

## 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**  $\langle G, * \rangle$  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  $\langle G, * \rangle$  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  $G$ .  $\square$

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

**Example 1** The set  $\langle \mathbb{Z}, + \rangle$ , 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  $-a$ .  $\square$

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  $\langle \mathbb{Z}, \cdot \rangle$ , 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  $\mathbb{Z}$ .  $\square$

**Example 3** The set  $\langle \mathbb{Q} \setminus \{0\}, \cdot \rangle$ , the set of rational numbers excluding 0, is a group with identity element 1. The inverse of an element  $a$  is  $1/a$ .  $\square$

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  $\langle \mathbb{Z}_5, + \rangle$  is a group.  $\square$

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

**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)

$\square$

**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

$$1 \rightarrow 3 \quad 2 \rightarrow 4 \quad 3 \rightarrow 1 \quad 4 \rightarrow 2$$

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

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

Let

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

The *composition* permutation  $p_1p_2$  first applies  $p_1$ , then  $p_2$ , so that

$$p_1p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

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  $(p_1p_2)p_3 = p_1(p_2p_3)$ . 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

$$p_2p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \neq p_1p_2$$

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

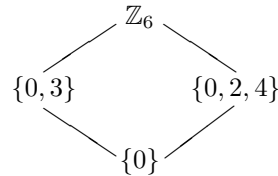
## 1.1 Subgroups

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.)

**Example 8** Let  $G = \langle \mathbb{Z}_6, + \rangle$ , the set of numbers  $\{0, 1, 2, 3, 4, 5\}$  using addition modulo 6. It is straightforward to verify that this forms a group. Let  $H = \langle \{0, 2, 4\}, + \rangle$ , with addition taken modulo 6. As a set,  $H \subset G$ , and it can be shown that  $H$  forms a group.

Let  $K = \langle \{0, 3\}, + \rangle$ , with addition taken modulo 6. Then  $K$  is a subgroup of  $G$ . □

It is sometimes useful to keep track of subgroup structure using a *lattice* diagram. A lattice diagram for the last example is shown here:



**Example 9** A variety of familiar groups can be arranged as subgroups. For example,

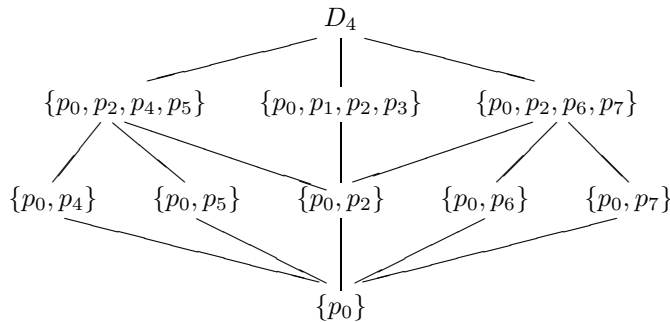
$$\langle \mathbb{Z}, + \rangle < \langle \mathbb{Q}, + \rangle < \langle \mathbb{R}, + \rangle < \langle \mathbb{C}, + \rangle.$$

□

**Example 10** The group of permutations on 4 letters,  $S_4$  has a subgroup formed by the permutations

$$\begin{aligned}
 p_0 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & p_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\
 p_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & p_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\
 p_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} & p_5 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\
 p_6 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} & p_7 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}
 \end{aligned} \tag{1}$$

It can be verified that compositions of these permutations is closed. These permutations correspond to the ways that the corners of a square can be made to correspond with each other by rotation and reflection about an axis (without bending the square). This group is known as  $D_4$ . Considered as a group,  $D_4$  itself has a variety of subgroups, with a lattice diagram as follows:



□

## 1.2 Cyclic groups; order of an element

In a group  $G$  with operation  $*$  we will use the notation  $a^n$  to indicate  $a*a*a*\dots*a$ , with the operand  $a$  appearing  $n$  times. Thus  $a^1 = a$ ,  $a^2 = a*a$ , etc., and we will take  $a^0$  to be the identity element in the group  $G$ . We will use  $a^{-2}$  to indicate  $(a^{-1})(a^{-1})$ , and  $a^{-n}$  to indicate  $(a^{-1})^n$ .

For a group with an additive operator  $+$ , the notation  $na$  is often used, which means  $a+a+a+\dots+a$ , with the operand appearing  $n$  times. Throughout this section we will use the  $a^n$  notation; making the switch for additive operator notation is straightforward.

Let  $G$  be a group, and let  $a \in G$ . Any subgroup containing  $a$  must (by closure) also contain  $a^2, a^3$ , and so forth. The subgroup must contain  $e = aa^{-1}$ , and hence  $a^{-2}, a^{-3}$ , and so forth. In fact, for any  $a \in G$ , the set  $\{a^n | n \in \mathbb{Z}\}$  generates a subgroup  $H$  of  $G$ . This subgroup is said to be a **cyclic subgroup**, and  $a$  is said to be the **generator** of the subgroup. The cyclic subgroup is denoted as  $\langle a \rangle$ .

If every element of a group can be generated by a single element, the group is said to be cyclic. For example, the group  $\langle \mathbb{Z}_5, + \rangle$  is cyclic, since every element in the set can be generated by  $a = 2$  (under the appropriate addition law):

$$2, 2+2=4, 2+2+2=1, 2+2+2+2=3, 2+2+2+2+2=0.$$

In this case we could write  $\mathbb{Z} = \langle 2 \rangle$ . Observe that there are several generators for  $\mathbb{Z}_5$ . The permutation group  $S_3$  is not cyclic: there is no element which generates the whole group.

**Definition 3** In a group  $G$ , with  $a \in G$ , the smallest  $n$  such that  $a^n$  is equal to the identity in  $G$  is said to be the **order** of  $a$ . If no such  $n$  exists,  $a$  is of **infinite order**.  $\square$

The order of an element should not be confused with the order of a group, which is the number of elements in the group.

In  $\mathbb{Z}_5$ , the computations above show that the element 2 is of order 5. In fact, the order of every nonzero element in  $\mathbb{Z}_5$  is 5.

**Example 11** Let  $G = \langle \mathbb{Z}_6, + \rangle$ . Then

$$\langle 2 \rangle = \{0, 2, 4\} \quad \langle 3 \rangle = \{0, 3\} \quad \langle 5 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6.$$

It is easy to verify that an element  $a \in \mathbb{Z}_6$  is a generator for the whole group if and only if  $a$  and 6 are relatively prime.  $\square$

## 1.3 Cosets

We begin with an example.

