

MATH 30A NOTES 2009

These are lecture notes from the first part of the course (sec 1-17) on elementary group theory.

CONTENTS

0. Introduction	2
0.1. Induction	2
0.2. Bijection (a)	2
0.3. Bijection (b)	3
0.4. Bijection (c)	4
0.5. Bijection (d)	4
0.6. Axiom of Choice	5
0.7. Power set	5
0.8. Relations and Cartesian products	6
0.9. Partitions and equivalence	7
0.10. Rhyme schemes and equivalence relations	8
1. Introduction and examples	10
1.1. Integers modulo n	10
1.2. Real numbers modulo a	11
1.3. complex numbers	11
1.4. unit circle	12
2. binary operations	14
3. isomorphic binary structures	16
3.1. showing that two structures are isomorphic	16
3.2. structural properties	17
3.3. finding isomorphisms	17
4. groups	18
4.1. definition of group	18
4.2. examples	19
4.3. cancellation	19
5. subgroups	20
5.1. definition and examples	20
5.2. cyclic subgroup	21
6. cyclic groups	22
6.1. division and order	22
6.2. subgroups of cyclic groups	24

Date: October 31, 2009.

7. Generating sets and Cayley digraphs	26
7.1. more about Cayley digraphs	27
8. Permutation groups	28
8.1. symmetric group	29
8.2. dihedral groups	29
8.3. Cayley's theorem	29
8.4. example of Cayley's theorem	31
9. Orbits, cycles and A_n	32
9.1. orbits	32
9.2. cycles	33
9.3. more about cycles	34
9.4. sign of a permutation	34
9.5. the alternating group A_n	36
10. Cosets	37
10.1. examples	37
10.2. properties of cosets	39
10.3. Lagrange theorem	40
11. Direct product	41
13. Homomorphisms	42
14. Factor groups	45
14.1. Example: \mathbb{Z}/n	46
14.2. Isomorphism theorems	46
15. Simple groups	48
15.1. Center of a group	48
15.2. Commutator subgroup	49
16. Group actions on sets	50
16.1. Definition	50
16.2. Substructures of G -actions on X	52
17. Group actions, continued	55
17.1. orbit-stabilizer	55
17.2. Burnside's theorem	57

0. INTRODUCTION

Algebra is the study of sets with binary operations. So, we will be talking about sets throughout the entire semester. I will spend the first two days reviewing set theory. Note that Math 23 is a prerequisite or corequisite for this course.

My main objective in this course is to teach students the language of Algebra: to understand the definitions and questions and be able to talk about it.

Review of set theory:

- a) Induction.
- b) Bijections and cardinality
- c) Power set
- d) Equivalence relations, congruence modulo n

0.1. **Induction.** Show by induction on n that

$$1 + 4 + 9 + 16 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

The basis for the induction is: When $n = 1$ this statement is true.

Now suppose by induction that $n \geq 1$ and the statement holds for n . Then we need to show that it holds for $n + 1$. On the LHS we have:

$$\begin{aligned} 1 + 4 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + \frac{(n+1)(6n+6)}{6} \\ &= \frac{(n+1)[2n^2 + n + 6n + 6]}{6} \end{aligned}$$

On the RHS we have:

$$\begin{aligned} \frac{(n+1)(n+2)(2(n+1)+1)}{6} &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)[2n^2 + 7n + 6]}{6} \end{aligned}$$

So, $LHS = RHS$ and the equation holds for $n + 1$.

0.2. **Bijection (a).** Prove that a differentiable function $f : \mathbb{R} \rightarrow \mathbb{R}$ whose derivative is always positive is 1-1 but not necessarily onto.

I used this example to explain the basic properties of mappings. First of all a *function* or *mapping* has three parts: a set A called the *domain* of f , a set B called the *codomain* of f and the function f . We write:

$$f : A \rightarrow B$$

For every $a \in A$ we get one element $f(a) \in B$. In set theory, where everything is a set, the function f is identified with its graph

$$G(f) = \{(a, b) \in A \times B \mid b = f(a)\}$$

which is explained below.

Problem (a) has two parts. The first part is to prove that any differentiable function with positive derivative is 1-1. The second part is to find an example of a function with these properties which is not onto.

I reviewed the definitions. *Surjective* or *onto* means that $f(x)$ gives all values on the right hand side of the arrow $f : \mathbb{R} \rightarrow \mathbb{R}$. For example, $f(x) = x^2$ is not onto \mathbb{R} . The formal definition is:

Definition 0.1. $f : A \rightarrow B$ is surjective or onto if, for every $b \in B$ there exists an $a \in A$ so that $f(a) = b$.

Someone came up with the example

$$f(x) = e^x$$

This is not surjective since e^x is always positive.

Definition 0.2. A function $f : A \rightarrow B$ is defined to be 1-1 if it sends two elements to two elements ("2-2" would be a better way to say this). In other words, any two distinct elements $a, b \in A$, $a \neq b$ go to two distinct elements of B : $f(a) \neq f(b)$.

So, to prove f is 1-1 we take two distinct elements of the domain $x_1, x_2 \in \mathbb{R}$. One of them will be bigger than the other, say $x_2 > x_1$. Then by the fundamental theorem of calculus we have

$$f(x_2) = f(x_1) + \int_{x_1}^{x_2} f'(x) dx$$

Since $f'(x) > 0$ for all x , its integral is positive:

$$\int_{x_1}^{x_2} f'(x) dx > 0$$

Therefore, $f(x_2) > f(x_1)$. In particular $f(x_2) \neq f(x_1)$. So f is 1-1.

