Math 333: Introduction to Algebraic Structures

Darshan Patel

Fall 2017

Contents

1 Operations

Definition 1.1. Let A be any set:
An operation $*$ on A is a rule which assigns to each ordered pair $(a,\ b)$ of elements of A exactly one element $a * b$ in A.

Stressed Aspects:

- $a * b$ is defined for every ordered pair $(a,\ b)$ of elements of A. Often, $a * b$ is defined for all the obvious choices of a and b, but remains undefined in a few exceptional cases.

  Example 1.1. Division does not qualify as an operation on the set $\mathbb{R}$ of the real numbers, for there are ordered pairs such as $(3,\ 0)$ whose quotient $3/0$ is undefined. In order to be an operation on $\mathbb{R}$, division would have to associate a real number a/b with every ordered pair $(a,\ b)$ of elements of $\mathbb{R}$.

- $a * b$ must be uniquely defined.

  Example 1.2. Define an operation $\Box$ on the set $\mathbb{R}$ of the real numbers by letting $a \Box b$ be the number whose square is ab. This is ambiguous because $2 \Box 8$ could be either 4 or -4. Thus $\Box$ does not qualify as an operation on $\mathbb{R}$.

- If a and b are in A, $a * b$ must be in A. This is expressed by saying that A is closed under the operation $*$.

  Example 1.3. Division cannot be regarded as an operation on the set of the integers, for there are pairs of integers such as (3, 4) whose quotient 3/4 is not an integer.
  On the other hand, division does qualify as an operation on the set of all the positive real numbers, for the quotient of any two positive real numbers is a uniquely defined positive real number.

An operation is any rule which assigns to each ordered pair of elements of A a unique element in A. Therefore in general, there are many possible operations on a given set A.

Example 1.4. If A is a set consisting of 2 distinct elements, a and b, each operation on A may be described by a table as follows

(x, y)	$x * y$
(a, a)	
(a, b)	
(b, a)	
(b, b)	

Here are four possible operations for four possible ordered pairs of elements of A and the value of $x * y$

(x,y)	1) $x*y$	2) $x*y$	3) $x*y$	4) $x*y$
(a,a)	a	a	b	b
(a,b)	a	b	a	b
(b,a)	a	a	b	b
(b,b)	a	b	a	a

Each row describes a different operation on A. In fact, there are 16 possible ways of filling the table and thus 16 possible operations on the set A.

Definition 1.2. An operation $*$ may be commutative, that is, it may satisfy

$$a*b=b*a$$

for any two elements a and b in set A.

Definition 1.3. An operation $*$ may be associative, that is, it may satisfy

$$(a*b)*c=a*(b*c)$$

for any 3 elements a, b and c in set A.

Example 1.5. The addition of real numbers is associative because

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

However, division of real numbers is not associative

$$\frac{3}{4/5}=\frac{15}{4} \text{ but } \frac{3/4}{5}=\frac{3}{20}$$

Definition 1.4. If there is an element e in A with the property that $e*a=a$ and $a*e=a$ for every element a in A, then e is called an identity of "neutral" element with respect to the operation $*$. When combined with any element a, it does not change a.

Example 1.6. In the set $\mathbb{R}$ of the real numbers, 0 is a neutral element for addition and 1 is a neutral element for multiplication.

Definition 1.5. If a is any element of A and x is an element of A such that $a*x=e$ and $x*a=e$, then x is called an inverse of a. When an element is combined with its inverse, it produces the neutral element.

Example 1.7. In the set $\mathbb{R}$ of the real numbers, $-a$ is the inverse of a with respect to addition; if $a\neq 0$, then $\frac{1}{a}$ is the inverse of a with respect to multiplication.

Note: Usually, the inverse of a is denoted by a^{-1}.

2 The Definition of Groups

Definition 2.1. By a group, we mean a set G with an operation $*$ which satisfies the axioms:

1. $*$ is associative
2. There is an element e in G such that $a * e = a$ and $e * a = a$ for every element in G
3. For every element a in G, there is an element a^{-1} in G such that $a * a^{-1} = e$ and $a^{-1} * a = e$

Note: A group is represented by the symbol $\langle G, * \rangle$.

Example 2.1. $\mathbb{Z}$ is the symbol used to denote the set

$$\{\dots, -3. -2, -1, 0, 1, 2, 3, \dots\}$$

of the integers. The set $\mathbb{Z}$, with the operation of addition, is obviously a group. It is called the additive group of the integers and represented by the symbol $\langle \mathbb{Z}, + \rangle$. Mostly, it is denoted simply by the symbol $\mathbb{Z}$.

Example 2.2. $\mathbb{Q}$ designates the set of the rational numbers (that is, quotients m/n of integers where $n \neq 0$). This set, with the operation of addition, is called the additive group of the rational numbers, $\langle \mathbb{Q}, + \rangle$. It is denoted by $\mathbb{Q}$.

Example 2.3. The symbol $\mathbb{R}$ represents the set of the real numbers. $\mathbb{R}$ with the operation of addition, is called the additive group of the real numbers and is represented by $\langle \mathbb{R}, + \rangle$, or simply $\mathbb{R}$.

Example 2.4. The set of the nonzero rational numbers is represented by $\mathbb{Q}^*$. This set, with the operation of multiplication, is the group $\langle \mathbb{Q}^*, \cdot \rangle$, or simply $\mathbb{Q}^*$.
Similarly, the set of all the nonzero real numbers is represented by $\mathbb{R}^*$. The set $\mathbb{R}^*$ with the operation of multiplication, is group $\langle \mathbb{R}^*, \cdot \rangle$, or simply $\mathbb{R}^*$.

Example 2.5. $\mathbb{Q}^{\text{pos}}$ denotes the group of all the positive rational numbers, with multiplication. $\mathbb{R}^{\text{pos}}$ denotes the group of all the positive real numbers, with multiplication.

Definition 2.2. Finite Groups: groups with a finite number of elements

Such groups occur often in applications, for in most situations of the real world, we deal with only a finite number of objects.

Definition 2.3. Group of Integers modulo n: consists of the set

$$\{0, 1, 2, \dots, n-1\}$$

with the operation of addition modulo n. Imagine the numbers 0 through $n-1$ to be points on the unit circle, each one separated from the next by an arc of length $2\pi/n$. To add two numbers h and k, start with h and move clockwise through an arc of k times $2\pi/n$. The sum $h+k$ will be one of the numbers 0 through $n-1$. From geometrical considerations it is clear that this kind of addition is associative. Zero is the neutral element of this group and $n-h$ is the inverse of h [for $h+(n-h) = n$, which coincides with 0]. This group, the group of integers modulo n, is represented by the symbol $\mathbb{Z}_n$.

When working with finite groups, it is useful to draw up an "operation table." The basic format of this table is as follows

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

with one row for each element of the group and one column for each element of the group. Then, for example, 3 + 4, is located in the row of 3 and the column of 4. In general, any finite group $\langle G, * \rangle$ has a table

$*$	$\cdots\cdots$	y	$\cdots\cdots$
$\vdots$			
x		$x + y$	
$\vdots$			

The entry in the row of x and the column of y is $x * y$.
sim
Note that the commutative law is not one of the axioms of group theory; hence the identity $a\ timesb = b * a$ is not true for every group. If the commutative law holds in a group G, such a group is called a commutative group, or more commonly, an abelian group.