**Example 12** Let  $G = \mathbb{Z}$  under addition, and let

$$S_0 = 3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\} \quad S_1 = 3\mathbb{Z} + 1 = \{\dots, -5, -2, 0, 1, 4, 7, \dots\}$$

$$S_2 = 3\mathbb{Z} + 2 = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

and define addition on  $S = \{S_0, S_1, S_2\}$  as follows: for  $A, B$  and  $C \in S$ ,

$$A + B = C \quad \text{if and only if } a + b = c \text{ for some } a \in A, b \in B \text{ and } c \in C.$$

That is, addition of the sets is defined by representatives in the sets. For example,  $S_2 + S_2 = S_1$ . An addition table can be established based on these rules. Based on the addition table, it is straightforward to verify that

$$S \sim \mathbb{Z}_3,$$

under addition.  $\square$

Example 12 leads us to the next important concept in group theory, cosets. From that example, we have

$$S_0 = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

the multiples of three. Note that under  $+$ , the elements of  $S_0$  form a subgroup of  $\langle \mathbb{Z}, + \rangle$ . The set  $S_1$  can be written as

$$S_1 = 1 + S_0.$$

Since there is no identity element under  $+$  this set does not form a group. Notice that every element in  $S_1$  is distinct from every element in  $S_0$ . The set  $S_2$  can be written as

$$S_2 = 2 + S_0,$$

which also does not form a group. The groups  $S_0, S_1$ , and  $S_2$  collectively cover the original group  $\mathbb{Z}$ :

$$\mathbb{Z} = S_0 \cup S_1 \cup S_2.$$

The sets  $S_1$  and  $S_2$  are said to be **cosets** of the subgroup  $S_0$ .

**Definition 4** Let  $H$  be a subgroup of  $\langle G, * \rangle$ , where  $G$  is not necessarily commutative, and let  $a \in G$ . The **left coset**  $a * H$  is the set  $\{a * h | h \in H\}$ . The right coset is similarly defined.  $\square$

Let  $G$  be a group and let  $H$  be a subgroup of  $G$ . Let  $a * H$  be a (left) coset of  $G$ . Then clearly  $b \in a * H$  if and only if  $b = a * h$  for some  $h \in H$ . This means (by cancellation) that we must have

$$a^{-1} * b \in H$$

Thus, to determine if  $a$  and  $b$  are in the same (left) coset, we determine if  $a^{-1} * b \in H$ .

**Example 13** For the cosets defined in example 12, let  $a = 4$  and  $b = 6$ . Then (since the operation is  $+$ ), we check whether  $(-a) + b = inS_0$ . However,  $-a + b = 2 \notin S_0$ , so  $a$  and  $b$  are not in the same coset.  $\square$

We can define a relation by saying  $a \sim b$  if and only if  $a$  and  $b$  are in the same (left) coset. That is,

$$a \sim b \text{ if and only if } a^{-1} * b \in H.$$

As the following lemmas demonstrate,  $G$  is partitioned into disjoint cosets of equal size.

**Lemma 1** *Every coset of  $H$  in a group  $G$  have the same number of elements.*

**Proof** We will show that every coset has the same number of elements as  $H$ . Let  $a * h_1 \in a * H$  and let  $a * h_2 \in a * H$  be two elements in the coset  $a * H$ . If  $a * h_1 = a * h_2$  then by cancellation we must have  $h_1 = h_2$ . Thus the elements of a coset are uniquely identified by the elements in  $H$ .  $\square$

**Lemma 2** *The relation “in the same coset” is transitive. That is, if  $a$  and  $b$  are in the same coset of  $H$ , and  $b$  and  $c$  are in the same coset of  $H$ , then  $a$  and  $c$  are in the same coset of  $H$ .*

**Proof** If  $a$  and  $b$  are in the same coset, then  $a^{-1} * b \in H$ , and if  $b$  and  $c$  are in the same coset, then  $b^{-1} * c \in H$ . Then

$$(a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H,$$

since the product of the two elements in  $H$  on the left must be in  $H$ .  $\square$

We summarize some important (and obvious) properties:

1. An element  $a$  is in the same coset as itself (reflexive)
2. If  $a$  and  $b$  are in the same coset, then  $b$  and  $a$  are in the same coset (symmetric)
3. If  $a$  and  $b$  are in the same coset, and  $b$  and  $c$  are in the same coset, then  $a$  and  $c$  are in the same coset (transitive).

A relationship which satisfies these three properties is said to be an *equivalence relation*. Every equivalence relation partitions its elements into *disjoint* sets. Let us consider our case, and show that all cosets are disjoint. Let  $A$  and  $B$  be two cosets. Then if  $A$  and  $B$  are not disjoint, then there is some element  $a$  which is common to both. But for every element  $c \in B$  which is in the same coset as  $A$ , that element must also be in  $A$ , thus  $A \subset B$ . The reverse also holds, so that  $B \subset A$ , so that  $A = B$ .

The following lemma will be of considerable use to us:

**Lemma 3 (Lagrange)** *Let  $G$  be a group of finite order  $n$ , and let  $H$  be a subgroup of  $G$ . Then the order of  $H$  divides the order of  $G$ .*

**Proof** Every coset of  $H$  in  $G$  has the same number of elements, which is the number of elements in  $H$ . Furthermore, every element of  $G$  is in some coset.  $\square$

**Lemma 4** *Every group of prime order is cyclic.*

**Proof** Let  $G$  be of prime order, let  $a \in G$ , and denote the identity in  $G$  by  $e$ . Let  $H = \langle a \rangle$ , the cyclic subgroup generated by  $a$ . Then  $a \in H$  and  $e \in H$ . But by lemma 3, the order of  $H$  must divide the order of  $G$ . Since  $G$  is of prime order, then we must have  $|H| = |G|$ ; hence  $a$  generates  $G$ , and  $G$  is cyclic.  $\square$

Let us continue our examination of the sets defined in example 12. In that example, we defined an operation on the cosets  $S_0, S_1$ , and  $S_2$  on the basis of what that operation does to elements of the coset. On this basis,

$$S_1 + S_1 = S_2,$$

since, for example,

$$1 + 4 = 5,$$

and  $1 \in S_1$ ,  $2 \in S_1$ , and  $5 \in S_2$ . The operation is said to be the induced operation on the cosets. More formally, we have the following.

**Definition 5** Let  $\langle G, * \rangle$  be a group,  $H$  a subgroup, and  $S = \{H_0 = H, H_1, H_2, \dots, H_M\}$  be the set cosets of  $H$  in  $G$ . Then the operation between cosets  $A$  and  $B$  in  $S$  is defined by

$$A * B = C \text{ if and only if } a * b = c$$

for some  $a \in A$ ,  $b \in B$  and  $c \in C$  is the *induced operation* on the cosets, provided that this operation is well defined.  $\square$

For commutative groups, the induced operation is well defined. Since groups employed in signal processing applications are frequently commutative, we will restrict our attention to this case. However, the reader should be cautioned that what follows does not fully generalize to noncommutative groups (the subgroups must be normal subgroups).

The induced operation provides a means of defining operations between cosets. Another example may clarify this.

**Example 14** Consider the group  $G = \langle \mathbb{Z}_6, + \rangle$ , and let  $H = \{0, 3\}$ . The cosets of  $H$  are

$$H_0 = \{0, 3\} \quad H_1 = 1 + H = \{1, 4\} \quad H_2 = 2 + H = \{2, 5\}$$

Then, for example,  $H_2 + H_2 = H_1$  since  $2 + 2 = 4$ , and  $4 \in H_1$ . We could also choose different representatives from the cosets. We get

$$5 + 5 = 4$$

in  $G$ . Since  $5 \in H_2$  and  $2 \in H_1$ , we again have  $H_2 + H_2 = H_1$ . (If, by choosing different elements from the addend cosets in the sum were to end up with different a different sum coset, the operation would not be well defined.) Let us write the addition table for  $\mathbb{Z}_6$  reordered and separated out by the cosets. The induced operation is clear, and we observe that  $H_0, H_1$  and  $H_2$  themselves constitute a group, with addition table also shown.