0.3. Bijection (b). If there is a mapping of sets $f : A \rightarrow B$ which is 1-1 but not onto then what can you say about the cardinality of the sets A, B ?

If f is not onto then B has at least one more element than A . This means that

$$|A| < |B| \text{ if } A \text{ is a finite set.}$$

The correct answer in general is:

$$|A| \leq |B|$$

Here $|A|$ denotes the *cardinality* of the set A . This is the number of elements of A . However, it can be various degrees of infinity. Cardinality will not play a large role in this course. So, I don't want to prove theorems about cardinality. I just want to discuss the concept and history.

If A, B are infinite sets then it could happen that they have the same number of elements and there might be a 1-1 mapping which is not onto. In fact, this is the definition of an infinite set.

Definition 0.3. *A set A is infinite if there exists a mapping $f : A \rightarrow A$ which is 1-1 but not onto.*

For example, the infinite set $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ has a 1-1 mapping $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ which is not onto given by $f(n) = 2n$.

0.4. **Bijection (c).** *Find a function $\mathbb{Z} \rightarrow \mathbb{Z}$ which is surjective but not 1-1.*

The first answer we got which I simplified here was:

$$f(n) = \begin{cases} n & \text{if } n < 2 \\ n - 1 & \text{if } n \geq 2 \end{cases}$$

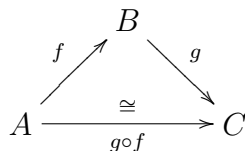
Since $f(1) = 1$ and $f(2) = 1$, this function is not 1-1. Then I asked for a formula with only one equation which would be easier to type and someone gave the example:

$$f(n) = \left\lceil \frac{n}{2} \right\rceil$$

where $\lceil - \rceil$ means *round up* to the nearest integer.

0.5. **Bijection (d).** *Suppose that $f : A \rightarrow B$ and $g : B \rightarrow C$ are mappings of sets so that $g \circ f : A \rightarrow C$ is a bijection. Then what can you say about f and g ?*

The answer is: f is an injection and g is a surjection. I asked for a proof that g is surjective. Here is a diagram which may be helpful.



Then we went through the proof that g is onto. First, recall the definition: g onto means that for every $c \in C$ there is a $b \in B$ so that $g(b) = c$. This is what we want to prove. We know that $g \circ f : A \rightarrow C$ is a bijection. Then implies that for every $c \in C$ there is a $a \in A$ so

that $(g \circ f)(a) = c$. But then $b = f(a)$ is an element of B which maps to c :

$$g(b) = (g \circ f)(a) = c.$$

So, g is surjective.

0.6. Axiom of Choice. The definition of g being *onto* suggests that we have a function from C to B . Call this s . Then for each $c \in C$ we have $b = s(c)$ so that $g(s(c)) = g(b) = c$. This means that $g \circ s : C \rightarrow C$ is the *identity mapping*: $g \circ s = id_C$. The existence of such a function s is called the *Axiom of Choice*.

$g : B \rightarrow C$ being surjective means that for each element $c \in C$ separately we can find $b = s(c)$. The Axiom of Choice says that we can do it all at once (make an infinite number of random choice at one time).

0.7. Power set. If A is any set, the *power set* $\mathcal{P}(A)$ is the set of all subsets of A . The cardinality of the power set is

$$|\mathcal{P}(A)| = 2^{|A|}$$

For example, if $A = \{a, b, c\}$ then $\mathcal{P}(A)$ has $2^3 = 8$ elements and they are:

$$\begin{aligned} & \{ \} \\ & \{a\}, \quad \{b\}, \quad \{c\} \\ & \{a, b\}, \quad \{a, c\}, \quad \{b, c\} \\ & \{a, b, c\} \end{aligned}$$

These sets can be written in a binary code as follows:

$$\begin{aligned} & 000 \\ & 100, \quad 010, \quad 001 \\ & 110, \quad 101, \quad 011 \\ & 111 \end{aligned}$$

The famous Cantor diagonalization argument shows the following theorem. You don't need to know the proof of this statement.

Theorem 0.4 (Cantor). *For any set A , the cardinality of $\mathcal{P}(A)$ is always strictly greater than the cardinality of A :*

$$|\mathcal{P}(A)| > |A|.$$

We checked that this is true in the case when $A = \{ \} = \emptyset$ is the empty set. Then $|A| = 0$, but $\mathcal{P}(A)$ has one element, namely, the empty set is a subset of the empty set:

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

and

$$|\mathcal{P}(A)| = 2^0 = 1$$

as the formula says.

0.8. Relations and Cartesian products. The *Cartesian product* $A \times B$ of two sets A, B is the set of all ordered pairs (a, b) where $a \in A, b \in B$. This is useful since the *graph* of a function $f : A \rightarrow B$ is a subset of the Cartesian product:

$$G(f) = \{(a, b) \in A \times B \mid b = f(a)\}$$

A *relation* \mathcal{R} on a set A is defined to be any subset of the Cartesian product $A \times A$. If $(a, b) \in \mathcal{R}$ then we write $a\mathcal{R}b$. For example, the relation $\mathcal{R} = (\leq)$ on \mathbb{R} is the set of all pairs of real numbers (x, y) so that $x \leq y$:

$$(\leq) = \{(x, y) \mid x, y \in \mathbb{R}, x \leq y\}$$

I put parentheses around the relation since $\mathcal{R} = \leq$ looks stupid.

If you shade in this set you note

- (1) The set includes the diagonal $\Delta = \{(x, x) \mid x \in \mathbb{R}\}$
- (2) The set is only above the diagonal and not below. So, it is not symmetric around the diagonal.