Example 2.6. Let G be the group which consists of the six matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

$$C = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \quad D = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad K = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$$

with the operation of matrix multiplication. this group has the following operation table

	1	A	B	C	D	K
1	I	A	B	C	D	K
A	A	I	C	B	K	D
B	B	K	D	A	I	C
C	C	D	K	I	A	B
D	D	C	I	K	B	A
K	K	B	A	D	C	I

In linear algebra it shown that the multiplication of matrices is associative. It is clear that I is the identity element of this group and by looking at the table, one can see that each of the six matrices in $[I, A, B, C, D, K]$ has in inverse in $[I, A, B, C, D, K]$. For example, B is the inverse of D, A is the inverse of A, and so on. Thus G is a group! Note however that $AB = C$ but $BA = K$, so G is not commutative. G is not an abelian group.

3 Elementary Properties of Groups

Is it possible for a group to have two different identity elements? Suppose e_1 and e_2 are identity elements of some group G. Then

$$e_1 * e_2 = e_2 \text{ because } e_2 \text{ is an identity element, and}$$
$$e_1 * e_2 = e_1 \text{ because } e_2 \text{ is an identity element}$$

Therefore

$$e_1 = e_2$$

This shows that in every group, there is exactly one identity element.
sim

Can an element a in a group have different inverses? If a_1 and a_2 are both inverses of a, then

$$a_1 * (a * a_2) = a_1 * e = a_1$$

and

$$(a_1 * a) * a_2 = e * a_2 = a_2$$

By the associative law, $a_1 * (a * a_2) = (a_1 * a) * a_2$. Hence $a_1 = a_2$. This shows that in every group, each element has exactly one inverse.

Definition 3.1. Additive Notation: refers $a + b$ as the sum of a and b

Definition 3.2. Multiplicative Notation: refers ab as the product of a and b

Theorem 3.1. Cancellation Law: If G is a group and a, b, c are elements of G, then

1. $ab = ac$ implies $b = c$
2. $ba = ca$ implies $b = c$

Proof. Suppose

$$ab = ac$$

Then

$$a^{-1}(ab) = a^{-1}(ac)$$

By the associative law,

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

that is,

$$eb = ec$$

Thus, finally,

$$b = c$$

□

Proof. Suppose

$$ba = ca$$

Then

$$a^{-1}(ba) = a^{-1}(ac)$$

By the associative law,

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

that is,

$$eb = ec$$

Thus, finally,

$$b = c$$

□

In general, a cannot be cancelled in the equation $ab = ca$.

Theorem 3.2. If G is a group and a, b are elements of G, then

$$ab = e \text{ implies } a = b^{-1} \text{ and } b = a^{-1}$$

Proof. If $ab = e$, then $ab = aa^{-1}$. So by the cancellation law, $b = a^{-1}$. Analogously, $a = b^{-1}$. □

This theorem says that if the product of two elements is equal to e, these elements are inverses of each other.

Theorem 3.3. If G is a group and a, b are elements of G, then

1. $(ab)^{-1} = b^{-1}a^{-1}$
2. $(a^{-1})^{-1} = a$

Proof.

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a[(bb^{-1})a^{-1}] \text{ by the associative law} \\ &= a[ea^{-1}] \text{ because } bb^{-1} = e \\ &= aa^{-1} \\ &= e\end{aligned}$$

Since the product of ab and $b^{-1}a^{-1}$ is equal to e, it follows from Theorem 3.2 that they are each other's inverses and thus $(ab)^{-1} = b^{-1}a^{-1}$. □

Proof. insert later □

In general, any two products, each involving the same factors in the same order, are equaL The net effect of the associative law is that parentheses are redundant. For example, the product of any four elements a, b, c and d in G is defined as

$$abcd = a(bcd)$$

By successive uses of the associative law,

$$a(bc)d = ab(cd) = (ab)(cd) = (ab)cd$$

Hence the product $abcd$ (without parentheses but without changing the order of its factors) is defined without ambiguity.
sim

By using the identity $(ab)^{-1} = b^{-1}a^{-1}$ repeatedly, it is true that

$$(a_1a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1}a_1^{-1}$$

Definition 3.3. If G is a finite group, the number of elements in G is called the order of G. It is denoted by the symbol $|G|$.

4 Subgroups

Definition 4.1. Let G be a group and S a nonempty subset of G. If the product of every pair of elements of S is in S, then S is closed with respect to multiplication. Then, it may happen that the inverse of every element of S is in S which means that S is closed with respect to inverses. If both these things happen, S is a subgroup of G.

Note: When the operation of G is denoted by the symbol $+$, then if the sum of every pair of elements of S is in S, then S is closed with respect to addition. If the negative of every element of S is in S, then S is closed with respect to negatives. if both of these things happen, S is a subgroup of G.

Example 4.1. The set of all the even integers is a subgroup of the additive group $\mathbb{Z}$ of the integers. The sum of any two even integers is an even integer and the negative of any even integer is an even integer.

Example 4.2. $\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$. indeed, $\mathbb{Q}^* \subseteq \mathbb{R}^*$ because every rational number is a real number. Furthermore, the product of any two rational numbers is rational and the inverse (the reciprocal) of any rational number is a rational number

If S is a subgroup of G, the operation of S is the same as the operation of G, If a and b are elements of S, the product ab computed in S is precisely the product ab computed in G.

Example 4.3. It is meaningless to say that $\langle \mathbb{Q}^*, \cdot \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$. Although it is true that $\mathbb{Q}^*$ is a subset of $\mathbb{R}$, the operations on these two groups are different.

Fact: If G is a group and S is a subgroup of G, then S itself is a group.

Example 4.4. $\mathscr{F}$ represents the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, the set of all real-valued functions of a real variable. $\mathscr{F}(\mathbb{R})$ with the operation $+$ for adding functions, is the group $\langle \mathscr{F}(\mathbb{R}), + \rangle$, or simply $\mathscr{F}(\mathbb{R})$. If f and g are functions from $\mathbb{R}$ to $\mathbb{R}$, then f and g are equal if and only if $f(x) = g(x)$ for every real number x.
sim

To check that + is associative, show that $f+[g+h]=[f+g]+h$, for every three functions f, g, h in $\mathscr{F}(\mathbb{R})$. This means that for any real number x, $\{f+[g+h]\}(x)=\{[f+g]+h\}(x)$ Well,

$$\{f+[g+h]\}(x)=f(x)+[g+h](x)=f(x)+g(x)+h(x)$$

and $\{[f+g]+h\}(x)$ has the same value.
sim
The neutral element of $\mathscr{F}(\mathbb{R})$ is the function $\mathscr{O}$ given by $\mathscr{O}(x)=0$ for every real number x. To show that $\mathscr{O}+\mathscr{F}=\mathscr{F}$, one must show that $[\mathscr{O}+f](x)=f(x)$ for every real number x. This is true because

$$[\mathscr{O}+f](x)=\mathscr{O}(x)+f(x)=0+f(x)=f(x)$$

The inverse of any function f is the function $-f$ given by

$$[-f](x)=-f(x)$$

for every real number x. It is perceived immediately that $f+[-f]=\mathscr{O}$ for every function f.

Example 4.5. $\mathscr{C}(\mathbb{R})$ represents the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. With the operation +, it is a subgroup of $\mathscr{F}(\mathbb{R})$ because the sum of any two continuous functions is a continuous function, and the negative $-f$ of any continuous function f is a continuous function. Because any subgroup of a group is itself a group, it can be concluded that $\mathscr{C}(\mathbb{R})$, with the operation +, is a group, denoted by $\langle\mathscr{C}(\mathbb{R}),+\rangle$, or simply $\mathscr{C}(\mathbb{R})$.