		$H_0$		$H_1$		$H_2$	
	$+$	0	3	1	4	2	5
$H_0$	0	0	3	1	4	2	5
$H_0$	3	3	0	4	1	5	2
$H_1$	1	1	4	2	5	3	0
$H_1$	4	4	1	5	2	0	3
$H_2$	2	2	5	3	0	4	1
$H_2$	5	5	3	0	3	2	4

	$+$	$H_0$	$H_1$	$H_2$
$H_0$	$H_0$	$H_1$	$H_2$	
$H_1$	$H_1$	$H_2$	$H_0$	
$H_2$	$H_2$	$H_0$	$H_1$	

The group of cosets is clearly isomorphic to  $\langle \mathbb{Z}_3, + \rangle$ . □

From this example, the cosets themselves form a group. The group formed by the cosets of  $H$  in a group (commutative)  $G$  is said to be the **factor group** of  $G$  modulo  $H$ , denoted by  $G/H$ . The cosets are said to be the **residue classes** of  $G$  modulo  $H$ .

In the last example, we could write  $\mathbb{Z}_3 \sim \mathbb{Z}_6/\mathbb{Z}_3$ . From example 12, the group of cosets was also isomorphic to  $\mathbb{Z}_3$ , and so we can write

$$\mathbb{Z}/3\mathbb{Z} \sim \mathbb{Z}_3.$$

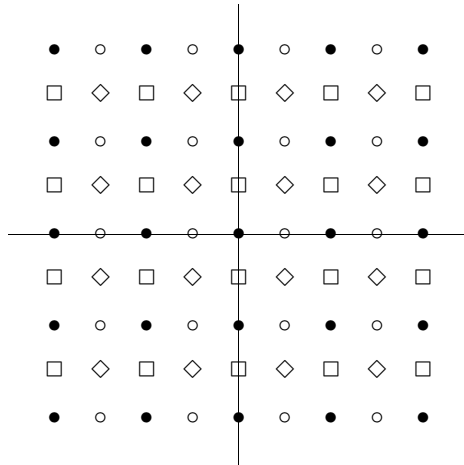
In general it can be shown that

$$\mathbb{Z}/n\mathbb{Z} \sim \mathbb{Z}_n.$$

**Example 15** For the lattice  $\Lambda = \mathbb{Z}^2$ , let  $\Lambda' = 2\mathbb{Z}^2$  be a subgroup. Then the cosets

$$\begin{aligned} S_0 &= \Lambda' (\bullet) & S_1 &= (1, 0) + \Lambda' (\circ) \\ S_2 &= (0, 1) + \Lambda' (\square) & S_3 &= (1, 1) + \Lambda' (\diamond) \end{aligned}$$

are indicated in the following diagram.



It is straightforward to verify that

$$\Lambda/\Lambda' \sim \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

## 2 Rings

Despite their usefulness in a variety of areas, groups are still limited because they have only one operation associated with them. The next algebraic category to work with is a ring.

**Definition 6** A ring  $\langle R, +, \cdot \rangle$  is a set  $R$  with two binary operations  $+$  and  $\cdot$  defined on  $R$  such that:

1.  $\langle R, + \rangle$  is an abelian (commutative) group.
2. The multiplication operation is associative.
3. The left and right distributive laws hold:

$$a(b + c) = ab + ac$$

$$(a + b)c = (ac) + (bc)$$

□

Notice that we do not require that the multiplication operation form a group: there may not be multiplicative inverses in a ring.

**Example 16** The set of  $2 \times 2$  matrices under usual definitions of addition and multiplication form a ring. □

**Example 17**  $\langle \mathbb{Z}_6, +, \cdot \rangle$  forms a ring. Recall that multiplication under  $\mathbb{Z}_6$  does *not* form a group. But  $\mathbb{Z}_6$  still satisfies the requirements to be a ring. □

**Definition 7** In a ring let  $a \in R$ ,  $R$  a ring and let  $na$  denote  $a + a + \dots + a$  with  $n$  arguments. If a positive integer exists such that  $na = 0$  for all  $a \in R$ , then the smallest such positive integer is the **characteristic of the ring**  $R$ . If no such positive integer exists, the  $R$  is of characteristic 0. □

**Example 18** In the ring  $\mathbb{Z}_6$ , the characteristic is 6. In general, in the ring  $\mathbb{Z}_n$ , the characteristic is  $n$ . In the ring  $\mathbb{Q}$ , the characteristic is 0. □

## 2.1 Rings of polynomials

Let  $R$  be a ring. A polynomial  $f(x)$  of degree  $n$  with coefficients in  $R$  is

$$f(x) = \sum_{i=0}^n a_i x^i$$

where  $a_i \neq 0$ . The symbol  $x$  is said to be an *indeterminate*. If the coefficient of the highest power of  $x$  is equal to 1, the polynomial is said to be **monic**. The set of all polynomials with an indeterminate  $x$  with coefficients in a ring  $R$  is denoted as  $R[x]$ .

**Example 19** Let  $R = \langle \mathbb{Z}_6, +, \cdot \rangle$ , and let  $S = R[x] = \mathbb{Z}_6[x]$ . Then some elements in  $S$  are: 0, 1,  $x$ ,  $1+x$ ,  $4+2x$ ,  $5+4x$ , etc. Example operations are

$$(4 + 2x) + (5 + 4x) = 3$$

$$(4 + 2x)(5 + 4x) = 2 + 2x + 2x^2.$$

□

**Example 20**  $\mathbb{Z}_2[x]$  is the ring of polynomials with coefficients that are either 0 or 1; it is appropriate for a variety of applications in digital systems, where 0 represents, for example, no connection, and 1 represents a connection. As an example of arithmetic in this ring, note that

$$(1 + x)(1 + x) = 1 + x^2$$

□

It is clear that polynomial multiplication does not, in general, have an inverse. For example, in the ring of polynomials with real coefficients  $\mathbb{R}[x]$ , there is no polynomial solution  $f(x)$  to

$$f(x)(x^2 + 3x + 1) = x^3 + 2x + 1$$

One reason polynomials are of interest in signal processing is that polynomial multiplication is equivalent to convolution. The convolution of the sequence

$$\mathbf{a} = \{a_0, a_1, a_2, \dots, a_n\}$$

with the sequence

$$\mathbf{b} = \{b_0, b_1, b_2, \dots, b_m\}$$

can be accomplished by forming the polynomials

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$b(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$$

and multiplying them

$$c(x) = a(x)b(x).$$

Then the coefficients of

$$c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n+m}x^{n+m}$$

are equal to the values obtained by convolving  $\mathbf{a} * \mathbf{b}$ .