Definition 0.5. A relation \mathcal{R} on a set A is called

- (1) reflexive if $x\mathcal{R}x$ for all $x \in A$
- (2) symmetric if $x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- (3) transitive if $x\mathcal{R}y, y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

The relation \leq is reflexive and transitive but not symmetric.

Draw a picture of a symmetric relation on the set of real numbers.

Explain why the drawing fits the definition.

Here is a problem which combines these concepts.

Show that $2^n > n^2$ for all integers $n \geq 5$. Give an interpretation in terms of sets. Does this make sense when n is infinite?

The proof is in the homework 1 instructions. The interpretation is:

If A is a set having at least 5 elements then the power set of A has strictly greater cardinality than the Cartesian product $A \times A$.

0.9. Partitions and equivalence.

Definition 0.6. A partition of a set A is a covering of A by disjoint nonempty subsets:

$$A = \coprod A_i$$

This means two things:

- (1) The subsets A_i cover A in the sense that every element of A is in one of the subsets A_i . In symbols this is:

$$A = \bigcup A_i$$

In other words, A is the union of the sets A_i .

- (2) The subsets A_i are disjoint. They don't overlap. In symbols: $A_i \cap A_j = \emptyset$ if $i \neq j$.

The symbol \coprod means disjoint union.

Often sets are partitioned. For example, real numbers are often partitioned into positive, negative and zero:

$$\mathbb{R} = \mathbb{R}^+ \coprod \mathbb{R}^- \coprod \{0\}$$

Partitions have the property that every element of the set lies in exactly one "part" or "cell" and no cell is allowed to be empty.

One extremely important example that we will use is the partition of the set of integers according to their remainder after dividing by some number n . For example, if $n = 10$ then we can partition the set \mathbb{Z}^+ of positive integers into ten cells according to their last digit. All positive integers ending in 1 are in one cell, etc. So, the cells of this partition are:

$$\begin{aligned} A_1 &= \{1, 11, 21, 31, \dots\} \\ A_2 &= \{2, 12, 22, 32, \dots\} \\ A_3 &= \{3, 13, 23, 33, \dots\} \\ A_4 &= \{4, 14, 24, 34, \dots\} \\ &\vdots \\ A_0 &= \{10, 20, 30, 40, \dots\} \end{aligned}$$

The last set A_0 is the set of all positive multiples of 10:

$$A_0 = \{10n \mid n \in \mathbb{Z}^+\}$$

For $k > 0$ the formula is:

$$A_k = \{10m + k \mid k \in \mathbb{Z}^{\geq 0}\}$$

Given a partition of a set A , we have a relation on this set which is "being in the same cell" So, two elements of A are related if they are

“cell-mates.”

$$x \sim y \Leftrightarrow x \text{ and } y \text{ are in the same cell}$$

I gave the example of a prison since the words and pictures suggest this. If x is your cell-mate and y is a cell-mate of x then y is also your cell-mate because you are all in the same cell! So, being cell-mates is transitive. You can think about why it is reflexive and symmetric.

Another example is $x \sim y$ if x, y are positive integers which have the same last digit in base 10. The last digit is equal to the remainder when dividing by 10. We could take other bases and say $x \equiv_n y$ if x, y have the same remainder when divided by n . For example $x \equiv_2 y$ means that x, y have the same *parity* which means they are either both even or both odd.

0.10. Rhyme schemes and equivalence relations. Around 1950, H.W. Becker wrote a series of papers giving a classification of all possible rhyming schemes and counting the number of rhyming schemes of each kind. What does this have to do with partitions and equivalence relations?

I showed an example using the second stanza of John Keats “Ode to a nightingale”. This has 10 lines with last words and rhyming scheme given in the following chart.

Line	last word	rhyme scheme
1	been	a
2	earth,	b
3	green,	a
4	mirth!	b
5	South,	c
6	Hippocrene,	a
7	brim,	d
8	mouth;	c
9	unseen,	a
10	dim:	d

The rhyming scheme is *abab cad cad*. This gives a partition of the set of lines:

$$a = \{1, 3, 6, 9\}$$

$$b = \{2, 4\}$$

$$c = \{5, 8\}$$

$$d = \{7, 10\}$$

The set of lines (actually line numbers) is $A = \{1, 2, \dots, 10\}$. Lines 1,3,6,9 rhyme so we put those lines into one set. (But we use only the numbers of the lines.) We have a relation on the set A , namely,

$$j \sim k$$

if Line j rhymes with Line k . This is

- (1) reflexive: Each line rhymes with itself.
- (2) symmetric: E.g.: since Line 2 rhymes with Line 4, it is also true that Line 4 rhymes with Line 2.
- (3) transitive: E.g.: Line 1 rhymes with Line 3 and Line 3 rhymes with Line 9 and therefore Line 1 rhymes with Line 9.

Therefore, “rhyming” is an equivalence relation.

Definition 0.7. *An equivalence relation of a set A is any relation which is reflexive, symmetric and transitive.*

What does this mean geometrically on the graph? Here is an example giving a typical graph:

$$\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \lfloor x \rfloor = \lfloor y \rfloor\}$$

where $\lfloor x \rfloor$ is the greatest integer $\leq x$, i.e., it is the integer part of x . The equivalence relation \mathcal{R} is “having the same integer part”

Theorem 0.8. *A partition of a set gives an equivalence relation of being cell-mates and an equivalence relation on a set A gives a partition of the set into equivalence classes:*

$$[a] = \{x \in A \mid x\mathcal{R}a\}$$

The proof is on page 8 of the book. We will discuss the theory of equivalence relations again when we get to factor groups.

