Overview

Mathematics (in particular, algebra) is the language of coding theory. The most important mathematical objects needed in coding theory are *groups*, *finite fields*, and *vector spaces*. The first part of the course is devoted to an in-depth discussion of these topics. (Note: finite field = Galois field.)

Definition: Set

set An arbitrary collection of elements. A set may be *finite* (e.g., $\{1, 2, 3\}$), countably infinite (e.g., the positive integers), or uncountably infinite (e.g., the real numbers).

cardinality The number of objects in the set. The cardinality of a set S is denoted by $|S|$.

order = cardinality (in particular, when dealing with groups and fields).

Definition: Group

A **group** is a set G on which a binary operation $\cdot : G \times G \to G$ is defined and for which the following requirements hold:

1. **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
2. **Identity:** there exists $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. **Inverse:** for all $a \in G$ there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

A group is said to be *commutative* or *abelian* if it satisfies one more requirement:

4. **Commutativity:** for all $a, b \in G$, $a \cdot b = b \cdot a$.

Examples of Groups

Example 1. The set of integers forms an infinite abelian group under integer addition, but not under integer multiplication (why not?).

Example 2. The set of $n \times n$ matrices with real elements forms an abelian group under matrix addition.

Finite Groups (1)

We are primarily interested in *finite* groups. One of the simplest methods for constructing finite groups lies in the application of modular arithmetic. We write

$$a \equiv b \pmod{m}$$

(pronounced "a is equivalent—or congruent—to b modulo m") if $a = b + km$ for some integer k. This relation is reflexive, symmetric, and transitive, and therefore divides the set of integers into m distinct *equivalence classes*.

Finite Groups (2)

Example. Integers modulo 5.
$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$,
$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$,
$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$,
$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$,
$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$.

Theorem 2-1. The equivalence classes $[0], [1], \ldots, [m-1]$ form an abelian group of order m under addition modulo m.

Theorem 2-2. The equivalence classes $[1], [2] \ldots, [m-1]$ form an abelian group of order $m-1$ under multiplication modulo m if and only if m is a prime.

The Two Groups of Order 4

·	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Addition mod 4

·	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

A dihedral group

A Multiplicative Group

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Multiplication mod 7

More Definitions

order of a group element The order of $g \in G$ is the smallest positive integer n such that $\underbrace{g \cdot g \cdot \dots \cdot g}_{n} = e$.

subgroup A subset $S \subseteq G$ that forms a group. It is *proper* if $S \neq G$.

Example. The group of addition modulo 4 contains the proper subgroups $\{0\}$ and $\{0, 2\}$.

Definition: Cosets

Let S be a subgroup of G. For any value of $x \in G$, the set $x \cdot S := \{x \cdot s, s \in S\}$ (respectively, $S \cdot x$) forms a **left coset** (respectively, **right coset**) of S in G. If G is abelian, $x \cdot S = S \cdot x$, and left and right cosets coincide and are simply called **cosets**.

Example. The subgroup $\{0, 2\}$ of the group of addition modulo 4 has the cosets $\{0, 2\}$ and $\{1, 3\}$.

Theorem 2-3. The distinct cosets of a subgroup $S \subseteq G$ are disjoint.

Lagrange's Theorem

Theorem 2-4. If S is a subgroup of G, then $|S|$ divides $|G|$.

Proof: By Theorem 2-3, two distinct cosets of S are disjoint. Moreover, all elements of G belong to some coset of S (for example, an element x belongs to $x \cdot S$). Therefore the distinct cosets, which are of order $|S|$, partition G, and the theorem follows. $\square$

Corollary. A group G of prime order has exactly the following subgroups: $\{e\}$ and G.

Definition: Ring

A **ring** is a set R with two binary operations $\cdot : R \times R \to R$ and $+ : R \times R \to R$ for which the following requirements hold:

1. R forms an abelian group under $+$. The additive identity element is labeled 0.
2. Associativity for $\cdot$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
3. The operation $\cdot$ distributes over $+$: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

A ring is said to be a **commutative ring** and a **ring with identity**, respectively, if the following two requirements hold:

4. The operation $\cdot$ commutes: $a \cdot b = b \cdot a$.
5. The operation $\cdot$ has an identity element, which is labeled 1.