In addition to the representing the arithmetic operations on sequences, polynomials can be used to represent a shift data. For the sequence

$$\mathbf{a} = \{a_0, a_1, \dots, a_n\}$$

a shifted version of the data, represented by the operator  $\sigma \mathbf{a}$  is

$$\sigma \mathbf{a} = \{0, a_0, a_1, \dots, a_n\}.$$

This shift can be represented using polynomials as a multiplication by  $x$ . If  $a(x)$  is the polynomial representing  $\mathbf{a}$ , then  $xa(x)$  is the polynomial representing  $\sigma \mathbf{a}$ .

Just as it is possible to define addition and multiplication modulo a number (as in  $\mathbb{Z}_5$  or  $\mathbb{Z}_2$ ), it is also possible to define multiplication modulo a polynomial. To clarify, if we write  $p(x) \pmod{q(x)}$ , what is commonly meant is to divide  $p(x)$  by  $q(x)$  and to take the remainder using conventional polynomial long division. Thus in  $\mathbb{R}[x]$ ,

$$x^2 + 3x + 2 \pmod{x + 2} = 0$$

since there is no remainder, and

$$x^2 + 3x + 4 \pmod{x + 4} = -x + 4.$$

Cyclic convolution can also be represented using polynomial multiplication. Cyclic convolution on  $n$  points is equivalent to multiplication of polynomials modulo  $x^n - 1$ . We will denote the  $n$ -point cyclic convolution of the sequence  $\mathbf{a}$  with the sequence  $\mathbf{b}$  as  $\mathbf{a} \otimes \mathbf{b}$  or, to emphasize the length,  $\mathbf{a} \otimes_n \mathbf{b}$ .

**Example 21** The 5-point cyclic convolution of  $\mathbf{a} = \{1, 1, 2\}$  and  $\mathbf{b} = \{2, 0, 0, 4\}$  can be computed using

$$c(x) = a(x)b(x) \pmod{x^5 - 1} = 10 + 2x + 4x^2 + 4x^3 + 4x^4.$$

where  $a(x) = 1 + x + 2x^2 + 3x^3$  and  $b(x) = 2 + 4x^3$ . Thus

$$\mathbf{a} \otimes \mathbf{b} = \{10, 2, 4, 4, 4\}$$

MATLAB warning: in MATLAB, make sure that the polynomial coefficients are in correct order, highest degree to lowest degree.  $\square$

It may be observed that a cyclic shift (wrap around shift) on the data can be accomplished using multiplication modulo a polynomial. Let the  $n$ -cyclic shift on the sequence

$$\{a_0, a_1, \dots, a_{n-1}\}$$

be defined by

$$\sigma_n \{a_0, a_1, \dots, a_{n-1}\} = \{a_{n-1}, a_0, a_1, \dots, a_{n-2}\}$$

This can be represented using polynomials as  $xa(x) \pmod{()x^n - 1}$ .

**Example 22** Let  $\mathbf{a} = \{1, 2, 3, 4, 5\}$ , and do a 5-cyclic shift on it:

$$\sigma_5 \mathbf{a} = \{5, 1, 2, 3, 4\}.$$

Using polynomials,  $a(x) = 1 + 2x + 3x^2 + 4x^3 + 5x^4$ , and  $xa(x) \pmod{x^5 - 1} = 5 + x + 2x^2 + 3x^3 + 4x^4$ .  $\square$

### 3 Fields

In a ring, not every element has a multiplicative inverse. In a field, the familiar arithmetic operations that take place in the usual real numbers are all available.

**Definition 8** A **field**  $\langle F, +, \cdot \rangle$  is a set  $F$  with two binary operations  $+$  and  $\cdot$  defined on  $F$  such that:

1.  $\langle F, + \rangle$  is an abelian group. (Denote by  $0$  the additive identity element.)
2. The set  $F \setminus \{0\}$  (the set  $F$  with the additive identity removed) forms a **commutative** group under  $\cdot$ . (Denote by  $1$  the multiplicative identity element.)
3. The operations  $+$  and  $\cdot$  distribute.

□

In comparing a field with a ring, we see that:

1. In a field, the elements except the additive identity form a group, whereas in a ring, there may not even be a multiplicative identity, let alone an inverse for every element.
2. The multiplicative group is in fact a commutative group.

Since they are inclusive, every field is a ring, but not every ring is a field.

**Example 23** The rational numbers  $\mathbb{Q}$  form a field. So do the real number  $\mathbb{R}$  and the complex numbers  $\mathbb{C}$ . □

**Example 24**  $\langle \mathbb{Z}_5, +, \cdot \rangle$  forms a field; every nonzero element has a multiplicative inverse. So this set forms not only a ring but also a group. Since this field has only a finite number of elements in it, it is said to be a **finite field**.

However,  $\langle \mathbb{Z}_6, +, \cdot \rangle$  does not form a field, since not every element has a multiplicative inverse. □

In a variety of signal processing applications, finite fields are employed as the basis for computation. One way to obtain finite fields is described in the following.

**Theorem 5** *The ring  $\langle \mathbb{Z}_p, +, \cdot \rangle$  is a field if and only if  $p$  is a prime.*

Before proving this, we need the following definition and lemma.

**Definition 9** In a ring  $R$ , if  $a, b \in R$  with both  $a$  and  $b$  not equal to zero but  $ab = 0$ , then  $a$  and  $b$  are said to be **zero divisors**. □

**Lemma 6** *In a ring  $\mathbb{Z}_n$ , the zero divisors are precisely those elements that are not relatively prime to  $n$ .*

**Proof** Let  $a \in \mathbb{Z}_n$  with  $a \neq 0$ , and let  $d$  be the greatest common divisor of  $n$  and  $a$ . (If the greatest common divisor equals 1, then  $a$  and  $n$  are relatively prime.) Then

$$a(n/d) = (a/d)n$$

which, being a multiple of  $n$ , is equal to 0 in  $\mathbb{Z}_n$ .

Conversely, suppose there is an  $a \in \mathbb{Z}_n$  relatively prime to  $n$  such that  $ab = 0$ . Then it must be the case that

$$ab = kn$$

for some integer  $k$ . Since  $n$  has no factors in common with  $a$ , then it must divide  $b$ , which means that  $b = 0$  in  $\mathbb{Z}_n$ . □

Observe from this theory that if  $p$  is a prime, there are *no* divisors of 0 in  $\mathbb{Z}_p$ . We now turn to the proof of theorem 5.

**Proof** We have already established that  $\langle \mathbb{Z}_p, + \rangle$  is a group. The key remaining requirement is to establish that  $\mathbb{Z}_p \setminus \{0\}$  forms a group. The multiplicative identity is 1 and multiplication is commutative. The key remaining requirement is to establish that every nonzero element in  $\mathbb{Z}_p$  has a multiplicative inverse.

Let  $1, 2, \dots, p-1$  be a list of the nonzero elements in  $\mathbb{Z}_p$ , and let  $a \in \mathbb{Z}_p$  be nonzero. Form the list

$$\{1a, 2a, \dots, (p-1)a\} \quad (2)$$

Every element in this list is distinct, since if any two were identical, say  $ma = na$  with  $m \neq n$ . Then  $a(m-n) = 0$ , which is impossible since there are no zero divisors in  $\mathbb{Z}_p$ . Since 1 is in the original list, it must appear in the list in (2).  $\square$

## 4 Vector spaces

The basic operations of vector spaces should be familiar. We review some definitions here.