1. INTRODUCTION AND EXAMPLES

Before giving the abstract definition of a group, we begin with examples. The three main examples in this section of the book are

- (1) \mathbb{Z}_n integers modulo n .
- (2) \mathbb{R}_a real numbers modulo a
- (3) The set U of unit complex numbers.

1.1. Integers modulo n .

Definition 1.1. *If n is a positive integer then \mathbb{Z}_n is the set of nonnegative integers less than n :*

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

This is a finite set with exactly n elements. n is called the modulus.

For example,

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

has 4 elements.

Addition modulo n is defined like this:

$$a +_n b := c \quad \text{if } c \text{ is the remainder of } a + b \text{ after dividing by } n$$

Since $0 \leq a + b \leq 2n - 2$, this can also be written as follows:

$$a +_n b = \begin{cases} a + b & \text{if } a + b < n \\ a + b - n & \text{otherwise} \end{cases}$$

The addition table forms a pattern which is very similar for every n .

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Problems:

- (1) Find $x \in \mathbb{Z}_4$ so that $x +_4 2 = 1$.
- (2) Find all $x \in \mathbb{Z}_4$ so that $x +_4 x = 2$.

1.2. Real numbers modulo a .

Definition 1.2. If a is a positive real number then \mathbb{R}_a is defined to be the half open interval:

$$\mathbb{R}_a = [0, a)$$

The most common moduli to take are $a = 1$ and $a = 2\pi$ since angles are real numbers modulo 2π . Addition modulo a real number a can be defined as follows:

$$x +_a y := \begin{cases} x + y & \text{if } x + y < a \\ x + y - a & \text{otherwise} \end{cases}$$

This formula always gives an element of the set $\mathbb{R}_a = [0, a)$.

If $a = 1$ then $x +_1 y$ is the *fractional part* of $x + y$ (but it might not be a fraction).

Problems:

- (1) Find all numbers $x \in \mathbb{R}_{2/3}$ so that $x +_{2/3} x = 0$.
- (2) What about $x +_{2/3} x = 1$?

1.3. complex numbers. Complex numbers are defined to be expressions of the form

$$z = a + bi$$

where $a, b \in \mathbb{R}$ and i is one of the square roots of -1 . Complex numbers are usually denoted by the letter z . Addition and multiplication are defined by

$$\begin{aligned} (a + bi) + (x + yi) &= (a + x) + (b + y)i \\ (a + bi)(x + yi) &= (ax - by) + (ay + bx)i \end{aligned}$$

For example:

$$(2 + 3i)(3 + 2i) = (6 - 6) + (4 + 9)i = 13i$$

There is another way to write complex numbers:

$$z = x + yi = re^{i\theta}$$

where these letters are related by

$$x = r \cos \theta, \quad y = r \sin \theta$$

and

$$r = |z| = \sqrt{x^2 + y^2}$$

It is not quite true that $\theta = \tan^{-1} y/x$ since this formula never gives you the angles in the second and third quadrant.

$r \geq 0$ is called the *absolute value* of z

$\theta \in \mathbb{R}_{2\pi}$ is called the *argument* of z .

This polar notation is useful for taking powers of complex numbers. For example, take

$$(1 + i)^{10}$$

The number $z = 1 + i$ has absolute value

$$r = \sqrt{1 + 1} = \sqrt{2}$$

and argument

$$\theta = \tan^{-1} 1 = \frac{\pi}{4}$$

So,

$$1 + i = \sqrt{2}e^{\pi i/4}$$

$$(1 + i)^{10} = (2^{1/2})^{10}e^{10\pi i/4} = 2^5e^{5\pi i} = 32e^{\pi i} = -32$$

Problem: Find all complex numbers z so that $z^3 = 1$.

Definition 1.3.

$$U_n := \{z \in \mathbb{C} \mid z^n = 1\}$$

These numbers (complex solutions of $z^n = 1$) are called the n th roots of unity.

For example, $U_4 = \{1, i, -1, -i\}$.

The n th roots of unity are given by $e^{2\pi k/n}$ where $k = 0, 1, 2, \dots, n-1$ (in other words, $k \in \mathbb{Z}_n$). For example, for $n = 8$, the arguments are the multiples of $\pi/4$. So, the 8th roots of unity are:

$$e^{\frac{\pi i}{4}}, e^{\frac{\pi i}{2}}, e^{\frac{3\pi i}{4}}, e^{\pi i}, e^{\frac{5\pi i}{4}}, e^{\frac{3\pi i}{2}}, e^{\frac{7\pi i}{4}}, e^{2\pi i}$$

1.4. **unit circle.** The **unit circle** is given by

$$U = \{z \in \mathbb{C} \mid |z| = 1\}$$

Since $r = |z| = 1$, we have $z = e^{i\theta}$. The key point is:

Multiplication of unit complex numbers is given by addition of the arguments (angles) modulo 2π :

$$e^{\alpha i} e^{\beta i} = e^{(\alpha+\beta)i}$$

This simple concept can be written in the following fancy way:

Theorem 1.4. *There is a bijection $\phi : \mathbb{R}_{2\pi} \rightarrow U$ given by $\phi(\theta) = e^{i\theta}$. Furthermore,*

$$\phi(\alpha + \beta) = \phi(\alpha)\phi(\beta)$$

This is what we call an *isomorphism* of algebraic structures. It means we have a bijection of two sets which makes a binary operation of one set correspond to a binary operation on the other set.

