$, x is a square if and only if $-x$ is not a square.

Proof First notice that $(\omega^{\frac{q-1}{2}} - 1)(\omega^{\frac{q-1}{2}} + 1) = \omega^{q-1} - 1 = 0$ and so either $\omega^{\frac{q-1}{2}} = 1$ or $\omega^{\frac{q-1}{2}} = -1$. But we know that $\omega^{\frac{q-1}{2}} \neq 1$ and so we must have $\omega^{\frac{q-1}{2}} = -1$. So for $q \equiv 1 \pmod{4}$, $x = \omega^{2i}$ if and only if $-x = (-1)\omega^{2i} = \omega^{\frac{q-1}{2}}\omega^{2i} = \omega^{2(\frac{q-1}{4}+i)}$; that is, x is a square if and only if $-x$ is a square. For $q \equiv 3 \pmod{4}$, we have $x = \omega^{2i}$ if and only if $-x = (-1)\omega^{2i} = \omega^{\frac{q-1}{2}}\omega^{2i} = \omega^{2(\frac{q-3}{4}+i)+1}$; that is, x is a square if and only if $-x$ is not a square. □

Chapter 4

Vector Spaces

Definition 4.1. A **vector space** consists of a set V (of vectors) and a field F, together with two binary operations, vector addition ($v_1 + v_2$ where $v_1, v_2 \in V$) and scalar multiplication (αv where $\alpha \in F$ and $v \in V$), satisfying the following axioms.

A1 CLOSURE: For all $v_1, v_2 \in V$, $v_1 + v_2 \in V$.

A2 ASSOCIATIVITY: For all $v_1, v_2, v_3 \in V$, $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_1$.

A3 COMMUTATIVITY: For all $v_1, v_2 \in V$, $v_1 + v_2 = v_2 + v_1$.

A4 IDENTITY: There exists a 'zero element' $0 \in V$ such that $v + 0 = v$ for all $v \in V$.

A5 INVERSES: For each $v \in V$ there exists a vector $-v \in V$ (the additive inverse of v) such that $v - v = 0$.

S1 CLOSURE: For all $\alpha \in F$ and $v \in V$, $\alpha v \in V$.

S2 ASSOCIATIVITY: For all $\alpha_1, \alpha_2 \in F$ and all $v \in V$, $\alpha_1(\alpha_2 v) = (\alpha_1 \alpha_2)v$.

S3 IDENTITY: For all $v \in V$, $1v = v$ where 1 is the multiplicative identity of F.

D1 DISTRIBUTIVITY: For all $\alpha_1, \alpha_2 \in F$ and all $v \in V$, $(\alpha_1 + \alpha_2)v = \alpha_1 v + \alpha_2 v$.

D2 DISTRIBUTIVITY: For all $\alpha \in F$ and all $v_1, v_2 \in V$, $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$.

□

Axioms A1-A5 state that $(V, +)$ is an abelian group, and the remaining axioms define the required properties of scalar multiplication of the vectors in V by the field elements. Simple examples of vector spaces are **coordinate spaces** where the vectors consist of n-tuples of elements of F, with addition and scalar multiplication defined by

$$\begin{aligned}&(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),\\&\alpha(x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).\end{aligned}$$

It is routine to check that coordinate spaces satisfy the axioms of a vector space. The coordinate space of n-tuples of elements of F is denoted by F^n. The coordinate space $\mathbb{R}^n$ is the familiar vector space of real-valued vectors in n dimensions.

Definition 4.2. Any subset U of a vector space V such that U is itself a vector space (under the binary operations of V) is called a **subspace** of V. Any vector of the form

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k \in F$ and $v_1, v_2, \ldots, v_k \in V$ is called a **linear combination** of the vectors $v_1, v_2, \ldots, v_k$. The **span** of a set $S = \{v_1, v_2, \ldots, v_k\}$ of vectors in a vector space V is the set of all linear combinations of $v_1, v_2, \ldots, v_k$, and is denoted by $\langle S \rangle$. That is,

$$\langle S \rangle = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k : \alpha_1, \alpha_2, \ldots, \alpha_k \in F\}.$$

□

The proofs of the following two theorems are straightforward.

Theorem 4.3. If V is a vector space and $S \subset V$, then S is a subspace if and only if $S \neq \emptyset$ and $S = \langle S \rangle$. In particular, $\langle S \rangle$ is a subspace of V.

Theorem 4.4. If a vector v_k is a linear combination of $v_1, v_2, \ldots, v_{k-1}$, then $\langle \{v_1, v_2, \ldots, v_{k-1}\} \rangle = \langle \{v_1, v_2, \ldots, v_k\} \rangle$.

Definition 4.5. A set $\{v_1, v_2, \ldots, v_k\}$ of vectors in V is **linearly independent** if

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0 \text{ implies } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 0.$$

Otherwise, $\{v_1, v_2, \ldots, v_k\}$ is **linearly dependent**. □

Theorem 4.6. A set S of vectors in a vector space V is a linearly independent if and only if no vector of S is a linear combination of the others.

