Algebraic structures: from groups to fields

This course concentrates on *linear block codes*.

Codeword vectors are linear transforms of message vectors: $\mathbf{c} = \mathbf{m}G$.

- codeword $\mathbf{c}$ is an n-tuple
- message $\mathbf{m}$ is a k-tuple
- generator matrix G is a $k \times n$ matrix

The components of $\mathbf{c}, \mathbf{m}, G$ can be operated on using $+, -, \times, \div$.

The algebraic structures that we use in algebraic coding are, top down,

- vector space: codewords are vectors
- field: codeword symbols are field elements
- ring: matrices can be added and multiplied
- group: addition and multiplication are associative and invertible

Also important: polynomials and matrices with coefficients from a field.

Groups

Definition: A group is an algebraic structure $(G, \cdot)$ consisting of a set G with a single operator $\cdot$ satisfying the following axioms:

1. Closure: $a \cdot b$ belongs to G for every a, b in G.
2. Associative law: $(a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$.
3. Identity element: there exists e such that $e \cdot a = a \cdot e = a$.
4. Inverse: for every a there is a^{-1} such that $a^{-1} \cdot a = a \cdot a^{-1} = e$.

A group is *commutative* or *abelian* if $a \cdot b = b \cdot a$ for every a, b in G.

Familiar examples of groups:

- numbers (integer, rational, real, complex) with addition
- integers with addition modulo m (finite group)
- integers relatively prime to m with modulo m multiplication
- permutations of a finite set (not commutative)
- translations and rotations of the plane (not commutative)

Group examples

Numeric groups are usually commutative, permutation groups are not.

Smallest nonabelian group is S_3, set of $3! = 6$ permutations on 3 objects.

S_3 can be represented using 3×3 *permutation matrices*.

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\ \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix},\ \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix},\ \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix},\ \begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix},\ \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$$

Example of noncommutative product:

$$\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\cdot\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}\neq\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}\cdot\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}$$

Fact: every group is a subgroup of a permutation group.

Other representations of permutations: list of values $[3\,2\,4\,1]$ or product of cycles $(1\,3\,4)(2\,5)$.

Commutative groups are called “abelian” in honor of the Norwegian mathematician Niels Henrik Abel (1802–1829), who proved the impossibility of solving the quintic equation in radicals.

Group operation tables

Finite groups can be described by operation tables. Examples:

$\oplus$	0	1
0	0	1
1	1	0

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

?	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Above examples are arithmetic. Operation table for symmetric group S_3:

	$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$
$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$
$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$
$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$
$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$
$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$
$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right]$

Simple group properties

- The identity element is unique.

  Proof: If e_1 and e_2 are identity elements then

  $$e_1 = e_1 \cdot e_2 \quad \text{and} \quad e_1 \cdot e_2 = e_2 \implies e_2 = e_2$$

  The first equality holds because e_2 is a right identity; the second equality holds because e_1 is a left identity.

- Every element has a unique inverse.

  Proof: If b_1 and b_2 are inverses of a then

  $$b_1 = b_1 \cdot e = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = e \cdot b_2 = b_2$$

  One-line proof uses associativity and definition of right and left inverse.

- The inverse of $a \cdot b$ is $b^{-1} \cdot a^{-1}$.

  Proof: Use the associative law and the definition of inverse:

  $$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$$

Cancelation property

Invertibility of the group operation implies the *cancelation properties*:

$$ab = ac \implies b = c \quad \text{and} \quad ba = ca \implies b = c$$

Proof: Multiply both sides of the equality by a^{-1} on the left (or the right).

Just for fun, here's a "one-line" proof. If $ab = ac$ then

$$b = e \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) = (a^{-1} \cdot a) \cdot c = e \cdot c = c$$

By the cancelation property, there are no duplicate elements in any row or column of the operation table for a group.

Not every operation table without duplicates defines a group.

A *quasi-group* is a set with a binary operation that satisfies the cancelation property.

Quasi-groups may lack associativity, identity, and inverses; they are not interesting for algebra.

Finite groups

Definition: The number of elements of a finite group is called its *order*.