Example 4.6. $\mathscr{D}(\mathbb{R})$ represents the set of all the differential functions from $\mathbb{R}$ to $\mathbb{R}$. It is a subgroup of $\mathscr{F}(\mathbb{R})$ because the sum of any two differentiable functions is differentiable and the negative of any differentiable function is differentiable. Thus, $\mathscr{D}(\mathbb{R})$, with the operation of adding functions, is a group denoted by $\langle\mathscr{D}(\mathbb{R}),+\rangle$, or simply $\mathscr{D}(\mathbb{R})$.

Definition 4.2. In any group G, the one element subset $\{e\}$, containing only the neutral element, is a subgroup. At the other extreme, the whole group G is a subgroup of itself. These are the trivial subgroups of G. All the other subgroups of G are called proper subgroups.

Definition 4.3. Suppose G is a group and a, b, and c are elements of G. Define S to be the subset of G which contains all the possible products of a, b, c and their inverses, in any order, with repetition of factors permitted. Thus, typical elements of S would be: $abac^{-1}$, $c^{-1}a^{-1}bbc$ and so on. It is easy to see that S is a subgroup of G: for if two elements of S are multiplied together, they yield an element of S and the inverse of any element of S is an element of S.Therefore, S is called the subgroup of G generated by a, b, and c.

Definition 4.4. If a is a single element of G, consider the subgroup generated by a. This subgroup is designated by the symbol $\langle a\rangle$ and is called a cyclic subgroup of G; a is called its generator. Note that $\langle a\rangle$ consists of all the possible products of a and a^{-1}. Since factors of a^{-1} cancel factors of a, there is no need to consider products involving both a and a^{-1} side by side. Thus, $\langle a\rangle$ contains $a, aa, aaa, \ldots$, $a^{-1}, a^{-1}a^{-1}, a^{-1}a^{-1}a^{-1}, \ldots$, as well as $aa^{-1}=e$.

Note: If the operation of G is denoted by +, the same definitions can be given with "sums" instead of "products."

Definition 4.5. If a group G is generated by a single element a, G is a cyclic group and is written as $G - \langle a \rangle$.

Example 4.7. The additive group $\mathbb{Z}_6$ is cyclic.

Definition 4.6. Every finite group G is generated by one or more of its elements. A set of equations, involving only the generators and their inverses, is called a set of defining equations for G if these equations completely determine the multiplication table of G.

Example 4.8. Let G be the group $\{e, a, b, b^2, ab, ab^2\}$ whose generators a and b satisfy the equations

$$a^2 = e$$
$$b^3 = e$$
$$ba = ab^2$$

These three equations do determine the multiplication table of G. To see this, note first that the equation $ba = ab^2$ allows to switch powers of a with powers of b, bringing powers of a to the left, and powers of b to the right. For example, to find the product of ab and ab^2,

$$(ab)(ab^2) = a \underbrace{ba}_{=ab^2} b^2 = aab^2b^2 = a^2b^4$$

But by the defining equations, $a^2 = e$ and $b^4 = b^3b = b$; so finally,

$$(ab)(ab^2) = b$$

All the entries in the table of G may be computed in the same fashion.

Definition 4.7. When a group is determined by a set of generators and defining equations, its structure can be efficiently represented in a diagram called a Cayley diagram.

5 Functions

Definition 5.1. If A and B are sets, then a function from A to B is a rule which to every element x in A assigns a unique element y in B. To indicate this connection between x and y, it is written as $y = f(x)$ and y is called the image of x under the function y.

Definition 5.2. If f is a function from A to B, it is customary to describe it by writing

$$f : A \to B$$

where the set A is called the domain of f and the range of f is the subset of B which consists of all the images of elements of A.

Definition 5.3. A function $f : A \to B$ is called injective if each element of B is the image of no more than one element of A.

The intended meaning is that each element y in B is the image of no two distinct elements of A. So if $f(x_1) = f(x_2)$, it must be true that $x_1 = x_2$.
sim
A convenient definition of "injective" is that a function $f : A \to B$ is injective if and only if

$$f(x_1) = f(x_2) \text{ implies } x_1 = x_2$$

Definition 5.4. A function $f : A \to B$ is called surjective if each element of B is the image of at least one element of A.

This is the same as saying that B is the range of f.

Definition 5.5. A function $f : A \to B$ is called bijective if it is both injective and surjective; in other words, each element of B is the image of at least one element of A and no more than one element of A.

Definition 5.6. Let $f : A \to B$ and $g : B \to C$ be functions. The composite function denoted by $g \circ f$ is a function from A to C defined as follows:

$$[g \circ f](x) = g(f(x)) \text{ for every } x \in A$$

Example 5.1. Let f and g be the following functions from $\mathbb{R}$ to $\mathbb{R}$: $f(x) = 2x$; $g(x) = x+1$. Their composites are the functions $g \circ f$ and $f \circ g$ given by

$$(x) = f(g(x)) = 2(x+1)$$
$$[g \circ f](x) = g(f(x)) = 2x + 1$$

Note, if $f : A \to B$ and $g : B \to C$ are functions, then the following are true:

- If f and g are injective, then $g \circ f$ is injective
- If f and g are surjective, then $g \circ f$ is surjective
- If f and g are bijective, then $g \circ f$ is bijective

Proof. Suppose that f and g are injective and prove that $g \circ f$ is injective. Thus show that if $[g \circ f](x) = [g \circ g](y)$ then $x = y$.
Suppose $[g \circ f](x) = [g \circ f](y)$, that is,

$$g(f(x)) = g(f(y))$$

Because g is injective,

$$f(x) = f(y)$$

and because f is injective

$$x = y$$

□

Proof. Suppose that f and g are surjective and prove that $g \circ f$ is surjective. Thus show that every element of C is $g \circ f$ of some element of A.
If $z \in C$, then since g is surjective, $x = g(y)$ for some $y \in B$; but f is surjective, so $y = f(x)$ for some $x \in A$. Thus

$$z = g(y) = g(f(x)) = [g \circ g](x)$$

□

Proof. If f and g are bijective, they are both injective and surjective. The two previous proofs showed that $g \circ f$ is injective and surjective. Thus $g \circ f$ is bijective. □

Definition 5.7. The inverse of function f from A to B, if it exists, is a function f^{-1} from B to A such that

$$x = f^{-1}(y) \text{ if and only if } y = f(x)$$

Note: A function $f : A \to B$ has an inverse if and only if it is bijective. In that case, the inverse f^{-1} is a bijective function from B to A.

6 Groups of Permutations

Definition 6.1. Any two functions f and g (from A to A) are equal if and only if $f(x) = g(x)$ for every element x in A.

Definition 6.2. If f and g are functions from A to A, their composite $f \circ g$ is also a function from A to A

$$[f \circ g](x) = f(g(x)) \text{ for every } x \in A$$

Note: The composition of functions is associative. Thus, if f, g and h are three functions from A to A, then

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Definition 6.3. A permutation of a set A is a bijective function from A to A, a one-to-one correspondence between A and itself

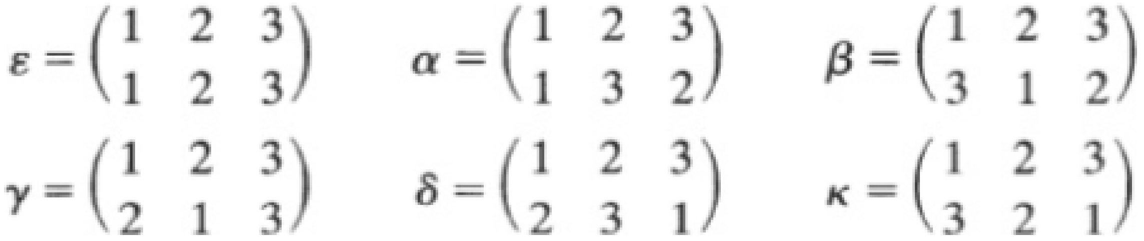
Definition 6.4. The composite of any two permutations of A is a permutation of A. It follows that the operation $\circ$ of composition can be regarded as an operation on the set of all the permutations of A.

