ECE 7670
Lecture 3 – Groups, rings, fields, and Galois fields

Objective: To become acquainted with some basic algebraic concepts.

1 Groups

A **group** formalizes some of the basic rules of arithmetic necessary for cancellation and solution of some algebraic equations.

Definition 1 A **group** $(G, *)$ is a set G together with a (closed) binary operation $*$ on G such that:

- (G1) The operator is associative.
- (G2) There is an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$. Such an element is the *identity element*
- (G3)For every $a \in G$, there is an element $b \in G$ such that $a * b = e$. This b is said to be the inverse of a with respect to $*$. The inverse of a is sometimes denoted as a^{-1}.

Where the operation is clear from context, the group $(G, *)$ may be denoted simply as G.

It should be noted that the notation $*$ and a^{-1} are generic labels to indicate the concept. The particular notation used is modified to fit the concept. Where the group operation is addition, the operator $+$ is used and the inverse of an element a is more commonly represented as $-a$. When the group operation is multiplication, either $\cdot$ or juxtaposition is used to indicate the operation and the inverse is denoted as a^{-1}.

Definition 2 If G has a finite number of elements, it is said to be a finite group. The **order** of a finite group G, denoted $|G|$, is the number of elements in G. □

This definition of order (of a group) is to be distinguished from the order of an element, given below. □

Example 1 The set $(\mathbb{Z}, +)$, which is the set of integers under addition, forms a group. The identity element is 0, since $0 + a = a + 0 = a$ for any $a \in \mathbb{Z}$. The inverse of any $a \in \mathbb{Z}$ is $-a$. □

As a matter of convention, a group that is commutative with an additive operator is said to be an **abelian** group (after N.H. Abel).

We now present several examples illustrating groups arising in a variety of contexts.

Example 2 The set $(\mathbb{Z}, \cdot)$, the set of integers under multiplication, does *not* form a group. There is a multiplicative identity, 1, but there is no multiplicative inverse for every element in $\mathbb{Z}$. □

Example 3 The set $(\mathbb{Q}\backslash\{0\}, \cdot)$, the set of rational numbers excluding 0, is a group with identity element 1. The inverse of an element a is $1/a$. □

The requirements on a group are strong enough to introduce the idea of cancellation. In a group G, if $a * b = a * c$, then $b = c$ (this is left cancellation). To see this, let a^{-1} be the inverse of a in G. Then

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

from which it is immediate, using associativity and the operation of the identity that $b = c$.

Under group requirements, we can also verify that solutions to linear equations of the form $a * x = b$ are unique. Using the group properties we get immediately that $x = a^{-1}b$. If x_1 and x_2 are two solutions, such that $a * x_1 = b = a * x_2$, then by cancellation we get immediately that $x_1 = x_2$.

Example 4 Let $\langle \mathbb{Z}_5, + \rangle$ denote addition on the numbers $\{0, 1, 2, 3, 4\}$ modulo 5. The operation is demonstrated in tabular form in the table below:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Clearly 0 is the identity element. Since 0 appears in each row and column, every element has an inverse. By the uniqueness of solution, we must have every element appearing in every row and column, as it does. Thus we verify that $\langle \mathbb{Z}_6, + \rangle$ is a group. □

In general we will denote by $\langle \mathbb{Z}_n, + \rangle$ the set of numbers $0, 1, \ldots, n-1$ with addition modulo n.

Example 5 Consider the set of numbers $\{1, 2, 3, 4, 5\}$ using the operation of multiplication modulo 6. The operation is shown in the following table:

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

The number 1 acts as an identity, but this does not form a group, since not every element has a multiplicative inverse. In fact, the only elements that have a multiplicative inverse are those that are relatively prime to 6, i.e., those numbers that don't share a divisor with 6 other than one. We will see this example later in the context of rings. □

Example 6 The group $\langle \mathbb{Z}_2 \times \mathbb{Z}_2, + \rangle$ consists of two-tuples with addition defined element-by-element modulo two. An addition for the group table is shown here:

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

□

Example 7 This example introduces the idea of *permutations* as elements in a group, and is interesting because it introduces a group operation that is function composition, as opposed to the mostly arithmetic group operations presented to this point. It is also interesting because permutations arise in a variety of contexts such as bit-reverse shuffling.

A permutation of a set A is a function one-to-one onto function (a bijection) of a set A onto itself. It is convenient for purposes of illustration to let A be a set of

n integers. For example,

$$A = \{1, 2, 3, 4\}.$$

A permutation $_p$ can be written in the notation

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

which means that

$$1 \rightarrow 3 \qquad 2 \rightarrow 4 \qquad 3 \rightarrow 1 \; 4 \rightarrow 2$$

We can think of p_1 as an operator, expressed in postfix notation. For example

$$1p_1 = 3 \qquad \text{or} \qquad 4p_1 = 2.$$

Let

$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

The *composition* permutation $p_1 p_2$ first applies p_1, then p_2, so that

$$p_1 p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

This is again another permutation, so the operation of composition of permutations is closed under the set of permutations. The identity permutation is

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

There is an inverse permutation under composition. For example,

$$p_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

It can be shown that composition of permutations is associative: for three permutations p_1, p_2 and p_3, then $(p_1 p_2)p_3 = p_1(p_2 p_3)$. Thus the set of all permutations on n elements (in our example $n = 4$ forms a group. This group is referred to as the symmetric group on n letters. The group is commonly denoted by S_n.

It is also interesting to note that the composition is *not* commutative. This is clear from this example since

$$p_2 p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \neq p_1 p_2$$

So S_4 is an example of a non-commutative group. □

1.1 Subgroups

A subgroup H is simply a group formed from a subset of elements in a group G with the same operation. If the elements of H are a strict subset of the elements of G, then the subgroup is said to be a **proper** subgroup. If $H = G$, then H is an improper subgroup of G. Notationally, we may write $H < G$ to indicate that H is a proper subgroup of G. (There should be no confusion using $<$ with comparisons between numbers because the operands are different in each case.)