Fact: for every integer $n \geq 1$ there is at least one group of order n:

$$\mathrm{Z}/(n) \;=\; \{0, 1, \ldots, n-1\} \;=\; \text{integers with addition modulo } n$$

How do we show that the integers with modulo n addition form a group? The first three axioms are obviously satisfied:

1. Closure: $0 \leq (a+b) \bmod n \leq n-1$.
2. The identity element is 0, since $a+0=0+a=a$.
3. The additive inverse of a is $(n-a) \bmod n = \begin{cases} n-a & a>0 \\ 0 & a=0 \end{cases}$

Associativity follows from *Fundamental Lemma of Modular Computation*.

Lemma: Every integer formula containing only the operators $+, -, \times$ can be computed modulo n using modulo n reductions on any subexpressions.

Proof: by induction on the depth of the formula.

Subgroups

Definition: A *subgroup* of a group G is a subset H of G that is itself a group under the operation of G:

- H is closed under the operation of G.
- H contains the identity element.
- H contains the inverse of every element of H.

A *proper* subgroup is a subgroup other than $\{e\}$ and G.

Obviously, the number of elements in a proper subgroup H satisfies

$$1 < |H| < |G|,$$

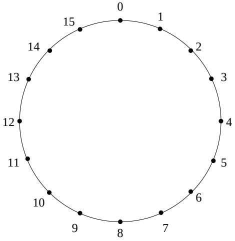
where $|S|$ denotes the number of elements in S. In fact, $|H|$ divides $|G|$.

Lagrange's theorem (proved later): the order of a (proper) subgroup is a (proper) divisor of $|G|$.

An elegant (but not quite correct) definition of subgroup: $a \cdot b^{-1} \in H$ for every a, b in H. The flaw in this definition: we must require that H be nonempty.

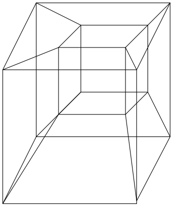
Subgroups: examples

Here are pictures of two of the five abelian groups of order 16.



$G_1 = \mathrm{Z}_{16} = \{0, 1, \ldots, 15\}$ with mod 16 addition.

G_1 has only one subgroup with 8 elements, the set of even integers $\{0, 2, \ldots, 14\}$.



$G_2 = \mathrm{Z}_2^4 = \{0, 1\}^4$, 4-bit vectors with bitwise XOR.

G_2 has many subgroups with 8 elements, e.g., $\{0\} \times \{0, 1\}^3$ and the set of binary 4-tuples with even parity.

The other groups of order 16 are $\mathrm{Z}_8 \times \mathrm{Z}_2$, $\mathrm{Z}_4 \times \mathrm{Z}_4$, and $\mathrm{Z}_4 \times \mathrm{Z}_2 \times \mathrm{Z}_2$

Subgroup generated by an element

The subgroup *generated by* a set $S \subseteq G$ is the smallest subgroup of G that contains all the elements of S. The subgroup generated by an element a is

$$e,\ a,\ a^{-1},\ a \cdot a = a^2,\ (a^{-1})^2 \stackrel{\Delta}{=} a^{-2},\ \ldots$$

and all other positive and negative powers of a, that is, $\{a^i : i \in \mathrm{Z}\}$.

In a *finite* group, some element of $\{e, a, a^2, a^3, \ldots\}$ appears twice. Suppose

$$a^i = a^{i+n}, \quad i \geq 0,\ n > 0$$

where i is the first such exponent and n is the smallest number for that i. Multiplying both sides by $a^{-i} = (a^i)^{-1}$ yields $e = a^n$. So the subgroup generated by a is $\{e, a, a^2, \ldots, a^{n-1}\}$.

If $0 \leq i, j < n - 1$ then $a^i \cdot (a^j)^{-1} = \begin{cases} a^{i-j} & \text{if } i \geq j \\ a^{i-j+n} & \text{if } i < j \end{cases}$

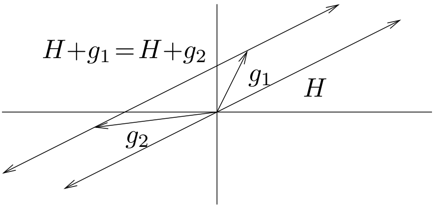
In other words, the subgroup generated by a "looks like" Z_n.

The *order* of a is the order of the subgroup generated by a.

Cosets

A subgroup H can be thought of as a smaller dimensional subspace of G.

H can be "translated" by adding a fixed g to every element of H.
These translates are called *cosets*.



Definition: a *left coset* of a subgroup H is

$$g \cdot H = \{g \cdot h : h \in H\}.$$

Similarly, a *right coset* is

$$H \cdot g = \{h \cdot g : h \in H\}.$$

In a noncommutative group, left and right cosets might be different,

Coset decomposition

Lemma: Every element of G belongs to exactly one coset of a subgroup H.