Definition 6.5. For any set A, the identity function on A, symbolized by ε_A or simply ε, is the function $x \to x$ which carries every element of A to itself

$$\varepsilon(x) = x \ \ \forall x \in A$$

Note: The set of all the permutations of A, with the operation $\circ$ of composition, is a group.

Example 6.1. List all the permutations of the set $\{1, 2, 3\}$.



$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \kappa = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

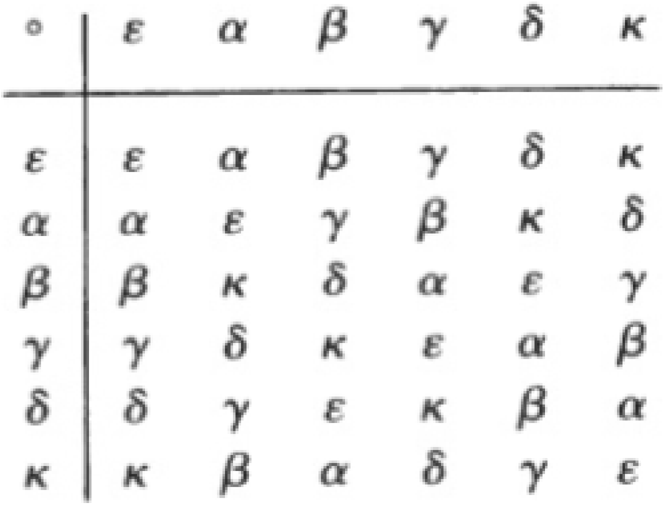
Then β is the function such that $\beta(1) = 3$, $\beta(2) = 1$ and $\beta(3) = 2$. The operation on elements of S_3 is composition. To find $\alpha \circ \beta$, note that

$$\begin{aligned} \beta t \qquad (1) &= \alpha(\beta(1)) = \alpha(3) = 2 \\ [\alpha \circ \beta](2) &= \alpha(\beta(2)) = \alpha(1) = 2 \\ [\alpha \circ \beta](3) &= \alpha(\beta(3)) = \alpha(2) = 3 \end{aligned}$$

Thus

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \gamma$$

Note that in $\alpha \circ \beta$, β is applied first and α next.
Here is the table of the group S_3



$\circ$	ε	α	β	γ	δ	κ
ε	ε	α	β	γ	δ	κ
α	α	ε	γ	β	κ	δ
β	β	κ	δ	α	ε	γ
γ	γ	δ	κ	ε	α	β
δ	δ	γ	ε	κ	β	α
κ	κ	β	α	δ	γ	ε

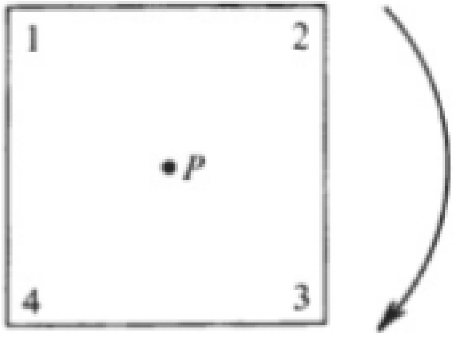
Definition 6.6. The inverse of any permutation of A is a permutation of A. Furthermore, if f is any permutation of A and f^{-1} is its inverse, then

$$f^{-1} \circ f = \varepsilon \text{ and } f \circ f^{-1} = \varepsilon$$

Definition 6.7. For any set A, the group of all the permutations of A is called the symmetric group on A, represented by S_A

Definition 6.8. For any positive integer n, the symmetric group on the set $\{1, 2, 3, \dots, n\}$ is called the symmetric group on n elements, denoted by S_n

Example 6.2. Group of Symmetries of the Square: Think of a symmetry of the square as any way of moving a square to make it coincide with its former position. Every time we do this, vertices will coincide with vertices, so a symmetry is completely described by its effect on the vertices.
Number the vertices as follows:



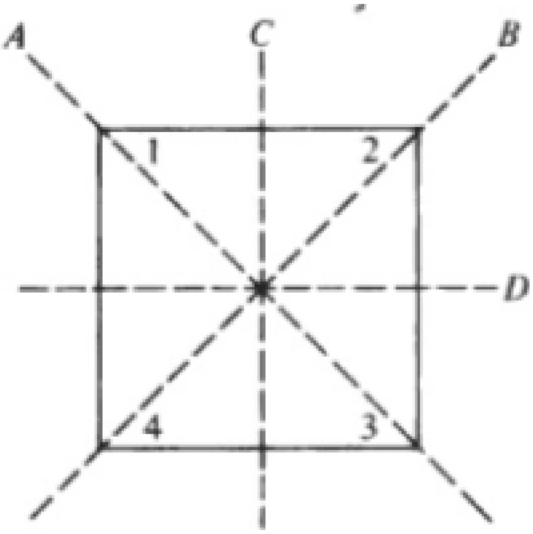
The most obvious symmetries are obtained by rotating the square clockwise around its center P, through angles of 90°, 180° and 270° respectively. Each symmetry is indicated as a permutation of the vertices, thus a clockwise rotation of 90° yields the symmetry

$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

for this rotation carries vertex 1 to 2, 2 to 3, 3 to 4 and 4 to 1. Rotations of 180° and 270° yield the following symmetries respectively

$$R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

The remaining symmetries are flips of the square about its axes A, B, C and D as follows



When the square is flipped about the axis A, vertices 1 and 3 stay put but 2 and 4 change places to get the following symmetry

$$R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

In the same way, the other flips are

$$R_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad R_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

and

$$R_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

The last symmetry is the identity

$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

which leaves the square as it is.
sim
The operation on symmetries is composite; $R_i \circ R_j$ is the result of first performing R_j and then R_i. For example, $R_1 \circ R_4$ is the result of first flipping the square about its axis A and then rotating it clockwise 90°

$$\begin{aligned} R_1 \circ R_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = R_6 \end{aligned}$$

Thus the net effect is the same as if the square had been flipped about its axis C.
sim
The eight symmetries of the square form a group under the operation $\circ$ of composition, called the group of symmetries of the square.

Definition 6.9. For every positive integer $n \geq 3$, the regular polygon with n sides has a group of symmetries, symbolized by D_n. The groups are called the dihedral groups.

