MAT 351 Supplementary Notes on Groups Spring 2013

(Note: These notes are meant to supplement the lectures. Full lecture notes can only be obtained by attending class lectures and taking notes.)

Binary Operation

A binary operation on a set S is a function from $S \times S$ to S.

Addition and multiplication are binary operations on the set $\mathbb{Z}$ of integers.

Definition of a Group A group is a set G, together with a binary operation $*$ satisfying the following properties:

- Associativity: The binary operation $*$ is associative.
- Identity property: There exists an element e in G such that $a * e = e * a = a$ for all $a \in G$.
- Inverse property: For each $a \in G$ there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Observations on the definition of a group:

- A binary operation is assumed to be a function from $G \times G$ to G, written $* : G \times G \longrightarrow G$, meaning that $*$ takes as input two elements of G and outputs one element of G.
- Sometimes G will used to indicate the set of elements, and sometimes it will be used to indicate the whole group with binary operation implied.
- Other notations (symbols) for a group, binary operation, identity and inverses will be used. The most common operations are multiplication (usually indicated with concatenation) and addition.

Alternative definition of group:

Suppose G is a nonempty set with an associative binary operation $*$, satisfying the property that for any $a, b \in G$, the equation $a * x = b$ has a unique solution for x, and for $c, d \in G$, the equation $y * c = d$ has a unique solution for y. Then G is a group with binary operation $*$.

Proof:

We need to show that there exists an (identity) element $e \in G$, with the property that $e * a = a * e = a$ for all $a \in G$, and that for any $a \in G$ there exists $b \in G$ (the inverse of a) such that: $a * b = e = b * a$.

Let $a, b \in G$, and let e_1 be the unique solution to the equation $a * x = a$ and let e_2 be the unique solution to $y * b = b$. Then $a * e_1 = a$ and $e_2 * b = b$. Then we can write:

$$a * b = a * (e_2 * b) = (a * e_2) * b.$$

This says that $a * e_2$ is a solution to the equation $y * b = (a * b)$. Since a is also obviously a solution, and by uniqueness of solutions, we get $a * e_2 = a$. But e_1 is the unique solution to $a * x = a$, so we get $e_1 = e_2$. So we have that a right identity for any element is equal to a left identity for any other element, and thus there exists one element e with the property that $a * e = e * a = a$ for all $a \in G$.

Now let $a \in G$, and let b be the unique solution to $a * x = e$. We would like to show that $b * a = e$ as well, so that b satisfies the property of an inverse of a. If we multiply $a * b = e$ on the left by b we have $b * (a * b) = b * e = b$. Then by associativity we have $(b * a) * b = b$ and by the uniqueness of e as solution of $y * b = b$ from above, we get $b * a = e$. This completes the proof.

Examples:

- Let $G = \{0, 1\}$, and let $*$ be addition modulo 2. Then we can write:

$$0 * 0 = 0, \quad 0 * 1 = 1, \quad 1 * 0 = 1, \quad \text{and } 1 * 1 = 0.$$

To check that $*$ is associative, we write all eight possible strings of values for three elements a,b,c:

a, b, c	$a * (b * c)$	$(a * b) * c$
$0, 0, 0$	$0 * (0 * 0) = 0$	$(0 * 0) * 0 = 0$
$1, 0, 0$	$1 * (0 * 0) = 1$	$(1 * 0) * 0 = 1$
$0, 1, 0$	$0 * (1 * 0) = 1$	$(0 * 1) * 0 = 1$
$0, 0, 1$	$0 * (0 * 1) = 1$	$(0 * 0) * 1 = 1$
$1, 1, 0$	$1 * (1 * 0) = 0$	$(1 * 1) * 0 = 0$
$1, 0, 1$	$1 * (0 * 1) = 0$	$(1 * 0) * 1 = 0$
$0, 1, 1$	$0 * (1 * 1) = 0$	$(0 * 1) * 1 = 0$
$1, 1, 1$	$1 * (1 * 1) = 1$	$(1 * 1) * 1 = 1$

To check the identity property, we see that $e = 0$ satisfies all the properties of the identity. We can also see that 0 has inverse 0, and 1 has inverse 1. This verifies all properties of a group. We can also write a group table which shows all operations, where the left side represents the left element a in an operation $a * b$, and the element b comes from the top row above the table:

$*$	0	1
0	0	1
1	1	0

- Let $G = \{1, -1\}$, and let $*$ be multiplication of integers. Then we can write:

$$1 * 1 = 1, \quad 1 * (-1) = -1, \quad (-1) * 1 = -1, \quad \text{and} \quad (-1) * (-1) = 1.$$

To check that $*$ is associative, we simply appeal to the fact that multiplication of integers is associative. This is indeed the easiest, and most common, way to verify associativity, to observe that it is already guaranteed by the choice of the operation $*$ from a familiar context.