Proof: Consider left cosets; proof for right cosets is same.

Obviously $g = g \cdot e$ belongs to at least one coset — namely, $g \cdot H$.

We must show that distinct cosets are disjoint.
Suppose g is a common element of two cosets, $g_1 \cdot H$ and $g_2 \cdot H$. Then

$$g = g_1 \cdot h_1 = g_2 \cdot h_2 \,, \ \text{ where } \ h_1, h_2 \in H \,.$$

Therefore

$$g_1 = g_2 \cdot h_2 \cdot h_1^{-1}$$

and so for every h_3 in H,

$$g_1 \cdot h_3 = (g_2 \cdot h_2 \cdot h_1^{-1}) \cdot h_3 = g_2 \cdot (h_2 \cdot h_1^{-1} \cdot h_3) \in g_2 \cdot H \,.$$

This shows that every element of $g_1 \cdot H$ belongs to $g_2 \cdot H$, so $g_1 \cdot H \subseteq g_2 \cdot H$.

Similarly, $g_2 \cdot H \subseteq g_1 \cdot H$. Therefore overlapping cosets are identical.

Lagrange's theorem

By cancelation property, there is a 1-1 correspondence between H and $g \cdot H$.

Thus every coset has the same number of elements as the subgroup.

Since cosets are disjoint, for any finite group G and any subgroup H,

$$|G| = |H| \cdot (\text{number of cosets of } H)\,.$$

Lagrange's theorem: The order of any (proper) subgroup of a finite group is a (proper) divisor of the order of the group.

Corollary: A group of prime order has no proper subgroups.

Corollary: The order of any element is a divisor of the order of the group.

The converse of Lagrange's theorem is not true in general. Given a divisor d of $|G|$, there need not exist a subgroup of G of order d. The smallest example is the alternating group A_4, which has 12 elements but no subgroup of order 6. However, if G is abelian, then there always exists a subgroup of order d. A partial converse for the general case is given by Cauchy's theorem, which states that if p is a *prime* divisor of $|G|$, then G has an element of order p.

Rings

Definition: A ring is a set R with binary operations, $+$ and $\cdot$, that satisfy the following axioms:

1. $(R, +)$ is a commutative group (five axioms)
2. Associative law for multiplication: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Distributive laws:
   $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)\,, \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$
   (Two distributive laws are needed if multiplication is not commutative.)

Here is an example of an "obvious" property that holds for all rings.

Proposition: In any ring, $0 \cdot a = 0$.

Proof: By the distributive law,

$$0 \cdot a = (0 + 0) \cdot a \;=\; (0 \cdot a) + (0 \cdot a)$$

Subtracting $0 \cdot a$ from both sides of equation yields $0 = 0 \cdot a$.

Important rings

Several rings will be used in this course:

- integers $\mathrm{Z} = \{\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots\}$
- integers modulo m: $\mathrm{Z}_m = \{0, 1, \ldots, m-1\}$
- polynomials with coefficients from a field:
$$F[x] \;=\; \{\, f_0 + f_1 x + \cdots + f_n x^n : n \geq 0,\ f_i \in F\,\}$$
- polynomials over a field modulo a prime polynomial $p(x)$ of degree m
- the $n \times n$ matrices with coefficients from a field

Similarities and differences between the rings of integers and of binary polynomials.

Similarities:

- Elements can be represented by bit strings
- Multiplication by shift-and-add algorithms

Differences:

- Arithmetic for polynomials does not require carries
- Factoring binary polynomials is easy but factoring integers seems hard.

Rings with additional properties

By adding more requirements to rings, we ultimately arrive at fields.

- *Commutative ring*: $a \cdot b = b \cdot a$.

  The 2×2 matrices are a familiar example of a *noncommutative* ring:

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

  Some *subgroups* of 2×2 matrices are commutative. E.g., complex numbers:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

- *Ring with identity*: there is an element 1 such that $1 \cdot a = a \cdot 1 = a$.

  Ring without identity: even integers $2\mathrm{Z} = \{\ldots, -4, -2, 0, +2, +4, \ldots\}$.

  If it exists, an identity is unique.

  Proof: $1_1 = 1_1 \cdot 1_2 = 1_2$. (Same as proof for groups.)