**Definition 10** Let  $F$  be a field. Let  $V$  be a set of elements called **vectors**. Let the addition operation  $+$  be defined such that  $\mathbf{v}, \mathbf{w} \in V$  implies that

$$\mathbf{v} + \mathbf{w} \in V$$

(closed under addition). Let a scalar multiplication  $\cdot$  be defined such that for every  $a \in F$  and  $\mathbf{v} \in V$ ,  $a \cdot \mathbf{v} \in V$ . Then  $V$  forms a vector space over  $F$  if:

1.  $V$  forms a commutative group under  $+$ .
2. The operations  $+$  and  $\cdot$  distribute:

$$a \cdot (\mathbf{v} + \mathbf{w}) = a \cdot \mathbf{v} + a \cdot \mathbf{w}$$

and

$$(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$$

3. Associative:  $(a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$
4. The identity in  $F$  is an identity for the scalar product.

The field  $F$  is commonly called the scalar field or ground field of  $V$ .  $\square$

One way to make a vector space is to form  $n$ -tuples of elements from the ground field, i.e.  $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ , with addition and scalar multiplication defined component-by-component.

**Definition 11** A set of vectors  $G = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$  is a **spanning set** if every vector in  $V$  can be expressed as a linear combination of the vectors in  $G$ .

A spanning set of minimal cardinality is called a **basis** for  $V$ .

The number of elements in a basis is called the **dimension** of  $V$ .  $\square$

The representation of a vector  $\mathbf{v}$  in terms of basis vectors is unique. Suppose there are two representations, so we can write

$$\mathbf{v} = a_0 \mathbf{v}_0 + a_1 \mathbf{v}_1 + \dots + a_{k-1} \mathbf{v}_{k-1}$$

and

$$\mathbf{v} = b_0\mathbf{v}_0 + b_1\mathbf{v}_1 + \cdots + b_{k-1}\mathbf{v}_{k-1}$$

Then we have

$$(a_0 - b_0)\mathbf{v}_0 + (a_1 - b_1)\mathbf{v}_1 + \cdots + (a_{k-1} - b_{k-1})\mathbf{v}_{k-1} = 0,$$

where  $a_i - b_i \neq 0$  for at least some  $i$ . But this cannot be, because the  $\mathbf{v}_i$  are linearly independent.

We can define an **inner product** between two vectors as

$$\mathbf{v} \cdot \mathbf{w} = \sum_{i=1}^{n-1} v_i w_i.$$

The inner product satisfies commutativity (for real vector spaces), associativity, and distributivity.

Two vectors are said to be **orthogonal** if their inner product is zero.

**Definition 12** Let  $S$  be a  $k$ -dimensional subspace of  $V$  and let  $S^\perp$  be the set of all vectors in  $V$  that are orthogonal to  $S$ . That is, if  $\mathbf{u} \in S$  and  $\mathbf{v} \in S^\perp$  then  $\mathbf{u} \cdot \mathbf{v} = 0$ .  $\square$

Fact: The set  $S^\perp$  is a vector space called the **dual space** of  $S$ . (show this!)

Fact: The dimension of  $S$  + the dimension of  $S^\perp$  = dimension of  $V$ .

## 5 Subfields and extension fields

A subfield of a field is a subset of the field that is also a field. Thus, for example,  $\mathbb{Q}$  is a subfield of  $\mathbb{R}$ .

A more potent concept is that of an extension field. Viewed one way, it simply turns the idea of a subfield around: an extension field  $E$  of a field  $F$  is a field that contains every element of  $F$ , so that  $F$  forms a subfield of  $E$ . The field  $F$  in this case is said to be the base field. But more importantly is the way that the extension field is created. Most commonly, extension fields are created to determine roots of polynomials that do not have roots in the base field.

**Definition 13** A nonconstant polynomial  $f(x) \in R[x]$  is **irreducible over  $R$**  if  $f(x)$  cannot be expressed as a product  $g(x)h(x)$  where both  $g(x)$  and  $h(x)$  are polynomials of degree less than the degree of  $f(x)$ , and  $g(x) \in R[x]$  and  $h(x) \in R[x]$ .  $\square$

In this definition, the ring (or field) in which the polynomial is irreducible makes a difference. For example, the polynomial  $f(x) = x^2 - 2$  is irreducible over  $\mathbb{Q}$ , but over the real numbers we can write

$$f(x) = (x + \sqrt{2})(x - \sqrt{2}).$$

We will demonstrate the construction of the familiar field of complex numbers as an extension of the real field. The polynomial  $p(x) \in \mathbb{R}[x]$  with real coefficients

$$p(x) = x^2 + 1$$

is irreducible over the real numbers. Additionally (and not quite the same thing), it has no solution over the real numbers. That is, there is no  $x \in \mathbb{R}$  such that  $p(x) = 0$ . We can create a new field, an extension to  $\mathbb{R}$ , essentially by *adjoining* a new element to the field that is specifically the root of  $p(x)$ . In this new field,

we must carefully and consistently define the operations of addition, multiplication, and so forth.

Let  $\alpha$  be an indeterminate. Let us create a field of *polynomials*, with multiplication modulo  $\alpha^2 + 1$ . We will denote this field (for the moment) as  $\langle \mathbb{R}[\alpha] \rangle_{\alpha^2+1}$ . We must verify that it in fact forms a field and not a ring. All elements in the field are of the form

$$a + b\alpha.$$

(Why?) Addition of elements of this form in the field is straightforward (i.e., polynomial addition)

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha.$$

Multiplication of these elements modulo  $\alpha^2 + 1$  can be written as

$$(a + b\alpha)(c + d\alpha) \pmod{\alpha^2 + 1} = (ac - bd) + (ad + bd)\alpha.$$

The multiplicative inverse of the nonzero element  $a + b\alpha$  can be verified to be

$$(a + b\alpha)^{-1} = \frac{(a - b\alpha)}{a^2 + b^2}.$$

Note that for the element  $\alpha \in \langle \mathbb{R}[\alpha] \rangle_{\alpha^2+1}$ ,

$$(\alpha)(\alpha) \pmod{\alpha^2 + 1} = -1,$$

so that  $\alpha$  is a root of the polynomial equation  $x^2 + 1 = 0$ . This field has the same rules of arithmetic as does the complex field  $\mathbb{C}$ . In fact, they are the *same field*. It is conventional to denote the indeterminate  $\alpha$  as  $i$  (the unit imaginary number) or as  $j$ .

The point of this is that if a polynomial exists which has no solution in a field  $F$ , a new field can be constructed in which a solution does exist. Related to this particular example, there are some other observations that can be made.