Examples of Rings

Example 1. The set of integers modulo m under addition and multiplication form a commutative ring with identity.

Example 2. Matrices with integer elements form a ring with identity under standard matrix addition and multiplication.

Example 3. The set of all polynomials with binary coefficients forms a commutative ring with identity under polynomial addition and multiplication with the coefficients taken modulo 2. This ring is usually denoted by $F_2[x]$ or GF(2)[x].

Definition: Field

A **field** is a set F with two binary operations $\cdot : F \times F \to F$ and $+ : F \times F \to F$ for which the following requirements hold:

1. F forms an abelian group under $+$. The additive identity element is labeled 0.
2. $F \setminus \{0\}$ forms an abelian group under $\cdot$. The multiplicative identity element is labeled 1.
3. The operations $+$ and $\cdot$ distribute: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

A field can also be defined as a commutative ring with identity in which every non-zero element has a multiplicative inverse.

Examples of Fields

Example 1. The rational numbers form an infinite field.

Example 2. The real numbers form an infinite field, as do the complex numbers.

Example 3. GF(2):

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Constructing Fields

Finite field = Galois field.

Theorem 2-5. Let p be a prime. The integers $\{0, 1, \ldots, p-1\}$ form the field GF(p) under addition and multiplication modulo p.

Theorem. The order of a finite field is p^m, where p is a prime. There is a *unique* field for each such order.

When $m > 1$ in the previous theorem, one cannot use simple modular arithmetic. Instead, such fields can be constructed as vector spaces over GF(p).

Vector Spaces

Let V be a set of *vectors* and F a field of *scalars* with two operations: $+ : V \times V \to V$ and $\cdot : F \times V \to V$. Then V forms a vector space over F if the following conditions are satisfied:

1. V forms an abelian group under $+$.
2. The operations $+$ and $\cdot$ distribute: $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$ and $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$.
3. Associativity: For all $a, b \in F$ and all $\mathbf{v} \in V$, $(a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$.
4. The multiplicative identity $1 \in F$ acts as multiplicative identity in scalar multiplication: for all $\mathbf{v} \in V$, $1 \cdot \mathbf{v} = \mathbf{v}$.

The field F is called the *ground field* of the vector space V.

On Vector Spaces

Example. A vector space over GF(3):
$(1, 0, 2, 1) + (1, 1, 1, 1) = (2, 1, 0, 2)$, $2 \cdot (1, 0, 2, 2) = (2, 0, 1, 1)$.

The expression $a_1 \cdot \mathbf{v}_1 + a_2 \cdot \mathbf{v}_2 + \cdots + a_m \cdot \mathbf{v}_m$ where $a_i \in F$, $\mathbf{v}_i \in V$ is called a *linear combination.* A set $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\} \subseteq V$ of vectors is called a **spanning set** if all vectors in V can be obtained as a linear combination of these vectors.

A set of vectors is said to be *linearly dependent* if (at least) one of the vectors can be expressed as a linear combination of the others. Otherwise, it is called *linearly independent.*

Basis and Dimension (1)

A spanning set that has minimum cardinality is called a **basis** for V.

Example. The set $\{1000, 0100, 0010, 0001\}$ is a (canonical) basis for V_2^4, where V_q^n denotes the set of q-ary n-tuples.

If a basis for a vector space V has k elements, then it is said to have **dimension** k, written $\dim(V) = k$.

Basis and Dimension (2)

Theorem 2-6. Let $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be a basis for a vector space V. For every vector $\mathbf{v} \in V$ there is a representation $\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$. This representation is unique.

Corollary. $|V| = |F|^k$.

A vector space V' is said to be a vector **subspace** of V if $V' \subseteq V$.