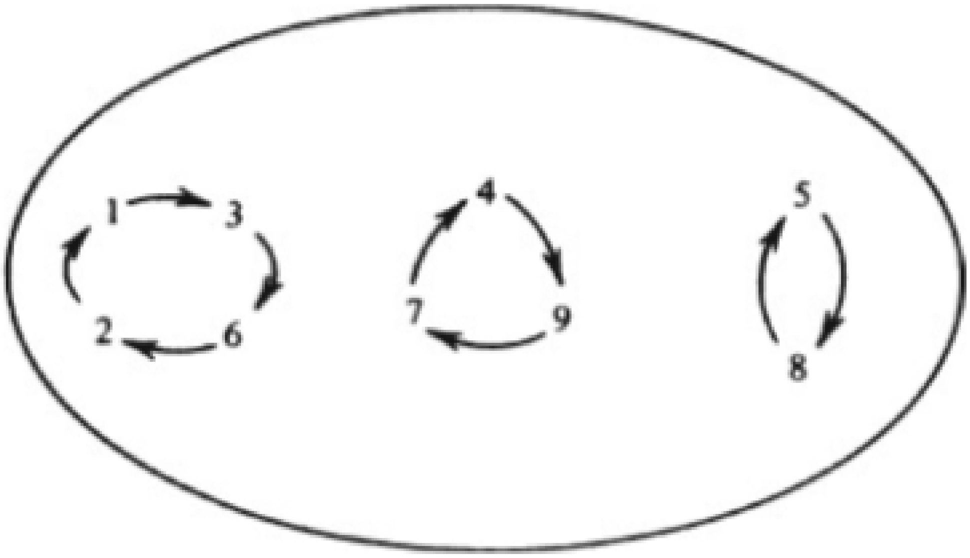
7 Permutations of a Finite Set

Definition 7.1. If n is a positive integer, consider a set of n elements, $\{1, 2, \dots, n\}$. The group of all the permutations of this set is called the symmetric group on n elements and is denoted by S_n.

Example 7.1. f is the permutation as follows

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 9 & 8 & 2 & 4 & 5 & 7 \end{pmatrix}$$

f moves the elements in its domain as follows:



Note how f decomposes its domain into three separate subsets, so that, in each subset, the elements are permuted cyclically so as to form a closed chain.

Definition 7.2. Let $a_1, a_2, \dots, a_s$ be distinct elements of the set $\{1, 2, \dots, n\}$. By the cycle $(a_1 a_2 \dots a_s)$ we mean the permutation

$$a_1 \to a_2 \to a_3 \to \cdots \to a_{s_1} \to a_s \to a_1$$

and so forth of $\{1, 2, \dots, n\}$ which carries a_1 to a_2, a_2 to a_3, ,,,, a_{s-1} to a_s and a_s to a_1, which leaving all the remaining elements of $\{1, 2, \dots, n\}$ fixed.

Example 7.2. In S_6, the cycle (1246) is the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$$

In S_5, the cycle (254) is the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$$

Definition 7.3. The composite of cycles is generally called the product and it is customary to omit the symbol $\circ$

Example 7.3. In S_5,

$$\begin{aligned} (254)(124) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix} \end{aligned}$$

It is very easy to compute the product of two cycles by reasoning in the following manner.

$$(\underbrace{2\ 4\ 5}_{\alpha})(\underbrace{1\ 2\ 4}_{\beta})$$

Remember that the permutation on the right is applied first and the permutation on the left is applied next. Now,
β carries 1 to 2, and α carries 2 to 4; hence $\alpha\beta$ carries 1 to 4
β carries 2 to 4, and α carries 4 to 5; hence $\alpha\beta$ carries 2 to 5
β carries 3 fixed and so does α; hence $\alpha\beta$ leaves 3 fixed
β carries 4 to 1 and α leaves 1 fixed; so $\alpha\beta$ carries 4 to 1
β leaves 5 fixed and α carries 5 to 2; hence $\alpha\beta$ carries 5 to 2

Definition 7.4. If $(a_1a_2\dots a_s)$ is a cycle, the integer s is called its length; thus $(a_1a_2\dots a_s)$ is a cycle of length s

Definition 7.5. If two cycles have no elements in common they are said to be disjoint

Note: Disjoint cycles comment; that is, if $(a_1\dots a_r)$ and $(b_1\dots b_s)$ are disjoint, then

$$(\underbrace{a_1\dots a_r}_{\alpha})(\underbrace{b_1\dots b_s}_{\beta}) = (\underbrace{b_1\dots b_s}_{\beta})(\underbrace{a_1\dots a_r}_{\alpha})$$

Theorem 7.1. Every permutation is either the identity, a single cycle, or a product of disjoint cycles

Example 7.4. Consider the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$$

and let us write f as a product of disjoint cycles. We begin with 1 and note that

$$1 \xrightarrow{f} 3 \xrightarrow{f} 5 \xrightarrow{f} 1$$

This is a complete cycle, which is (135). Next, take the first number which hasn't yet been used, namely, 2. We see that

$$2 \xrightarrow{f} 4 \xrightarrow{f} 2$$

This is a complete cycle, (24). The only remaining number is 6, which is fixed. Thus

$$f = (135)(24)$$

Note: The product of cycles is unique, except for the order of the factors.

Definition 7.6. A cycle of length 2 is called a transposition. In other words, a transposition is a cycle (a_i, a_j) which interchanges the two numbers a_i and a_j. Every cycle can be expressed as a product of one or more transpositions. in fact,

$$(a_1a_2\dots a_r) = (a_ra_{r-1})(a_ra_{r-2})\dots(a_ra_3)(a_ra_2)(a_ra_1)$$

Example 7.5. Note the following

$$\begin{aligned}(12345) &= (54)(53)(52)(41)\\ &= (15)(14)(13)(12)\\ &= (54)(52)(51)(14)(32)(41)\end{aligned}$$

This shows that every permutation, after it has been decomposed into disjoint cycles, may be broken down further and expressed as a product of transpositions. However, the expression as a product of transpositions is not unique and even the number of transpositions involved is not unique.

Definition 7.7. A permutation is called even if it is a product of an even number of transpositions and odd if it is a product of odd number of transpositions

Theorem 7.2. No matter how ε is written as a product of transpositions, the number of transpositions is even

Theorem 7.3. If $\pi \in S_n$, then π cannot be both an odd permutation and an even permutation

Definition 7.8. The set of all the even permutations in S_n is a subgroup of S_n. It is denoted by A_n and is called the alternating group on the set $\{1, 2, \dots, n\}$

8 Isomorphism

Definition 8.1. If G_1 and G_2 are any groups, an isomorphism from G_1 to G_2 is a one-to-one correspondence f from G_1 to G_2 with the following property: For every pair of elements a and b in G_1,

$$\text{If } f(x) = a' \text{ and } f(b) = b' \text{ then } f(ab) = a'b'$$

In other words, let G_1 and G_2 be groups. A bijective function $f : G_1 \to G_2$ with the property that for any two elements a and b in G_1,

$$f(ab) = f(a)f(b)$$

is called an isomorphism from G_1 to G_2.

Definition 8.2. If there exists an isomorphism from G_1 to G_2, then G_1 is isomorphic to G_2 and can be written as

$$G_1 \cong G_2$$

To Recognize if Two Groups are Isomorphic:

1. Make an educated guess and come up with a function $f : G_1 \mathcal{F} G_2$ which looks as though it might be an isomorphism

2. Check that f is injective and surjective

3. Check that f satisfies the identity

$$f(ab) = f(a)f(b)$$

Example 8.1. $\mathbb{R}$ under addition

To Recognize if Two Groups are not Isomorphic:

1. Perhaps G_1 is commutative and G_2 is not
2. Perhaps G_1 has an element which is its own inverse and G_2 does not
3. Perhaps G_1 is generated by two elements whereas G_2 is not generated by any choice of two of its elements
4. Perhaps every element of G_1 is the square of an element of G_1 whereas G_2 does not have this property

Note: This list is not exhaustive. Be on the lookout for properties which do not depend merely on the names assigned to individual elements.

Definition 8.3. If G_1 and G_2 cannot be put in one-to-one correspondence (say G_1 has more elements than G_2), clearly they cannot be isomorphic.

Theorem 8.1. Cayley's Theorem: Every group is isomorphic to a group of permutations.