Theorem 1.5. *There is a bijection $\phi_n : \mathbb{Z}_n \rightarrow U_n$ given by $\phi_n(k) = e^{2\pi k/n}$. Furthermore,*

$$\phi_n(j+k) = \phi_n(j)\phi_n(k)$$

Example 1.6. *For $n = 4$ this bijection gives the correspondence:*

$$\begin{array}{ccc} \mathbb{Z}_4 & \cong & U_4 \\ \hline 0 & \leftrightarrow & 1 \\ 1 & \leftrightarrow & i \\ 2 & \leftrightarrow & -1 \\ 3 & \leftrightarrow & -i \end{array}$$

In particular, $2 \in \mathbb{Z}_4$ correspond to $-1 \in U_4$. So the solutions of the equation

$$x +_4 x = 2$$

in \mathbb{Z}_4 correspond to the solutions of the equation $z^2 = -1$ which are $i, -i$ corresponding to $1, 3 \in \mathbb{Z}_4$.

2. BINARY OPERATIONS

A **binary operation** on a set S is defined to be a mapping

$$S \times S \rightarrow S$$

The notation is $(a, b) \mapsto a * b$. In words: for every ordered pair of not necessarily distinct elements (a, b) in the set S the binary operation assigns a unique element $a * b \in S$. The key point is that a, b are elements of the same set S and $a * b$ is another element of the same set S . No exceptions are allowed.

For example, the binary operation x/y is not defined for $y = 0$. But it is defined for all positive real numbers x, y and the result $x/y = x \div y$ is also positive real. So, in this case the set could be $S = \mathbb{R}^+$, $* = (\div)$.

The pair $(S, *)$ is called a **binary structure**. In the example (\mathbb{R}^+, \div) is a binary structure. The idea is to study the common properties of all operations. If we say we have a “binary operation” then we are talking simultaneously about addition, multiplication, subtraction, division, raising to powers, etc. This is very general and universally applicable.

The operation $*$ gives a *structure* on S . A set S by itself is homogeneous. All elements are equally important. There is no way to distinguish between them. Once there is a structure, some elements become much more important than others. For example, take (\mathbb{Z}, \times) , the set of integers under multiplication. The numbers 0 and 1 become very important.

0 is the “annihilator” since it “kills” all the other elements:

$$0 \times n = n \times 0 = 0.$$

1 is called “unity” since

$$1 \times n = n \times 1 = n$$

It leaves everyone unaltered.

The numbers 0,1 are called *idempotents* since they are two of the solutions of the equation

$$x^2 = x$$

The word “idem-potent” means “self-power” i.e., its powers are itself. (Prove this: $x^n = x$ if x is idempotent.)

A subset $T \subseteq S$ is said to be *closed* under the operation $*$ if $t_1 * t_2 \in T$ for all $t_1, t_2 \in T$. If this is true then $(T, *)$ is another binary structure.

Example 2.1. Let $S = \mathbb{R}$ with operation $*$ representing subtraction:

$$a * b = a - b$$

Then the set of integers \mathbb{Z} is closed under this operation. So, $(\mathbb{Z}, -)$ is also a binary structure.

Theorem 2.2. *There is a bijection $\exp : \mathbb{R} \rightarrow \mathbb{R}^+$ which makes subtraction in \mathbb{R} correspond to division in \mathbb{R}^+ :*

$$\exp(x) = e^x$$

$$\exp(x - y) = \exp(x) \div \exp(y)$$

What is the inverse mapping

$$\mathbb{R}^+ \rightarrow \mathbb{R} \quad ?$$

Definition 2.3. *We say that a binary operation $*$ on a set S is*

- (1) **commutative** if $x * y = y * x$ for every $x, y \in S$
- (2) **associative** if $(x * y) * z = x * (y * z)$ for all $x, y, z \in S$.

Problems:

- (1) Let $S = \mathbb{R}$. Is the binary operation $x * y = x - y$ commutative? associative?
- (2) Let $S = \mathbb{Z}$. Is the binary operation $a * b = 2ab$ commutative? associative?
- (3) Let $S = \mathbb{R}$. Is the binary operation

$$x * y = x + y + xy$$

commutative? associative?

If the binary operation $*$ is not associative then, given three elements of the set

$$(x * y) * z \neq x * (y * z).$$

Given four elements x, y, z, w there are 5 ways to put the parentheses. Find them.

If a binary operation on S is associative but not commutative then there are two ways to “multiply” x, y (Usually we speak of the operation $*$ as “multiplication” or “product”. A commutative operation is often called a “addition” or “sum”.)

Given four elements $x, y, z, w \in S$ and a binary operation $*$ which is associative but not commutative, how many ways can you multiply x, y, z, w ?

Here is a very important example: Suppose that X is any set and S is the set of all mappings

$$f : X \rightarrow X$$

The binary operation \circ (composition of functions) is associative but not commutative. Give an example to show it is not commutative.

Prove that an operation $*$ on a set can have at most one annihilator.

3. ISOMORPHIC BINARY STRUCTURES

Two binary structures $(S, *)$ and $(T, *)$ are called **isomorphic** if there is a bijection $\phi : S \rightarrow T$ so that

$$\phi(a * b) = \phi(a) * \phi(b)$$

for all $a, b \in S$. This equation is called the *homomorphism property*. Mathematicians also say “ ϕ commutes with multiplication.” The notation is $(S, *) \cong (T, *)$.

The word “commutes” means $ab = ba$. In this case

$a =$ “ ϕ of” and

$b =$ “the product of”

So:

(ϕ of)(the product of) a and b is equal to

(the product of)(ϕ of) a and b

A bijection with the homomorphism property is called an *isomorphism*.