1. Miraculously enough, once the real field is extended to the complex field, *all* polynomials with coefficients either from  $\mathbb{R}$  or  $\mathbb{C}$  have solutions in the field. There is thus no need in usual computations to form extensions to larger fields. (This fact tends to make the idea of extension fields a little foreign at first, since we have a large enough field for most purposes at hand.) This fact is known as the fundamental theorem of algebra.
2. Consider as an example the polynomial  $q(x) \in \mathbb{Q}[x]$  with

$$q(x) = x^2 - 2,$$

The polynomial  $q(x)$  has no zeros in  $\mathbb{Q}$ , and so an extension field can be created in which  $q(x)$  has a zero. Elements in this field are of the form  $a + b\sqrt{2}$ , where  $a, b \in \mathbb{Q}$ . Arithmetic in this field is done modulo the polynomial  $x^2 - 2$ ; This field is an extension of  $\mathbb{Q}$ ; it is large enough to contain roots of  $q(x)$ , but not large enough to contain roots of every polynomial in  $\mathbb{Q}[x]$ . For example,  $r(x) = x^2 - 3$  does not have roots in this field, so another extension is necessary.

In this discussion about extension fields, the extension obtained has been stated to be a field, and seems to obey the properties of a field for the cases examined. That the extensions are in fact fields may be rigorously established, but requires some theoretical machinery (regarding maximal ideals) which we are not ready for yet.

**Box 1: Évariste Galois (1811–1832)**

The life of Galois is a study in brilliance and tragedy. At an early age, Galois studied the works in algebra and analysis of Abel and Lagrange, convincing himself (justifiably) that he was a mathematical genius. His stultifying schoolwork, however, remained mediocre. He attempted to enter the École Polytechnique, but his poor academic performance resulted in rejection, the first of many disappointments. At the age of seventeen, he wrote his discoveries in algebra in a paper which he submitted to Cauchy, who lost it. Meanwhile, his father, an outspoken local politician who instilled in Galois a hate for tyranny, committed suicide after some persecution. Some time later, Galois submitted another paper to Fourier. Fourier took the paper home, dying shortly thereafter and resulting in the loss of another paper. As a result of some outspoken criticism against the director, Galois was expelled from the normal school he was attending. Yet another paper presenting his works in finite fields was a failure, being rejected by the reviewer (Poisson) as being too incomprehensible.

Disillusioned, Galois joined the National Guard, where his outspoken nature led to some time in jail for a purported insult against Louis Philippe. Later he was challenged to a duel — probably a setup — to defend the honor of a woman. The night before the duel, Galois wrote a lengthy letter describing his discoveries. The letter was eventually published in *Revue Encyclopédique*. Alas, Galois was not there to read it: he was shot in the stomach in the duel and died the following day of peritonitis at the tender age of twenty.

## 5.1 Galois fields

In addition from providing some interesting insight into the structure of the numbers and equations we commonly deal with, the idea of extension fields provides a means of describing all fields of finite order, or finite fields. We have already observed that  $(\mathbb{Z}_p, +, \cdot)$  forms a field when  $p$  is prime. It turns out that *all* finite fields have  $p^m$  elements in them, where  $p$  is prime. For  $m > 1$ , the finite fields are obtained as extension fields to  $\mathbb{Z}_p$  using an irreducible polynomial in  $\mathbb{Z}_p[x]$  of degree  $m$ . These finite fields are usually denoted by  $GF(p^m)$  or  $GF(q)$  where  $q = p^m$ , where  $GF$  stands for “Galois field,” named after the French mathematician Évariste Galois.

Before introducing and proving some key properties of Galois fields, it is interesting to see a construction of one such field,  $GF(2^3)$ . As may be verified by direct substitution, the polynomial  $p(x) = x^3 + x + 1$  is irreducible over  $GF(2)$ . (The polynomial is also primitive). We will form the extension field by adjoining the root of  $p(x)$ . Let  $\alpha$  be such a root; then  $p(\alpha) = \alpha^3 + \alpha + 1 = 0$ , so  $\alpha^3 = \alpha + 1$ . The elements of  $GF(2^3)$  are the polynomials of the form  $a + ab + \alpha^2c$  for  $a, b, c \in GF(2)$ . Another representation is simply as a 3-tuple  $(a, b, c)$ . We observe that there must therefore be 8 elements in  $GF(2^3)$ . Addition is performed as usual (element-by-element, just as in polynomial addition). Multiplication is performed *modulo* the irreducible polynomial that was used to create the extension field. (Point out analogy with forming fields modulo a number). In our example, the elements are These are

$$0, 1, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2$$

These field elements can be expressed as triplets of the coefficients:

$$\begin{aligned}
 0 &\rightarrow (0, 0, 0) \\
 1 &\rightarrow (0, 0, 1) \\
 \alpha &\rightarrow (0, 1, 0) \\
 \alpha^2 &\rightarrow (1, 0, 0) \\
 1 + \alpha &\rightarrow (0, 1, 1) \\
 \alpha^2 &\rightarrow (1, 0, 0) \\
 1 + \alpha^2 &\rightarrow (1, 0, 1) \\
 \alpha + \alpha^2 &\rightarrow (1, 1, 0) \\
 1 + \alpha &\rightarrow (0, 1, 1) \\
 1 + \alpha + \alpha^2 &\rightarrow (1, 1, 1)
 \end{aligned}$$

Addition is easily accomplished in either the polynomial form or in the equivalent triplet form. From this form, we recognize that *the elements of the Galois field form a vector space over the base field  $GF(2)$* . Observe that for any element  $\beta \in GF(2^3)$ ,  $\beta + \beta = 0$ . Recalling the definition of the characteristic of a ring (which also applies to fields), we see that the characteristic of this field is 2.

Multiplication in the field is polynomial multiplication modulo  $p(\alpha)$ . For example,

$$(1 + \alpha^2)(\alpha + \alpha^2) = \alpha + \alpha^2 + \alpha^3 + \alpha^4 \pmod{\alpha^3 + \alpha + 1} = 1 + \alpha$$

Another useful representation is as powers of  $\alpha$ . Since  $\alpha^3 = \alpha + 1$ , we can form the following list of the nonzero elements in the field:

$$\begin{aligned}
 \alpha^0 &= 1 \\
 \alpha^1 &= \alpha \\
 \alpha^2 &= \alpha^2 \\
 \alpha^3 &= \alpha + 1 \\
 \alpha^4 &= \alpha(\alpha + 1) = \alpha^2 + \alpha \\
 \alpha^5 &= \alpha^2 + \alpha + 1 \\
 \alpha^6 &= \alpha^2 + 1
 \end{aligned}$$

The next power is  $\alpha^7 = \alpha^3 + \alpha = 1$ , so the list is complete. All of the nonzero elements of the field are generated by  $\alpha$ ;  $\alpha$  is said to be a **primitive element** of the field. The fact that  $\alpha$  is the root of the polynomial  $p(x)$  and also a primitive element is because  $p(x)$  is a primitive polynomial.

In the exponential notation, multiplication of field elements is easy. For example, since  $1 + \alpha^2 = \alpha^6$  and  $\alpha + \alpha^2 = \alpha^4$ , we have

$$(1 + \alpha^2)(\alpha + \alpha^2) = \alpha^6 \alpha^4 = \alpha^{10} = \alpha^7 \alpha^3 = \alpha^3 = \alpha + 1.$$

Having presenting an examples, we now present some important ideas associated with Galois fields.