9 Order of Group Elements

Definition 9.1. Let G be an arbitrary group, with its operation denoted multiplicatively. Exponential notation is a convenient shorthand: for any positive integer n, let

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ times}}$$

$$a^{-n} = \underbrace{a^{-1}a^{-1}\dots a^{-1}}_{n \text{ times}}$$

and

$$a^0 = e$$

Theorem 9.1. Laws of Exponents: If G is a group and $a \in G$, the following identities hold for all integers m and n:

- $a^m a^n = a^{m+n}$
- $(a^m)^n = a^{mn}$
- $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

Theorem 9.2. Division Algorithm: If m and n are integers and n is positive, there exist unique integers q and r such that

$$m = nq + r \text{ and } 0 \geq r < n$$

q is called the quotient and r is the remainder in the division of m by nx.

Definition 9.2. Let G be a group and a an element of G. If there exists a nonzero integer m such that $a^m = e$, then there exists a positive integer n such that $a^n = e$.

Definition 9.3. If there exists a nonzero integer m such that $a^m = e$, then the order of the element a is defined to be the least positive integer n such that $a^n = e$. If there does not exist any nonzero integer m such that $a^m = e$, then a has order infinity.

Note: In $\mathbb{Z}$, every nonzero number has infinite order.

Theorem 9.3. Let G be an arbitrary group and a is any element of G. If the order of a is n, there are exactly n different powers of a, namely

$$a^0, a, a^2, a^3, \dots, a^{n-1}$$

Theorem 9.4. Let G be an arbitrary group and a is any element of G. Suppose an element a in the group G has order n. Then $a^t = e$ if and only if t is a multiple of n.

10 Cyclic Groups

Definition 10.1. If G is a group and $a \in G$, it may happen that every element of G is a power of a.

$$G = \{a^n : n \in \mathbb{Z}\}$$

In that case, G is called a cyclic group and a is called its generator.

$$G =< a >$$

Definition 10.2. If $G =< a >$ is the cyclic group generated by a and a has order n, then G is a cyclic group of order n. If the generator of G has order infinity, then G is cyclic group of order infinity.

Theorem 10.1. Isomorphism of Cyclic Groups

1. For every positive integer n, every cyclic group of order n is isomorphic to $\mathbb{Z}_n$. thus, any two cyclic groups of order n are isomorphic to each other.

2. Every cyclic group of order infinity is isomorphic to $\mathbb{Z}$ and therefore any two cyclic groups of order infinity are isomorphic to each other.

If G is any group and $a \in G$, it is easy to see that

- The product of any two powers of a is a power of a: $a^m a^n = a^{m+n}$

- The inverse of any power of a is a power of a because $(a^n)^{-1} = a^{-n}$
- The set of all the powers of a is a subgroup of G

This subgroup is called the cyclic subgroup of G generated by a.

Theorem 10.2. Every subgroup of a cyclic group is cyclic.

Definition 10.3. Let a be an element of order n in a group G. There are exactly n different powers of a, hence $< a >$ has n elements. Thus, if $\text{ord}(a) = n$, then $| < a > | = n$. That is, the order of a cyclic group is the same as the order of its generator.

11 Partitions and Equivalence Relations

Definition 11.1. By a partition of a set A, we mean a family $\{A_i : i \in I\}$ of nonempty subsets of A such that:

- If any two classes, say A_i and A_j, have a common element x (that is, are not disjoint), then $A_i = A_j$ and
- Every element x of A lies in one of the classes

By an equivalence relation on a set A, we mean a relation $\sim$ which is:

- Reflexive: that is, $x \sim x$ for every x in A
- Symmetric: that is, if $x \sim y$, then $y \sim x$
- Transitive: that is, if $x \sim y$ and $y \sim z$ then $x \sim z$

Note: Two elements are "equivalent" if they are members of the same class.

Definition 11.2. Let $\sim$ be an equivalence relation on A and x an element of A. The set of all the elements equivalent to x is called the equivalence class of x and is denoted by $[x]$. In symbols,

$$[x] = \{y \in A : y \sim x\}$$

Property: If $x \sim y$, then $[x] = [y]$. In other words, if two elements are equivalent, they have the same equivalence class.

Theorem 11.1. If $\sim$ is an equivalence relation on A, the family of all the equivalence classes, that is, $\{[x] : x \in A\}$, is a partition on A.

When $\sim$ is an equivalence relation on A and A is partitioned into its equivalence classes, this partition is called the partition determined by the equivalence relation $\sim$.

12 Counting Cosets

Definition 12.1. Let G be a group and H a subgroup of G. For any element a in G, the symbol

$$aH$$

denotes the set of all products ah, as a remains fixed and h ranges over H. aH is called a left coset of H in H.
In similar fashion

$$Ha$$

denotes the set of all products ha as a remains fixed and h ranges over H. Ha is called a right coset of H in G.

Note: It will not make a difference which coset you use as long as you are consistent.
Fact: Every coset in group G is a subset of G. To prove that two cosets Ha and Hb are equal, show that they are equal sets; which means, show that every element $x \in Ha$ is in Hb and every element $y \in Hb$ is in Ha.

Fact: If $a \in Hb$, then $Ha = Hb$.

Theorem 12.1. The family of all the cosets Ha, as a ranges over G, is a partition of G.

Theorem 12.2. If Ha is any coset of H, there is a one-to-one correspondence from H to Ha.
A consequence of this is that all cosets of H have the same number of elements.

Note: The number of elements in G is equal to the number of elements in H, multiplied by the number of distinct cosets of H.

Theorem 12.3. Lagrange's Theorem: Let G be a finite group and H any subgroup of G. The order of G is a multiple of the order of H.

Theorem 12.4. If G is a group with a prime number p of elements, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G.

Theorem 12.5. The order of any element of a finite group divides the order of the group.

Definition 12.2. If G is a group and H is a subgroup of G, the index of H in G is the number of cosets of H in G, denoted by $(G : H)$. Since the number of elements in G is equal to the number of elements in H, multiplied by the number of cosets of H in G,

$$(G : H) = \frac{\text{order of } G}{\text{order of } H}$$

13 Homomorphisms

Definition 13.1. If G and H are groups, a homomorphism from G to H is a function $f : G \to H$ such that for any two elements a and b in G,

$$f(ab) = f(a)f(b)$$

If there exists a homomorphism from G onto H, then H is a homomorphic image of G.

Theorem 13.1. Let G and H be groups and $f : G \to H$ a homomorphism. Then

1. $f(e) = e$
2. $f(a^{-1}) = [f(a)]^{-1}$ for every element $a \in G$

Definition 13.2. Let H be a subgroup of a group G. H is called a normal subgroup of G if it is closed with respect to conjugates, that is, if

$$\text{for any } a \in H \text{ and } x \in G \text{ then } xax^{-1} \in H$$

Definition 13.3. Let $f : G \to H$ be a homomorphism. The kernel of f is the set K of all the elements of G which are carried by f onto the neutral element of H. That is,

$$K = \{x \in G : f(x) = e\}$$

Theorem 13.2. Let $f : G \to H$ be a homomorphism.

1. The kernel of f is a normal subgroup of G
2. The range of f is a subgroup of H

Note: If f is a homomorphism, the kernel of f and the range of f are represented as follows

$$\ker(f) \text{ and } \operatorname{ran}(f)$$

14 Quotient Groups

Theorem 14.1. If H is a normal subgroup of G, then $aH = Ha$ for every $a \in G$.

In other words, there is no distinction between left and right cosets for a normal subgroup.

Definition 14.1. Coset Multiplication: Let G be a group and let H be a subgroup of G. The coset of a, multiplied by the coset of b, is defined to be the coset of ab

$$Ha \cdot Hb = H(ab)$$

Theorem 14.2. Let H be a normal subgroup of G. If $Ha = He$ and $Hb = Hd$, then $H(ab) = H(cd)$.