To check the identity property, we see that $e = 1$ satisfies all the properties of the identity. We can also see that 1 has inverse 1, and -1 has inverse -1. This verifies all properties of a group. We can also write a group table as we did for the previous example:

$*$	1	-1
1	1	-1
-1	-1	1

Isomorphic finite groups

We can see that in the previous two examples, the basic structure of the group table is the same, but just with different labels in each case. We say that these two groups are *isomorphic*. Indeed, both tables can be put into the abstract form below, where there is no indication of what the binary operation is. In fact, the binary operation is simply defined by the table.

$*$	e	a
e	e	a
a	a	e

Definition of Isomorphism for finite groups

Two groups are said to be *isomorphic* if their group tables can be made to be the same after relabeling and reordering the elements.

Basic Definitions and Results on Groups

- A subgroup of a group G is a subset H of G which is closed under the binary operation from G and satisfies all the properties of a group within the set H.
- For x in any group G, let $ord(x)$ denote the smallest positive integer k such that $x^k = e$, where $x^k = x*x*\cdots*x$ means x combined (multiplied) with itself (k factors) using the binary operation of G. Thus $ord(e) = 1$ and $ord(x) \geq 2$ for all other elements of G.
- If G is a finite group, then $|G|$ denotes the number of elements of G.
- If G is a finite group and $g \in G$, then $ord(g)$ is the smallest positive integer k such that $g^k = e$.
- (Lagrange Theorem) Let G be any finite group, $a \in G$, and H a subgroup of G. Then $ord(g)$ divides $|G|$, and $|H|$ divides $|G|$.
- In any group G, the identity and inverses are unique.
- In any group G, the cancellation law holds: for $a, b, c \in G$ if $ab = ac$ or $ba = ca$, then we can conclude that $b = c$.
- It is a fact that the orders of elements are preserved by an isomorphism, and the order of any element in a group must be a divisor of the number of elements in the group.
- A group G is called *commutative* if $a * b = b * a$ for all $a, b \in G$.
- The set of permutations (one-to-one functions) of the set $\{1, 2, \ldots, n\}$ to itself is a group, with composition as the binary operation, and there are a total of $n!$ elements in this group.

Additive groups of numbers

The main groups of numbers that we consider are the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, the integers $\mathbb{Z}$, and the complex numbers $\mathbb{C}$. Each of these sets forms a group with binary operation addition, identity element zero, and inverses are the usual negatives. In the case of complex numbers, the addition is equivalent to vector addition in $\mathbb{R}^2$.

There are also subgroups of the form $\mathbb{Z}[\alpha]$ or $\mathbb{Q}[\alpha]$ where α is a transcendental or algebraic number like π or $\sqrt{2}$. These groups are defined as

$$\mathbb{Z}[\alpha] = \{x + y\alpha : x, y \in \mathbb{Z}\} \text{ and } \mathbb{Q}[\alpha] = \{x + y\alpha : x, y \in \mathbb{Q}\},$$

with the same binary operation of addition in $\mathbb{R}$.

Integers modulo n

The group $\mathbb{Z}_n$ consists of the elements $\{0, 1, 2, \ldots, n-1\}$ with the binary operation being addition mod n. This means that for x and y in $\{0, 1, 2, \ldots, n-1\}$ we first add $x + y = z$ as integers, then we subtract n if neccessary to put the result back into the same set $\{0, 1, 2, \ldots, n-1\}$. When we speak of the group $\mathbb{Z}_n$ we implicitly mean both the set $\{0, 1, 2, \ldots, n-1\}$ and the operation of addition mod n.

The group $|\mathbb{Z}_n|$ has order n, ie. $|\mathbb{Z}_n| = n$.

Some Group Tables

- Group table for $\mathbb{Z}_3$: (+ means addition mod 3).

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- Group table for $\mathbb{Z}_4$: (+ means addition mod 4).

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

Symmetry Groups

Symmetry Groups are collections of rigid motions of an object in 3D which preserve the shape of the object. In fact these are always rotations. It is best to make this more precise through some examples.

Examples:

- We start with the "Klein 4-group" (order 4) which is the group of symmetries of a rectangle which is not a square. There are four elements to the group corresponding to the identity, the 2 180-degree rotations about axes through the midpoints of opposite sides, and the axis sticking out through the center of the rectangle. The direction of rotation doesn't matter since the final position of the object is the same.
- Tetrahedron Symmetry Group (order 12)
- Cube Symmetry Group (order 24) is isomorphic to Permuatation Group S_4. (The isomorphism comes from the action of the symmetry rotations on the set of 4 long diagonals of the cube.)