**Definition 14** Let  $\beta \in GF(q)$ . The **order** of  $\beta$ , written  $\text{ord}(\beta)$  is the smallest positive integer  $n$  such that  $\beta^n = 1$ .  $\square$

**Definition 15** An element with order  $q - 1$  in  $GF(q)$  is called a primitive element in  $GF(q)$ .  $\square$

Note: the notation  $a|b$  means:  $a$  divides  $b$ , and  $(a, b)$  is the greatest common divisor of  $a$  and  $b$ .

**Lemma 7** If  $\beta \in GF(q)$  and  $\beta \neq 0$  then  $\text{ord}(\beta)|(q - 1)$ .

**Proof** Let  $t = \text{ord}(\beta)$ . The set  $\{\beta, \beta^2, \dots, \beta^t = 1\}$  forms a subgroup of the nonzero elements in  $GF(q)$  under multiplication. Since the order of a subgroup must divide the order of the group (Lagrange's theorem), the result follows.  $\square$

**Lemma 8** If  $\alpha \in GF(q)$  and  $\beta \in GF(q)$  with  $\beta = \alpha^i$  for some  $i$ , and if  $\text{ord}(\alpha) = t$  then

$$\text{ord}(\beta) = \frac{t}{(i, t)}$$

**Proof** If  $\text{ord}(\alpha) = t$ , then  $\alpha^s = 1$  if and only if  $t|s$ . (Use the division algorithm:  $s = qt + r$  with  $0 \leq r < t$ ,  $\alpha^s = \alpha^{qt+r} = \alpha^r = 1$ .)

Let  $\text{ord}(\beta) = u$ . Note that  $i/(i, t)$  is an integer. Then

$$\beta^{t/(i, t)} = (\alpha^i)^{t/(i, t)} = (\alpha^t)^{i/(i, t)} = 1.$$

Thus  $u|t/(i, t)$ . We also have

$$(\alpha^i)^u = 1$$

so  $t|iu$ . This means that  $t/(i, t)|u$ . Combining the results, we have

$$u = t/(i, t).$$

$\square$

**Definition 16** An element in  $GF(q)$  with order  $q-1$  is called a **primitive element** in  $GF(q)$ .  $\square$

In other words, a primitive element has the highest possible order. The question of whether there are any primitive elements in  $GF(q)$ , and how many, is now addressed.

**Definition 17** The **Euler totient function**  $\phi(n)$  is the number of positive integers less than  $n$  that are relative prime to  $n$ . This is also called the **Euler**  $\phi$  function, or sometimes just the  $\phi$  function.  $\square$

**Example 25**

1.  $\phi(5) = 4$
2.  $\phi(4) = 2$
3.  $\phi(6) = 2$

$\square$

It can be shown that the  $\phi$  function can be written as

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is taken over all primes  $p$  dividing  $n$ . For example,

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

We observe that:

1.  $\phi(p) = p - 1$  if  $p$  is prime.
2.  $\phi(p_1 p_2) = (p_1 - 1)(p_2 - 1)$  for primes  $p_1$  and  $p_2$ .

3.  $\phi(p^m) = p^{m-1}(p-1)$  for  $p$  prime.
4.  $\phi(p^m q^n) = p^{m-1} q^{n-1} (p-1)(q-1)$  for distinct primes  $p$  and  $q$ .

**Theorem 9** For a Galois field  $GF(q)$ :

1. If  $t \nmid (q-1)$ , then there are no elements of order  $t$  in  $GF(q)$
2. if  $t \mid q-1$  then there are  $\phi(t)$  elements of order  $t$  in  $GF(q)$

**Proof** Part 1 we have already seen. For part 2, let  $\alpha$  be an element with order  $t$ . Then by the previous theorem, if  $\beta = \alpha^i$  for some  $i$  such that  $(i, t) = 1$ , then  $\beta$  also has order  $t$ . But the number of such  $i$ s is  $\phi(t)$ .  $\square$

From this theorem we make the following observation: there are  $\phi(q-1)$  primitive elements in  $GF(q)$ .

**Example 26** In  $GF(7)$ , the numbers 5 and 2 are primitive:

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

We also have  $\phi(q-1) = \phi(6) = 2$ .  $\square$

Collecting our thoughts, we observe that in  $GF(q)$ , there are  $\phi(q-1) > 1$  primitive elements, and that all non-zero elements of the field can be constructed as powers of the primitive element. We will frequently denote the primitive element in the field as  $\alpha$ .

**Lemma 10** The characteristic of a Galois field is always a prime integer.

(Recall that the characteristic is the smallest positive integer such that  $m(1) = 1 + 1 + \dots + 1 = 0$ .)

**Proof** Suppose that  $k$  is the characteristic and that  $k$  is a composite number  $k$ . Then  $k(1) = 0$ , and there are integers  $m$  and  $n$  such that  $k = mn$ . Then

$$0 = k(1) = (mn)(1) = m(1)n(1) = 0,$$

by the distributive property. But a field has no zero divisors, so either  $m(1)$  or  $n(1)$  is the characteristic, violating the minimality of the characteristic.  $\square$

On the basis of this lemma, we can observe that in a field  $GF(q)$ , there are  $p$  elements ( $p$  a prime number)  $\{0, 1, 2, \dots, (p-1)(1)\}$  which behave as a field (i.e., we can define addition and multiplication on them as a field). Thus  $\mathbb{Z}_p$  (or something isomorphic to it, which is the same thing) is a subfield of every Galois field  $GF(q)$ . In fact, a stronger assertion can be made:

**Theorem 11** The order  $q$  of every finite field  $GF(q)$  must be a power of a prime.

**Proof**

$\mathbb{Z}_p$  is a prime-order subfield of  $GF(q)$ . We will show that  $GF(q)$  acts like a vector space over hits subfield  $GF(p)$ .

Let  $\beta_1 \in GF(q)$ , with  $\beta_1 \neq 0$ . As  $\alpha_1$  varies over the  $p$  elements in  $GF(p)$ , the product  $\beta_1 \alpha_1$  takes on  $p$  distinct values. (For if  $x\beta_1 = y\beta_1$  we must have  $x = y$ , since there are no zero divisors in a field.) If by these  $p$  products we have covered all the elements in the field, we are done: they form a vector space over  $GF(p)$ .

If not, let  $\beta_2$  be an element which has not been covered. Then form  $\alpha_1 \beta_1 + \alpha_2 \beta_2$  as  $\alpha_1$  and  $\alpha_2$  vary independently. This must lead to  $p^2$  distinct values in  $GF(q)$ . If still not done, then continue, forming the linear combinations

$$\alpha_1 \beta_1 + \alpha_2 \beta_2 + \dots + \alpha_m \beta_m$$

Each combination of coefficients  $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$  corresponds to a distinct element of  $GF(q)$ . Therefore, there must be  $p^m$  elements in  $GF(q)$ .  $\square$

This points the way to constructing every finite field. To construct  $GF(p^m)$ , we a polynomial degree  $m$  irreducible over  $GF(p)$ , and form the extension field for this polynomial, as we did for the example of  $GF(2^3)$  above.