Definition 14.2. Let G be a group and let H be a normal subgroup of G. The set consisting of all the cosets of H is denoted by the symbol G/H. Thus if Ha, Hb, He, $\dots$, are cosets of H then

$$G/H = \{Ha, Hb, Hc, \dots\}$$

Theorem 14.3. *G/H with coset multiplication is a group.*

Definition 14.3. The group G/H is called the factor group, or quotient group of G by H.

Theorem 14.4. *G/H is a homomorphic image of G.*

Theorem 14.5. *Let G be a group and H a subgroup of G. Then*

1. *$Ha = Hb$ iff $ab^{-1} \in H$*
2. *$Ha = H$ iff $a \in H$*

Definition 14.4. Let G be an arbitrary group; by a commutator of G, we mean any element of the form $aba^{-1}b^{-1}$ where a and b are in G

$$aba^{-1}b^{-1} = e \text{ iff } ab = ba$$

In other words, $aba^{-1}b^{-1}$ reduces to the neutral element whenever a and b commute.

Note: When we factor out the commutators of G, we get a quotient group which has no commutators and is therefore abelian.

Definition 14.5. To say that G/H is abelian is to say that any two elements Hx and Hy in G/H, $HxHy = HyHx$; that is, $Hxy = Hyx$. But

$$Hxy = Hyx \text{ iff } xy(yx)^{-1} \in H$$

Now $xy(yx)^{-1}$ is the commutator $xyx^{-1}y^{-1}$; so if all commutators are in H then G/H is abelian.

15 The Fundamental Homomorphism Theorem

Let G be any group. Every quotient group of G is a homomorphic image of G. It is also true that ever homomorphic image of G is isomorphic to a quotient group of G. It follows that, for any groups G and H, H is a homomorphic image of G iff H is (or is isomorphic to) a quotient group of G.

Theorem 15.1. *Let $f : G \to H$ be a homomorphism with kernel K. Then*

$$f(a) = f(b) \text{ iff } Ka = Kb$$

In other words, any two elements a and b in G have the same image under f iff they are in the same coset of K.

This says that if f is a homomorphic from G to H with kernel K, then all the elements in any fixed coset of K have the same image, and conversely, elements which have the same image are in the same coset of K.

Theorem 15.2. Let $f : G \to H$ be a homomorphism of G onto H. If K is the kernel of f, then

$$H \cong G/K$$

The above theorem is often called the Fundamental Homomorphism Theorem. It asserts that every homomorphic image of G is isomorphic to a quotient group of G. Which specific quotient group of G? If f is a homomorphism from G onto H, then H is isomorphic to the quotient group of G by the kernel of f.

Note: The fact that f is a homomorphism from G onto H may be symbolized by writing

$$f : G \twoheadrightarrow H$$

Furthermore, the fact that K is the kernel of this homomorphism may be indicated by writing

$$f : G \twoheadrightarrow_K H$$

Thus, the fundamental homomorphism theorem says that

$$\text{If } f : G \twoheadrightarrow_K H \text{ then } H \cong G/H$$

16 Rings: Definitions and Elementary Properties

Definition 16.1. By a ring, we mean a set A with operations called addition and multiplication which satisfy the following axioms:

1. A with addition alone is an abelian group
2. Multiplication is associative
3. Multiplication is distributive over addition. That is, for all a, b, and c in A,

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

and

$$(b + c)a = ba + ca$$

Note: Since A with addition alone is an abelian group, there is in A a neutral element for addition called the zero element and is written 0. Also, every element has an additive inverse called its negative; the negative of a is denoted by $-a$.

Example 16.1. The set $\mathbb{Z}$ of the integers, with conventional addition and multiplication, is a ring called the ring of the integers and is denoted $\mathbb{Z}$. Similarly, $\mathbb{Q}$ is the ring of rational numbers, $\mathbb{R}$ is the ring of the real numbers and $\mathbb{C}$ is the ring of the complex numbers, each under conventional addition and multiplication.

Example 16.2. $\mathcal{F}(\mathbb{R})$ represents the set of all the functions from $\mathbb{R}$ to $\mathbb{R}$ and with the operation of addition and multiplication of functions, it is a ring, called the ring of real functions.

Definition 16.2. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathcal{F}(\mathbb{R})$ are all infinite rings, that is, rings with infinitely many elements.
There are also finite rings: rings with a finite number of elements. Examples of these are $\mathbb{Z}_n$.

Note: Let A be any ring. Since A with addition alone is an abelian group, the following is true for ring A

$$a + b = a + c \text{ implies } b = c$$

$$a + b = 0 \text{ implies } a = -b \text{ and } b = -a$$

$$-(a + b) - -a + -b \text{ and } -(-a) = a$$

These statements are true in every ring,

Theorem 16.1. Let a and b be any elements of a ring A.

1. $a0 = 0$ and $0a = 0$
2. $a(-b) = -(ab)$ and $(-a)b = -(ab)$
3. $(-a)(-b) = ab$

Definition 16.3. By definition, addition is commutative in every ring but multiplication is not. When multiplication also is commutative in a ring, that ring is called a commutative ring.

Definition 16.4. If there is in ring A a neutral element for multiplication, it is called the unity of A and is denoted by the symbol 1. Thus $a \cdot 1 = a$ and $1 \cdot a = a$ for every a in A. If A has a unity, A is a ring with unity.

Example 16.3. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathcal{F}$ are all examples of commutative rings with unity.

Definition 16.5. A ring whole only element is 0 is called a trivial ring; a ring with more than one element is nontrivial. In a nontrivial ring with unity, necessarily $1 \neq 0$. This is true because if $1 = 0$ and x is any element of the ring, then

$$x = x1 = x0 = 0$$

In other words, if $1 = 0$ then every element of the ring is equal to 0; hence 0 is the only element of the ring.

Definition 16.6. If A is a ring with unity, they may be elements in A which have a multiplicative inverse. Such elements are said to be invertible. Thus, an element a is invertible in a ring if there is some x in the ring such that

$$ax = xa = 1$$

Note: Zero is never an invertible element of a ring except if the ring is trivial.

Definition 16.7. If A is a commutative ring with unity in which every nonzero element is invertible, A is called a field.

Example 16.4. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

Definition 16.8. In any ring, a nonzero element a is called a divisor of zero if there is a nonzero element b in the ring such that the product ab or ba is equal to zero.

Note: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ do not have any divisors of zero.

Definition 16.9. A ring is said to have the cancellation property if

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

for any elements a, b, and c in the ring if $a \neq 0$.

Theorem 16.2. A ring has the cancellation property if and only if it has no divisors of zero.

Definition 16.10. An integral domain to defined to be a commutative ring with unity having the cancellation property. It may also be defined as a commutative ring with ring having no divisors of zero.

Note: If is easy to see that every field is an integral domain. The converse is not true though.

Example 16.5. $\mathbb{Z}$ is an integral domain but not a field.

17 Ideals and Homomorphisms

Definition 17.1. If a nonempty subset $B \subseteq A$ is closed with respect to addition, multiplication and negatives, then B with the operations of A is a ring.

Definition 17.2. B is a subring of A if and only if B is closed with respect to subtraction and multiplication.