Proof If $S = \{v_1, v_2, \ldots, v_k\}$ and $v_k = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{k-1} v_{k-1}$, then we have $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{k-1} v_{k-1} + \alpha_k v_k = 0$ where $\alpha_k = -1$. Thus, S is linearly dependent. Conversely, if S is linearly dependent, then without loss of generality we have $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0$ for some $\alpha_k \neq 0$. Thus, we have

$$v_k = -\frac{\alpha_1}{\alpha_k} v_1 - \frac{\alpha_2}{\alpha_k} v_2 - \cdots - \frac{\alpha_{k-1}}{\alpha_k} v_{k-1}$$

(so v_k is written as a linear combination of the other vectors of S). □

Definition 4.7. A set S of vectors in a vector space V is a **basis** for V if S is linearly independent and spans V. □

Theorem 4.8. If S is a basis for V, then any vector of V can be expressed as a linear combination of the vectors of S in exactly one way.

Proof Since S is spanning, any $v \in V$ can be expressed as a linear combination of the vectors of S in at least one way. If v can be expressed in two distinct ways, say $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$ and $v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k$, then

$$\begin{aligned} & (\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \cdots + (\alpha_k - b_k)v_k \\ = \; & (\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k) - (\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k) \\ = \; & v - v = 0. \end{aligned}$$

But since the two expressions for v were assumed to be distinct, $(\alpha_1 - \beta_1), (\alpha_2 - \beta_2), \ldots, (\alpha_k - b_k)$ are not all zero, which contradicts the fact that S is linearly independent. □

Theorem 4.9. If S is a basis for a vector space V, then any set of more than $|S|$ vectors from V is linearly dependent. That is, any linearly independent set of vectors from V has at most $|S|$ elements. Consequently, every basis for V contains the same number of elements.

Proof Let $S = \{e_1, e_2, \ldots, e_n\}$ be a basis for a vector space V over a field F and let $\{v_1, v_2, \ldots, v_m\}$ be a set of vectors from V with $m > n$. Since S is a basis, each of $v_1, v_2, \ldots, v_m$ can be written as a linear combination of $e_1, e_2, \ldots, e_n$. That is,

$$\begin{aligned} v_1 &= \alpha_{11}e_1 + \alpha_{12}e_2 + \cdots + \alpha_{1n}e_n \\ v_2 &= \alpha_{21}e_1 + \alpha_{22}e_2 + \cdots + \alpha_{2n}e_n \\ &\vdots \\ v_m &= \alpha_{m1}e_1 + \alpha_{m2}e_2 + \cdots + \alpha_{mn}e_n \end{aligned}$$

where $\alpha_{11}, \ldots, \alpha_{mn} \in F$.

Now consider the following set of equations.

$$\begin{aligned} \alpha_{11}x_1 + \alpha_{21}x_2 + \cdots + \alpha_{m1}x_m &= 0 \\ \alpha_{12}x_1 + \alpha_{22}x_2 + \cdots + \alpha_{m2}x_m &= 0 \\ &\vdots \\ \alpha_{1n}x_1 + \alpha_{2n}x_2 + \cdots + \alpha_{mn}x_m &= 0 \end{aligned}$$

This is a set of n equations in the m unknowns $x_1, x_2, \ldots, x_m$, which has a solution $x_1 = \beta_1, x_2 = \beta_2, \ldots, x_m = \beta_m$ in which $\beta_1, \beta_2, \ldots, \beta_m$ are not all zero, because $m > n$. But then we have

$$\begin{aligned} & \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_m v_m \\ = \; & \beta_1(\alpha_{11}e_1 + \alpha_{12}e_2 + \cdots + \alpha_{1n}e_n) + \cdots + \beta_m(\alpha_{m1}e_1 + \alpha_{m2}e_2 + \cdots + \alpha_{mn}e_n) \\ = \; & (\alpha_{11}\beta_1 + \alpha_{21}\beta_2 + \cdots + \alpha_{m1}\beta_m)e_1 + \cdots + (\alpha_{1n}\beta_1 + \alpha_{2n}\beta_2 + \cdots + \alpha_{mn}\beta_m)e_n \\ = \; & 0 \end{aligned}$$

with $\beta_1, \beta_2, \ldots, \beta_m$ not all zero, which means that $v_1, v_2, \ldots, v_m$ are linearly dependent. □

Definition 4.10. The **dimension** of a vector space V is the number of elements in a basis for V and is denoted by $\dim(V)$. If $\dim(V) = n$, then V is said to be an **n-dimensional** vector space. □

Theorem 4.11. If V is an n-dimensional vector space, then any set of n linearly independent vectors from V is a basis for V.