Permutation Groups

We use the notation S_n to denote the permutation group on n elements. To understand this group, we first need some basic definitions and facts about permutations.

A permutation on n elements is a 1-1 function from the set $\{1, 2, \ldots, n\}$ to itself.

Composition of permutations is now just composition of functions. We can give a permutation in a number of different notations. First is the *list* notation. For example

$$5, 3, 4, 1, 2$$

is a reordering of the list $1, 2, 3, 4, 5$. This is the usual way of thinking about permutations. Then there is the *row* notation:

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

which simply emphasizes the original order by writing it along the top. From this we can obtain the function notation also. Here we need to think of the domain and range as the set $\{1, 2, 3, 4, 5\}$. If we input 1, then the output is 5, ie. the number below 1 in the list. Another way to write this as a function is the *mapping* notation:

$$\begin{array}{rcl} 1 & \mapsto & 5 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 4 \\ 4 & \mapsto & 1 \\ 5 & \mapsto & 2 \end{array}$$

Next, if we give the function a name like ϕ, we can use the *explicit functional* notation:

$$\begin{array}{rcl} \phi(1) & = & 5 \\ \phi(2) & = & 3 \\ \phi(3) & = & 4 \\ \phi(4) & = & 1 \\ \phi(5) & = & 2. \end{array}$$

The functional notation can also be inserted back into all of the others just by substitution: ie. since we know that $\phi(1) = 5$, $\phi(2) = 3$, $\phi(3) = 4$, $\phi(4) = 1$, and $\phi(5) = 2$, the original reordered list becomes: $\{\phi(1), \phi(2), \phi(3), \phi(4), \phi(5)\}$.

Next we look at composition of permutations using all of these notations. First, with the functional notation, suppose we have another permutation called ψ given by:

$$\begin{array}{rcl} \psi(1) & = & 2 \\ \psi(2) & = & 4 \\ \psi(3) & = & 3 \\ \psi(4) & = & 1 \\ \psi(5) & = & 5. \end{array}$$

Now to compose the two permutations (as functions) we write $\psi \circ \phi$ to denote the permutation which takes input x and gives output $\psi \circ \phi(x) = \psi(\phi(x))$.

$$\begin{array}{rcccl} \psi \circ \phi(1) & = & \psi(\phi(1)) & = & \psi(5) = 5 \\ \psi \circ \phi(2) & = & \psi(\phi(2)) & = & \psi(3) = 3 \\ \psi \circ \phi(3) & = & \psi(\phi(3)) & = & \psi(4) = 1 \\ \psi \circ \phi(4) & = & \psi(\phi(4)) & = & \psi(1) = 1 \\ \psi \circ \phi(5) & = & \psi(\phi(5)) & = & \psi(2) = 4. \end{array}$$

Associativity of function composition:

It is an important general fact that composition of functions is an associative operation. This works regardles of the types of functions involved, as long as the composition is defined. By this we mean that if f, g and h are functions, and x is in the domain of f, and $f(x)$ is in the domain of g, and $g(f(x))$ is in the domain of h, then the symbol $h(g(f(x)))$ can be evaluated using either $[h \circ (g \circ f)](x)$ or $[(h \circ g) \circ f](x)$, and the answer is the same. If there are no such x, then the composition is simply not defined. Those x for which $h(g(f(x)))$ is defined then make up the domain of the composition function which can be written as:

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

S_n as a group:

Since the composition of permutations as $1-1$ functions is associative, and each $1-1$ function has an inverse, and the identity function is simply $e(x) = x$, we can see that all the group axioms are satisfied.

Disjoint cycle notation:

Cycle notation for permutations consists of a list in parentheses, such as (abc), which is interpreted as a function that takes a to b, b to c, and c to a.

Examples:

- The permutation ϕ which has the function description:

$$\begin{array}{rcl} \phi(1) & = & 2 \\ \phi(2) & = & 3 \\ \phi(3) & = & 1 \end{array}$$

  also has the cycle notation:

$$(123).$$

- The permutation ψ which has the function description:

$$\begin{array}{rcl} \psi(1) & = & 3 \\ \psi(2) & = & 1 \\ \psi(3) & = & 2 \end{array}$$

  also has the cycle notation:

$$(132).$$

Any permutation can be written as a product of disjoint cycles, which can be seen from the process of composition of cycles, working from right to left, just as we do with functions.