Definition 17.3. Let A be a ring and B a nonempty subset of A. B is called an ideal of A if B is closed with respect to addition and negatives and B absorbs products in A

$$\forall b \in B \text{ and } x \in A, xb \text{ and } bx \text{ are in } B$$

Example 17.1. In a commutative ring with unity, the simplest example of an ideal is the set of all the multiplies of a fixed element a by all the elements in the ring. In other words, the set of all the products xa as a remains fixed and x ranges over all the elements of the ring. this set is an ideal because

$$xa + ya = (x + y)a$$

$$-(xa) = (-x)a$$

and

$$y(xa) = (yx)a$$

This ideal is called the principal ideal generated by a and is denoted by $\langle a \rangle$.

Definition 17.4. If B is a nonempty subset of A then B is an ideal of A if and only if B is closed with respect to subtraction and B absorbs products in A.

Definition 17.5. A homomorphism from a ring A to a ring B is a function $f : A \to B$ satisfying the identities

$$f(x_1 + x_2) = f(x_1) + f(x_2)$$
$$f(x_1x_2) = f(x_1)f(x_2)$$

Note: If there is a homomorphism from A onto B, we call B a homomorphic image of A. If f is a homomorphism from a ring A to a ring B, not necessarily onto, the range is a subring of B. Thus, the range of a ring homomorphism is always a ring.

Definition 17.6. If f is a homomorphism from a ring A to a ring B, the kernel of f is the set of all the elements of A which are carried by f onto the zero element of B. In symbols, the kernel of f is the set

$$K = \{x \in A : f(x) = 0\}$$

Note: The kernel of f is an ideal of A.

Definition 17.7. If A and B are rings, an isomorphism from A to B is a homomorphism which is a one-to-one correspondence from A to B. In other words, it is an injective and surjective homomorphism. If there is an isomorphism from A to B, then A is isomorphic to B

$$A \cong B$$

18 Quotient Rings

Definition 18.1. Let A be a ring and J an ideal of A. For any elements $a \in A$, the symbol $J + a$ denotes the set of all sums $j + a$ as a remains fixed and j ranges over J. That is,

$$J + a = \{j + a : j \in J\}$$

$J + a$ is called a coset of J in A.

If we provisionally ignore multiplication, A with addition alone is an abelian group and J is a subgroup of A. Thus, the cosets are precisely the cosets of the subgroup J in the group A, with the notation being additive. In additive notation:

$$\begin{aligned} a \in J + b &\iff J + a = J + b \\ J + a = J + b &\iff a - b \in J \\ J + a = J &\iff a \in J \end{aligned}$$

By the reasoning which lead up to Lagrange's Theorem, the family of all the cosets $J + a$ as a ranges over A, is a partition of A.
There is a way of adding and multiplying cosets which works as follows:

$$(J + a) + (J + b) = J + (a + b)$$
$$(J + a)(J + b) = J + ab$$

In other words, the sum of the coset of a and the coset of b is the coset of $a + b$; the product of the coset of a and the coset of b is the coset of ab.

Theorem 18.1. Let J be an ideal of A. If $J + a = J + c$ and $J + b = J + d$, then

1. $J + (a + b) = J + (c + d)$
2. $J + ab = J + cd$

Definition 18.2. The set which consists of all the cosets of J in A is

$$A/J = \{J + a, J + b, J + c, \dots\}$$

Theorem 18.2. A/J with coset addition and multiplication is called the quotient ring of A by J.

Theorem 18.3. A/J is a homomorphic image of A.

Definition 18.3. The natural homomorphism from A onto A/J is the function f which carries every element to its own coset, that is, the function f given by

$$f(x) = J + x$$

Theorem 18.4. Fundamental Homomorphism Theorem for Rings: Let $f : A \to B$ be a homomorphism from a ring A onto a ring B and let K be the kernel of f. Then $B \cong A/K$.

Therefore, every quotient ring of A is a homomorphic image of A and conversely, every homomorphic image of A is isomorphic to a quotient ring of A. Thus, quotients and homomorphic images of a ring are the same.

Let A be a ring and let J be an ideal of A which contains all the differences $ab - ba$ as a and b ranges over A. Then A/J is commutative. In other words, for any two cosets $J + a$ and $J + b$,

$$(J + a)(J + b) = (J + b)(J + a) \text{ that is } J + ab = J + ba$$

This is true if and only if $ab - ba \in J$ Thus, if every difference $ab - ba \in J$, then any two cosets commute.

Definition 18.4. An ideal J of a commutative ring is said to be a prime ideal if for any two elements a and b in the ring, if $ab \in J$ then $a \in J$ or $b \in J$. Note: Whenever J is a prime ideal of a commutative ring with unity A, the quotient ring A/J is an integral domain.

Definition 18.5. An ideal of a ring is called proper if it is not equal to the whole ring.

Definition 18.6. A proper ideal of a ring A is called a maximal ideal if there exists no proper ideal K of A such that $J \subseteq K$ with $J \neq K$.

Note: If A is a commutative ring with unity, then J is a maximal ideal of A if and only if A/J is a field.

19 Factoring into Primes

Theorem 19.1. Every ideal of $\mathbb{Z}$ is principal.

Definition 19.1. If r and s are integers, then s is a multiple of r if there is an integer k such that

$$s = rk$$

If this is the case, then r is a factor of s, or r divides s, denoted by

$$r|s$$

Theorem 19.2. The only invertible elements of $\mathbb{Z}$ are 1 and -1.

Definition 19.2. A pair of integers r and s are called associates if they divide each other, that is, if $r|s$ and $s|r$. If r and s are associates, this means there are integers k and l such that $r = ks$ and $s = lr$. Thus $r = ks = klr$, hence $kl = 1$. By the above theorem, k and l are ± 1 and therefore $r = \pm s$. Thus, if r and s are associates in $\mathbb{Z}$, then $r = \pm s$.

Definition 19.3. An integer t is called a common divisor of integers r and s if $t|r$ and $t|s$.

Definition 19.4. A greatest common divisor of r and s is an integer t such that

1. $t|r$ and $t|s$
2. For any integer u, if $u|r$ and $u|s$ then $u|t$

Theorem 19.3. Any two nonzero integers r and s have a greatest common divisor t. Furthermore, t is equal to a linear combination of r and s. That is,

$$t = kr + ls$$

for some integers k and l.

Definition 19.5. A pair of integers r and s are said to be relatively prime if they have no common divisors except ± 1.

Definition 19.6. If m is any integer, the trivial factors of m are ± 1 and $\pm m$. If m has any other factors, those are proper factors of m.

Definition 19.7. If an integer m has proper factors, m is called composite. If an integer $p \neq 0, 1$ has no proper factors, then p is called prime.

Theorem 19.4. If a positive integer m is composite, then $m = rs$ where $1 < r < m$ and $1 < s < m$.

Theorem 19.5. Let m and n be integers and let p be a prime. If $p|(mn)$, then either $p|m$ or $p|n$.

Theorem 19.6. Let $m_1, \dots, m_t$ be integers and let p be a prime. If $p|(m_1 \dots m_t)$ then $p|m_i$ for one of the factors m_i among $m_1, \dots, m_t$.

Theorem 19.7. Let $q_1, \dots, q_t$ and p be positive primes. If $p|(q_1 \dots q_t)$ then p is equal to one of the factors $q_1, \dots, q_t$.

Theorem 19.8. Every integer $n > 1$ can be expressed as a product of positive primes. That is, there are one or more primes $p_1, \dots, p_r$ such that

$$n = p_1 p_2 \dots p_r$$

Theorem 19.9. Suppose n can be factored into positive primes in two ways, namely,

$$n = p_1 \dots p_r = q_1 \dots q_r$$

Then $r = t$ and the p_i are the same numbers as the q_j except, possibly, for the order in which they appear.

Note: Every integer m can be factored into primes and the prime factors of m are unique.