Proof If $v_1, v_2, \dots, v_n$ is a linearly independent set of vectors from V that does not span V, then there exists a $v \in V$ which is not a linear combination of $v_1, v_2, \dots, v_n$. Thus, $\{v_1, v_2, \dots, v_n, v\}$ is a linearly independent set of more than n vectors in V, which contradicts Theorem 4.9. □

Theorem 4.12. If $S = \{v_1, v_2, \dots, v_m\}$ is any linearly independent set of vectors from an n-dimensional vector space V and $m < n$, then there exist vectors $v_{m+1}, v_{m+2}, \dots, v_n \in V$ such that $\{v_1, v_2, \dots, v_n\}$ is a basis for V.

Proof Since any basis for an n-dimensional vector space has n elements, S is not a basis and so there is a vector $v \in V$ which is not a linear combination of $v_1, v_2, \dots, v_m$. This means that $S \cup \{v\}$ is linearly independent. Vectors can be added in this manner until a linearly independent set of n vectors is obtained. Any such set is a basis by Theorem 4.11. □

Definition 4.13. If V is a vector space and $S_1, S_2 \subseteq V$, then $S_1 + S_2$ is defined by $S_1 + S_2 = \{x + y : x \in S_1, y \in S_2\}$. □

Theorem 4.14. If V is a vector space and U and W are subspaces of V, then both $U \cap W$ and $U + W$ are subspaces of V and $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

Proof Let V be a vector space and let U and W be subspaces of V. Since U and W are subspaces, $0 \in U$ and $0 \in W$ and so $U \cap W \neq \emptyset$. Also, any linear combination of vectors from $U \cap W$ is in both U and W, and so $\langle U \cap W \rangle = U \cap W$. Thus, $U \cap W$ is a subspace. It is clear that $U + W = \langle U \cup W \rangle$, and thus that $U + W$ is a subspace of V. It remains to show that $\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

Let $r = \dim(U \cap W)$, $s = \dim(U)$, $t = \dim(W)$, and let $\{x_1, x_2, \dots, x_r\}$ be a basis for $U \cap W$. By Theorem 4.12, there exists a basis $\{x_1, x_2, \dots, x_r, y_1, y_2, \dots, y_{s-r}\}$ for U and a basis $\{x_1, x_2, \dots, x_r, z_1, z_2, \dots, z_{t-r}$ for W. We now show that

$$B = \{x_1, x_2, \dots, x_r, y_1, y_2, \dots, y_{s-r}, z_1, z_2, \dots, z_{t-r}\}$$

is a basis for $U + W$.

It is clear that B spans $U + W$. To see that B is linearly independent, suppose

$$\sum_{i=1}^{r} \alpha_i x_i + \sum_{i=1}^{s-r} \beta_i y_i + \sum_{i=1}^{t-r} \gamma_i z_i = 0.$$

Define $v = \sum_{i=1}^{s-r} \beta_i y_i = -\sum_{i=1}^{r} \alpha_i x_i - \sum_{i=1}^{t-r} \gamma_i z_i$. Since v is a linear combination of $y_1, y_2, \dots, y_{s-r}$ we have $v \in U$ and since v is a linear combination of $x_1, x_2, \dots, x_r, z_1, z_2, \dots, z_{t-r}$ we have $v \in W$. Thus, $v \in U \cap W$ and so $v = \alpha'_1 x_1 + \alpha'_2 x_2 + \cdots + \alpha'_r x_r$ for some $\alpha'_1, \alpha'_2, \dots, \alpha'_r$. But we also have $v =$

$-\sum_{i=1}^{r}\alpha_i x_i - \sum_{i=1}^{t-r}\gamma_i z_i$ and since v can be written as a linear combination of $x_1, x_2, \ldots, x_r, z_1, z_2, \ldots, z_{t-r}$ in exactly one way (see Theorem 4.8), we have $\alpha_i = -\alpha_i'$ for $i = 1, 2, \ldots, r$ and $\gamma_1 = \gamma_2 = \cdots \gamma_{t-r} = 0$. By similar argument, we also have $\beta_1 = \beta_2 = \cdots = \beta_{s-r} = 0$. Thus, $\sum_{i=1}^{r}\alpha_i x_i = 0$ and this implies that $\alpha_1 = \alpha_2 = \cdots = \alpha_r = 0$ (because $x_1, x_2, \ldots, x_r$ are linearly independent). This proves that B is linearly independent and hence that B is a a basis for $U + V$. It follows that $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$. □

Bibliography

[1] P. J. Cameron, Introduction to Algebra, Oxford University Press, 1998.

[2] J. B. Fraleigh, A First Course in Abstract Algebra (seventh edition), Addison Wesley, 2003.

[3] K. H. Kim and F. W. Roush, Applied Abstract Algebra, Wiley, 1983.

[4] M. Mignotte and D. Ştefănescu, Polynomials: An Algorithmic Approach, Springer, 1999.