Examples:

- The composition of ϕ and ψ from the above examples can be done as:

$$\phi \circ \psi = (123)(132) = (1)(2)(3) = e.$$

- Also:

$$\psi \circ \phi = (132)(123) = (1)(2)(3) = e.$$

- The composition of a 2-cycle and a 3-cycle:

$$(132)(12) = (1)(23) = (23), \quad \text{and} \quad (12)(132) = (13)(2) = (13).$$

- The composition of two 2-cycles:

$$(13)(12) = (123), \quad \text{and} \quad (12)(13) = (132).$$

Group Tables for Permutation Groups S_n:

Examples:

- S_2 has two elements: the identity e and non-identity element a, such that $a(1) = 2$ and $a(2) = 1$, which is the only other $1-1$ function on the set $\{1, 2\}$. The group table is:

$*$	e	a
e	e	a
a	a	e

With disjoint cycle notation, the element a is simply (12). So the table can also be written:

$\circ$	e	(1 2)
e	e	(1 2)
(1 2)	(1 2)	e

- S_3 has six elements: the identity e, and non-identity elements which can be represented as 2-cycles or 3-cycles. These are: (12), (13), (23), (123), (132). The group table is then:

	e	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
e	e	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	e	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	e	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	e	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	e
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	e	(1 2 3)

Note: S_3 is our first example of a non-commutative group.

Finite Quaternion Group

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where the group elements are abbreviations for 2×2 matrices with entries in the complex numbers (matrix entry $i = \sqrt{-1}$) as follows:

$$\pm 1 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm i = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm j = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm k = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Thus Q_8 is realized as a subgroup of $GL_2(\mathbb{C})$.

Exercise: Fill in the following group table for Q_8:

*	1	-1	i	-i	j	-j	k	-k
1								
-1								
i								
-i								
j								
-j								
k								
-k								

List of groups of small order

Here is a summary of our investigations of groups so far, for small orders:

- Order 1: (only 1 isomorphism type) The trivial group consisting only of the identity element $\{e\}$.
- Order 2: (only 1 isomorphism type) The group $\mathbb{Z}_2$, which is isomorphic to $\{1, -1\}$ with multiplication.
- Order 3: (only 1 isomorphism type) The group $\mathbb{Z}_3$
- Order 4: (2 isomorphism types)
  - The group $\mathbb{Z}_4$
  - The group K_4, which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$
- Order 5: (only 1 isomorphism type) The group $\mathbb{Z}_5$
- Order 6: (2 isomorphism types)
  - The group $\mathbb{Z}_6$
  - The group S_3 which is noncommutative
- Order 7: (only 1 isomorphism type) The group $\mathbb{Z}_7$
- Order 8: (4 isomorphism types)
  - The group $\mathbb{Z}_8$
  - The group $\mathbb{Z}_2 \times \mathbb{Z}_4$
  - The group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
  - The finite quaternion group Q_8 which is noncommutative
  - The dihedral group D_4 (symmetries of a square) which is noncommutative

Matrix Groups

- $GL_n(F)$ is the group of invertible $n \times n$ matrices with entries in the field F. (More on fields later - for now think of real or complex numbers.)

- $O_n(F)$ is the group of orthogonal $n \times n$ matrices with entries in the field F, and $SO_n(F)$ is the subgroup of $O_n(F)$ consisting of matrices with determinant 1.
- When F is the real numbers $\mathbb{R}$ we abbreviate $O_n(\mathbb{R})$ as $O(n)$ and $SO_n(\mathbb{R})$ as $SO(n)$.

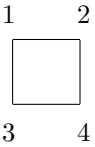
Another special case for F is the finite field $\mathbb{F}_p$ which consists of the set $\mathbb{Z}_p$ for some prime number p with the operations of addition and multiplication mod p.

The group $GL_2(\mathbb{F}_2)$

Product Groups

Dihedral group D_4

The dihedral group D_4 is another example of a symmetry group, in this case for the square. We think of labeling each corner of a square and then rotating it in 3D back to its original image but perhaps with the corners exchanged. There are 8 ways to do this, including the identity element. We can list the elements according to permutation and also rotation. If we start with the original image of the square labelled like this:



then we can choose different axes for rotation, such as

- C: center point (2D rotation)
- V: vertical axis
- H: horizontal axis
- D1: diagonal axis through corners 1 and 4
- D2: diagonal axis through corners 2 and 3

Then the rotation through 180° about V also has the permutation type (12)(34) in disjoint cycle notation. We can then list the elements as:

- e – identity element
- a – V, 180° – (12)(34)
- b – H, 180° – (13)(24)
- c – C, 90° – (2134)
- c^2 – C, 180° – (23)(14)
- c^3 – C, 270° – (2431)
- d – D1, 180° – (23)
- f – D2, 180° – (14)

The group table for D_4 then looks like this:

$*$	e	a	b	c	c^2	c^3	d	f
e	e	a	b	c	c^2	c^3	d	f
a	a	e						
b	b		e					
c	c							
c^2	c^2				c^2			
c^3	c^3							
d	d						e	
f	f							f