Example 3.1. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. The isomorphism $\phi : \mathbb{R} \rightarrow \mathbb{R}^+$ is given by $\phi(x) = e^x$. The homomorphism property is verified by the properties of exponents:

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

People say: “ ϕ takes addition to multiplication.”

3.1. showing that two structures are isomorphic. To show that two binary structures are isomorphic:

$$(S, *) \cong (T, *)$$

we need to do four things:

- (1) Write down a mapping $\phi : S \rightarrow T$.
- (2) Show that ϕ is one-to-one.
- (3) Show that ϕ is onto.
- (4) Show that ϕ has the homomorphism property:

$$\phi(x * y) = \phi(x) * \phi(y)$$

for all $x, y \in S$.

The last step has a conceptual interpretation. Once we have a bijection $\phi : S \rightarrow T$, the binary operation on S will correspond to some binary operation on T , namely, given two elements of T , you take the corresponding elements of S , multiply in S , giving a product in S , and take the corresponding element of T .

Example 3.2. Suppose that an isomorphism $\phi : (\mathbb{R}, +) \rightarrow (\mathbb{R}, *)$ is given by

$$\phi(x) = 2x + 6$$

then what is the binary operation $*$?

3.2. structural properties. To show that two binary structures are not isomorphic, we look at the *structural properties*. These are the properties shared by all isomorphic structures. For example, the cardinality of the set is a structural property. Commutativity and associativity are structural properties. Having an identity¹ is a structural property. The identity, if it exists is called e or e_S .

Example 3.3. Take the binary structure (S, \cdot_8) where $S = \{1, 3, 5, 7\}$ and \cdot_8 is multiplication modulo 8

\cdot_8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

This set has the following structural properties:

- (1) $|S| = 4$
- (2) S has an identity $e = 1$
- (3) The operation is commutative
- (4) $x * x = e$ for all $x \in S$.

The last structural property shows: *This binary structure is not isomorphic to $(\mathbb{Z}_4, +_4)$* since 0 is the identity for $+_4$ in \mathbb{Z}_4 and $1 +_4 1 = 2 \neq 0$.

3.3. finding isomorphisms. If you have binary structures with the same structural properties then you should suspect that they are isomorphic. To find an isomorphism, you need to match the structures.

Example 3.4. Find an isomorphism $\phi : (\mathbb{R}, \cdot) \cong (\mathbb{R}, *)$ where $*$ is defined by

$$x * y = xy + x + y$$

(\mathbb{R}, \cdot) has identity 1 and annihilator 0. $(\mathbb{R}, *)$ has identity 0 and annihilator -1 . So, ϕ if it exists must send 0 to -1 and 1 to 0.

¹This is what I called “unity” last week. The identity is also called a “neutral element” and my word “unity” refers to a multiplicative identity.

4. GROUPS

4.1. definition of group. A **semigroup** is a set with an associative binary operation. The way you say/write it is: $(S, *)$ is a semigroup. Or: S is a semigroup under the operation $*$. For example: The set of even integers is a semigroup under multiplication.

A **monoid** is a semigroup with an identity e . (Recall that the identity element e is unique if it exists.) For example, $(\mathbb{Z}^+, +)$ is a semigroup but not a monoid since the identity 0 is not in the set. On the other hand, \mathbb{Z}^+ is a monoid under multiplication since the multiplicative identity 1 is in the set \mathbb{Z}^+ . Note the two different wordings.

To get a group we need one more concept: the inverse.

Definition 4.1. Suppose that $(M, *)$ is a monoid with identity e . Then an **inverse** of an element $a \in M$ is defined to be an element $b \in M$ so that

$$a * b = b * a = e \quad (\text{the identity}).$$

Just like the identity, a can have at most one inverse.

Theorem 4.2. Suppose that $(M, *)$ is a monoid and $a \in M$. Then the inverse of a is unique if it exists.

Proof. Suppose that a has two inverses b, c . Then we will show that $b = c$.

Given that b is an inverse of a we get $b * a = e$. So:

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

Given that c is an inverse of a we get $a * c = e$. So:

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

By associativity of $*$, these are equal. So, $c = b$. □

Because the inverse is unique, we can write $b = a^{-1}$ if it exists.

Definition 4.3. A **group** is a pair $(G, *)$ where $*$ is a binary operation on G satisfying the following conditions.

G1. $*$ is **associative**. In other words, $(G, *)$ is a semigroup. I.e.,

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

for all $a, b, c \in G$.

G2. G contains an **identity** e . In other words, $(G, *)$ is a monoid.

$$e * x = x = x * e$$

for all $x \in G$.

G3. Every element of $a \in G$ has an inverse $b \in G$. I.e.,

$$(\forall a \in G)(\exists b \in G) a * b = e = b * a$$

We also say G is a group under $*$.

4.2. **examples.** Groups under addition. The following are groups.

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +)$$

The following sets are groups under multiplication:

$$\mathbb{Q}^+, \quad \mathbb{R}^+, \quad \mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$$

$GL(n, \mathbb{R})$ is the set of all $n \times n$ invertible matrices with real entries. This set forms a group under matrix multiplication.

G1 Matrix multiplication is associative. I won't prove that.

G2 I_n is the identity: $I_n A = A = A I_n$.

G3 We have inverses since we took only the invertible matrices!