Inner Product and Dual Spaces

The inner product $\mathbf{u} \bullet \mathbf{v}$ of $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ is defined as

$$\mathbf{u} \bullet \mathbf{v} = \sum_{i=0}^{n-1} u_i \cdot v_i.$$

Let C be a k-dimensional subspace of a vector space V. The **dual space** of C, denoted by $C^{\perp}$, is the set of vectors $\mathbf{v} \in V$ such that for all $\mathbf{u} \in C$, $\mathbf{u} \bullet \mathbf{v} = 0$.

Theorem 2-8. The dual space $C^{\perp}$ of a vector subspace $C \subseteq V$ is itself a vector subspace of V.

The Dimension Theorem

Theorem 2-9. Let C be a vector subspace of V. Then $\dim(C) + \dim(C^{\perp}) = \dim(V)$.

Example. A code $C \subseteq V_2^4$: $C = \{0000, 0101, 0001, 0100\}$, $C^{\perp} = \{0000, 1010, 1000, 0010\}$. Then $\dim(C) + \dim(C^{\perp}) = 2{+}2 = 4 = \dim(V)$.

Question. What is the dual space $C^{\perp}$ when $C = V$?

Properties of Finite Fields (1)

With $\beta \in \mathrm{GF}(q)$ and 1 the multiplicative identity, consider the sequence

$$1, \beta, \beta^2, \ldots.$$

In a finite field, this sequence must begin to repeat at some point.

Question. Why must 1 be the first element to repeat?

The *order* of an element $\beta \in \mathrm{GF}(q)$, written $\mathrm{ord}(\beta)$, is the smallest positive integer m such that $\beta^m = 1$ (cf. order of group element).

Properties of Finite Fields (2)

Theorem 2-10. If $t = \mathrm{ord}(\beta)$, then $t \mid (q-1)$.

Proof: The set $\{\beta, \beta^2, \ldots, \beta^{\mathrm{ord}(\beta)} = 1\}$ forms a subgroup of the nonzero elements in $\mathrm{GF}(q)$ under multiplication. The result then follows from Lagrange's theorem (Theorem 2-4). $\square$

Example. The elements of the field $\mathrm{GF}(16)$ can only have orders in $\{1, 3, 5, 15\}$.

The Euler Totient Function

The **Euler** ϕ (or **totient**) **function**, $\phi(t)$, denotes the number of integers in $\{1, 2, \ldots, t-1\}$ that are *relatively prime* to t. This function can be computed as follows when $t > 1$ ($\phi(1) = 1$):

$$\phi(t) = t \prod_{p \mid t} \left(1 - \frac{1}{p}\right).$$

Example 1. $\phi(56) = \phi(2^3 \cdot 7) = 56(1 - 1/2)(1 - 1/7) = 24.$

Example 2. If t is a prime, then $\phi(t) = t(1 - 1/t) = t - 1$, as expected.

Primitive Elements in Finite Fields

▷ If $t \nmid (q-1)$, then there are no elements of order t in GF(q) (Theorem 2-10).

Theorem 2-12. If $t \mid (q-1)$, then there are $\phi(t)$ elements of order t in GF(q).

An element in GF(q) with order $(q-1)$ is called a **primitive element** in GF(q). There are $\phi(q-1)$ primitive elements in GF(q).

$\Rightarrow$ All nonzero elements in GF(q) can be represented as $(q-1)$ consecutive powers of a primitive element.

Example: GF(7)

Order i	Elements of order i	$\phi(i)$
1	$\{1\}$	1
2	$\{6\}$	1
3	$\{2, 4\}$	2
4	None	–
5	None	–
6	$\{3, 5\}$	2

For example, $5^1 = 5$, $5^2 = 4$, $5^3 = 6$, $5^4 = 2$, $5^5 = 3$, $5^6 = 1$.

Characteristic of Field

The **characteristic** of GF(q) is the smallest integer m such that $\underbrace{1 + 1 + \cdots + 1}_{m} = 0$.

Theorem 2-13. The characteristic of a finite field is a prime.

Theorem 2-14. The order of a finite field is a power of a prime.