## 5.2 Irreducible and Primitive polynomials

**Definition 18** A nonconstant polynomial  $f(x) \in GF(q)[x]$  is **irreducible over**  $GF(q)$  if  $f(x)$  cannot be expressed as a product  $g(x)h(x)$  where both  $g(x)$  and  $h(x)$  are polynomials of degree less than the degree of  $f(x)$ , and  $g(x) \in GF(q)[x]$  and  $h(x) \in GF(q)[x]$ .  $\square$

While any irreducible polynomial can be used to construct the extension field, computation in the field is easier if a primitive polynomial is used. First, we make the following observation:

**Theorem 12** An irreducible  $m$ th-degree polynomial  $f(x) \in GF(p)[x]$  divides  $x^{p^m-1} - 1$ .

**Example 27**  $(x^3 + x + 1) \mid x^7 + 1$  in  $GF(2)$  (Show by long division).  $\square$

**Definition 19** An irreducible polynomial  $p(x) \in GF(p)[x]$  of degree  $m$  is said to be **primitive** if the smallest positive integer  $n$  for which  $p(x)$  divides  $x^n - 1$  is  $n = p^m - 1$ .  $\square$

It can be shown that the polynomial  $p(x) = x^3 + x + 1$  used above is primitive in  $GF(2)[x]$ , since  $x^7 - 1$  is divisible by  $p(x)$ ,

$$x^7 - 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1),$$

but no smaller  $n$  exists such that  $x^n - 1$  is divisible by  $p(x)$ . Not every irreducible polynomial is primitive. The following theorem, provides the motivation for using primitive polynomials.

**Theorem 13** The roots of an  $m$ th degree primitive polynomial  $p(x) \in GF(p)[x]$  are primitive elements in  $GF(p^m)$ .

**Proof** Let  $\alpha$  be a root of an  $m$ th-degree primitive polynomial  $p(x)$ . We have

$$x^{p^m-1} - 1 = p(x)q(x)$$

for some  $q(x)$ . Observe that

$$\alpha^{p^m-1} - 1 = p(\alpha)q(\alpha) = 0q(\alpha) = 0$$

from which we note that

$$\alpha^{p^m-1} = 1$$

Now the question is, might there be a smaller power  $t$  of  $\alpha$  such that  $\alpha^t = 1$ ? If this were the case, then we would have

$$\alpha^t - 1 = 0.$$

There would therefore be some polynomial  $x^t - 1$  that would have  $\alpha$  as its roots. However, any root of  $x^t - 1$  must also be a root of  $x^{p^m-1} - 1$ , because  $\text{ord}(\alpha) | p^m - 1$ . To see this, suppose (to the contrary) that  $\alpha \not| p^m - 1$ . Then

$$p^m - 1 = k \text{ord}(\alpha) + r$$

for some  $r$  with  $0 < r < \text{ord}(\alpha)$ . Therefore we have

$$1 = \alpha^{p^m-1} = \alpha^{k \text{ord}(\alpha)+r} = \alpha^r,$$

which contradicts the minimality of the order.

Thus, all the roots of  $x^t - 1$  are the roots of  $x^{p^m-1} - 1$ , so

$$x^t - 1 | x^{p^m-1} - 1.$$

Fact: all the roots of an irreducible polynomial are of the same order. (To be proven later). This means that  $p(x) | x^t - 1$ . But by the definition of a primitive polynomial, we must have  $t = p^m - 1$ .  $\square$

All the nonzero elements of the field can be **generated as powers of the roots of the primitive polynomial**.

**Example 28** We will produce the field  $GF(8)$ . The polynomial  $x^3 + x + 1$  is primitive in  $GF(2)[x]$ . Let  $\alpha$  be a root of  $p(x)$ , so that

$$\alpha^3 + \alpha + 1 = 0,$$

or, equivalently,

$$\alpha^3 = \alpha + 1.$$

Now we list the powers of  $\alpha$ :

exponential representation	polynomial representation	vector space representation
$\alpha^0$	1	(0,0,1)
$\alpha^1$	$\alpha$	(0,1,0)
$\alpha^2$	$\alpha^2$	(1,0,0)
$\alpha^3$	$\alpha + 1$	(0,1,1)
$\alpha^4$	$\alpha^2 + \alpha$	(1,1,0)
$\alpha^5$	$\alpha^2 + \alpha + 1$	(1,1,1)
$\alpha^6$	$\alpha^2 + 1$	(1,0,1)
0	0	(0,0,0)

Note that all possible 3-tuples are present. Also note that this can be drawn using a linear feedback shift register.

Observe that, as a general rule, multiplication is easier using the exponential form, while addition is easier using the polynomial or vector space form.  $\square$

**Example 29** The polynomial  $p(x) = x^2 + x + 2$  is primitive in  $GF(5)$ . Let  $\alpha$  represent a root of  $p(x)$ . The elements in  $GF(5)$  can be represented as powers of  $\alpha$  as shown in the following table.

0	$\alpha^0 = 1$	$\alpha^1 = \alpha$	$\alpha^2 = 4\alpha + 3$	$\alpha^3 = 4\alpha + 2$
$\alpha^4 = 3\alpha + 2$	$\alpha^5 = 4\alpha + 4$	$\alpha^6 = 2$	$\alpha^7 = 2\alpha$	$\alpha^8 = 3\alpha + 1$
$\alpha^9 = 3\alpha + 4$	$\alpha^{10} = \alpha + 4$	$\alpha^{11} = 3\alpha + 3$	$\alpha^{12} = 4$	$\alpha^{13} = 4\alpha$
$\alpha^{14} = \alpha + 2$	$\alpha^{15} = \alpha + 3$	$\alpha^{16} = 2\alpha + 3$	$\alpha^{17} = \alpha + 1$	$\alpha^{18} = 3$
$\alpha^{19} = 3\alpha$	$\alpha^{20} = 2\alpha + 4$	$\alpha^{21} = 2\alpha + 1$	$\alpha^{22} = 4\alpha + 1$	$\alpha^{23} = 2\alpha + 2$

As an example of some arithmetic in this field,

$$(3\alpha + 4) + (4\alpha + 1) = 2\alpha$$

$$(3\alpha + 4)(4\alpha + 1) = \alpha^9 \alpha^{22} = \alpha^{31} = (\alpha^{24})(\alpha^7) = 2\alpha.$$

□

## 6 Subfields of GF

**Theorem 14** *An element  $\beta \in GF(q^m)$  lies in  $GF(q)$  if and only if  $\beta^q = \beta$ .*

**Proof** If  $\beta \in GF(q)$ , then:  $\text{ord}(\beta) | q - 1$ , so that  $\beta^q = \beta$ .

Conversely, assume  $\beta^q = \beta$ . Then  $\beta$  is a root of

$$x^q - x = 0.$$

Now observe that all  $q$  elements of  $GF(q)$  satisfy this polynomial. Hence  $\beta \in GF(q)$ .

□