There is one more property we need to show: **closure**: $a * b$ lies in the set. We need to verify that the product of two invertible matrices is invertible.

$$\begin{aligned} AB(B^{-1}A^{-1}) &= AI_nA^{-1} = AA^{-1} = I_n \\ \Rightarrow B^{-1}A^{-1} &= (AB)^{-1} \end{aligned}$$

Notation: I will switch to the standard notation ab instead of $a * b$.

4.3. **cancellation.** One of the main properties of groups is called the *cancellation property*.

Theorem 4.4. Suppose that G is a group and $a, b \in G$ are any two elements. Then there is a unique solution $x \in G$ to the equation

$$ax = b$$

In particular this means that

$$ax = ay \quad \Rightarrow \quad x = y$$

This is the *left cancellation rule*. What is the statement and proof of the right cancellation rule?

Proof. The solution of the equation $ax = b$ is $x = a^{-1}b$.

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

To see that this is the only solution, suppose that $ay = ax = b$. Then, multiplying both by a^{-1} on the left we get:

$$a^{-1}ay = a^{-1}ax$$

The LHS is $ey = y$ and the RHS is $ex = x$. So, $x = y$. □

5. SUBGROUPS

A *subgroup* is a subset H of a group G which is closed under the operation (the one that makes G into a group) and which satisfies the definition of a group. Since associativity is automatic, the definition can be stated as follows.

5.1. definition and examples.

Definition 5.1. A **subgroup** of a group G is defined to be a subset H with the following properties.

- (1) H is closed under multiplication in the group.
- (2) H contains the identity e
- (3) H contains the inverse h^{-1} of any element $h \in H$.

We write $H \leq G$. ($H < G$ means H is a proper subgroup of G , in other words, H is not the whole group.)

The first condition is usually written:

$$HH \subseteq H$$

The notation means:

$$HH := \{h_1h_2 \mid h_1, h_2 \in H\}$$

In general AB means the set of all products ab where $a \in A$ and $b \in B$.

The third condition is written:

$$H^{-1} \subseteq H$$

Other examples of this set notation are:

$$aB = \{ab \mid b \in B\}$$

$$a + B = \{a + b \mid b \in B\}$$

Examples of subgroups are:

- (1) $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.
- (2) U_n is a subgroup of (U, \cdot) .
- (3) $SL(n, \mathbb{Z}) < GL(n, \mathbb{Z})$ where $SL(n, \mathbb{Z})$ is the group of $n \times n$ integer matrices with determinant 1.

Theorem 5.2. A subset H of a group G is a subgroup if and only if it is nonempty and satisfies

$$H^{-1}H \subseteq H.$$

The notation means:

$$H^{-1}H = \{h_1^{-1}h_2 \mid h_1, h_2 \in H\}.$$

Proof. We want to show that H is closed under multiplication, has the identity e and is also closed under inverse. Associativity is automatic since $H \subseteq G$.

- (1) ($e \in H$) Since H is nonempty, it has some element h . Then $h^{-1}h = e \in H^{-1}H \subseteq H$.
- (2) (H is closed under inverse.) Since $e \in H$, $H^{-1} = H^{-1}e \subseteq H^{-1}H \subseteq H$. Also, $H \subseteq H^{-1}$ since each $h \in H$ is equal to $(h^{-1})^{-1} \in H^{-1}$. Thus $H = H^{-1}$.
- (3) (H is closed.) $HH = H^{-1}H \subseteq H$.

Thus, H is a subgroup of G . □

5.2. cyclic subgroup. If a is an element of a group G then the set of all powers of a forms a subgroup denoted $\langle a \rangle$ and called the *cyclic subgroup generated by a* :

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$$

Why is this a subgroup?

Take the group U of complex numbers with absolute value 1. What is $\langle i \rangle$? What happened to the negative powers of i ?

If we can find an element of the group $a \in G$ so that $G = \langle a \rangle$ then G is called a **cyclic group** with generator a . For example \mathbb{Z}_n is a cyclic group (under addition) with generator 1. Can you find another generator?

The Klein four group is often denoted V (for **v**ier). I would call it the 2-bit addition group:

$$V = \{00, 01, 10, 11\}$$

with addition given on each coordinate without carrying. The elements form a square.

Find all cyclic subgroups of V . Conclude that V is not a cyclic group.

If we add a parity bit (the sum of the digits) V becomes isomorphic to a subgroup of the 3-bit addition group:

$$H = \{000, 011, 101, 110\} < \{a_1a_2a_3 \mid a_i = 0 \text{ or } 1\}$$

If we draw a picture we would see that H forms a tetrahedron inside a cube. This demonstrates the three fold symmetry of the Klein 4-group V . (In general the n -bit addition group has $n + 1$ fold symmetry.)

6. CYCLIC GROUPS

Definition 6.1. A cyclic group is a group G which is equal to $\langle g \rangle$ for some $g \in G$. Thus

$$G = \langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

We say that g generates G

Examples:

- (1) $(\mathbb{Z}, +)$ is a cyclic group generated by $g = 1$.
- (2) (U_n, \cdot) is a cyclic group generated by $\zeta = e^{2\pi i/n}$.
- (3) For any element g of any group G , $\langle g \rangle$ is a cyclic group generated by g .

Problem: Show that any cyclic group is abelian (commutative).

6.1. division and order. We use the word *order* for the cardinality of a group. For example \mathbb{Z}_5 is a group of order 5. \mathbb{Z} is an additive group of infinite order.

Definition 6.2. The **order** of an element g of any group is defined to be the order of the cyclic group that it generates:

$$o(g) := |\langle g \rangle|$$

For example, in \mathbb{Z}_6 the order of the 6 elements and the cyclic subgroup that they generate are:

g	$o(g)$	$\langle g \rangle$
0	1	$\{0\}$
1	6	$\{0, 1, 2, 3, 4, 5\}$
2	3	$\{0, 2, 4\}$
3	2	$\{0, 3\}$
4	3	$\{0, 4, 2\}$
5	6	$\{0, 5, 4, 3, 2, 1\}$

The properties of the order of an element are related to the *division algorithm* also called the *Euclidean algorithm* since it was first written down by Euclid.

Theorem 6.3 (division algorithm). *If n is a positive integer and k is any integer, there exist unique integers q and r so that*

$$k = qn + r$$

and $0 \leq r < n$. q is called the quotient and r is called the remainder of k when divided by n .

Euclid did not know about negative numbers. He assumed that k was positive and his algorithm was just to keep subtracting n from k until you can't. Then you are left with r and the number of times you subtracted was q .

You can read the proof in the book. Here I will explain what this has to do with $o(g)$, the order of $g \in G$.

Theorem 6.4. *Suppose that G is a group and $g \in G$ is an element of finite order $o(g) = |\langle g \rangle| < \infty$. Then*

(1) *the subgroup $\langle g \rangle \leq G$ is equal to the set*

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

for some positive n and there is no repetition in this list of elements.

(2) $o(g) = n$.

(3) $g^n = e$

Proof. By definition, $\langle g \rangle$ consists of all powers g^k of g . Since this is assumed to be a finite set, the elements

$$g, g^2, g^3, g^4, \dots$$

cannot all be different. So, two of them are equal, say $g^i = g^j$ where $j > i$. This equation can be written as:

$$g^i g^{j-i} = g^j = g^i = g^i e$$

By cancellation this gives:

$$(6.1) \quad g^{j-i} = e$$

Let $n = j - i$. Then $g^n = e$ and $n > 0$. This shows that condition (3) holds for some positive integer n . Let n be the smallest positive integer satisfying equation (3).

If g^k is any element of $\langle g \rangle$ then the division algorithm gives

$$k = nq + r$$

where q, r are integers and $0 \leq r < n$. So,

$$g^k = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = e^q g^r = g^r.$$

So, $e, g, g^2, \dots, g^{n-1}$ are all the elements of $\langle g \rangle$.

To see that there are no repetitions suppose that $0 \leq i < j \leq n - 1$ and $g^i = g^j$. Then, we have equation (6.1)

$$g^{j-i} = e$$

But $j - i < n$ which is a contradiction to the minimality of n . Therefore, there are no repetitions in the list. \square

Corollary 6.5. *If $g \in G$ has finite order n then $\langle g \rangle$ is isomorphic to \mathbb{Z}_n .*

Proof. The isomorphism $\phi : \mathbb{Z}_n \rightarrow \langle g \rangle$ is given by $\phi(k) = g^k$. The first part (1) in the theorem above tells us that this mapping is a bijection. The third equation tells us that this satisfies the isomorphism property since, if $x + y \geq n$ then $x +_n y = x + y - n$ and

$$\phi(x+_n y) = \phi(x+y-n) = g^{x+y-n} = g^x g^y g^{-n} = \phi(x)\phi(y)e^{-1} = \phi(x)\phi(y)$$

And if $x + y < n$ then $x +_n y = x + y$ and it is clear that $\phi(x +_n y) = \phi(x)\phi(y)$. \square

Problem: Show that $g^k = e$ if and only if k is a multiple of the order of g .

Example: Let $G = GL(2, \mathbb{Z})$ and

$$g = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Then

$$g^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad g^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = e$$

Then $o(g) = 3$ and $g^{3k} = I_2, g^{3k+1} = g, g^{3k+2} = g^2$ are the three elements of $\langle g \rangle$.

6.2. subgroups of cyclic groups. The main theorem about cyclic groups is the following.

Theorem 6.6. *Every subgroup of a cyclic group is cyclic.*

Proof. We are given that $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. If $H \leq G$, let k be the smallest positive integer so that $g^k \in H$. Then $H = \langle g^k \rangle$. If there is no such k then $H = \{e\}$ which is also cyclic. \square

This theorem has a very nice application.

Corollary 6.7. *The greatest common divisor d of two positive integers r and s can be written as*

$$d = nr + ms$$

where $n, m \in \mathbb{Z}$.

Proof. Let $G = \mathbb{Z}$ and

$$H = \{nr + mx \mid n, m \in \mathbb{Z}\}$$

Then H is a subgroup of \mathbb{Z} . The theorem implies $H = \langle d \rangle$ for some integer d . So, $H = d\mathbb{Z}$. Since $d \in H$ it has the form $d = nr + ms$. So, we just need to show the following.

Claim: d is the greatest common divisor (gcd) of r and s .

Pf: Since $r = 1r + 0s \in H$, r is a multiple of d . Similarly, s is a multiple of d . So, d is a common divisor of r and s . Suppose that d is not the gcd. Then there is another common divisor D . Then D divides both r and s so it divides $nr + ms = d$. So, $D \leq d$. Therefore d is the greatest common divisor. \square

Euclid's algorithm for finding $d = \gcd(r, s)$ was to take the two positive integers r, s and subtract the smaller from the larger, and repeat this until the two numbers are equal. Then the result is d, d .

Homework 4

page 56 numbers 21, 22, 23, 26, 31, 32, 41, 54. (Do all these problems for next Thursday, Sept 24. I will give you a practice quiz on that day.)

Problems from section 6 will be in the HW5/review problems. HW5 will consist of a number of review problems which I will give you answers to most of them. A small number of these will be left for you to do. Remember: Quiz one will be on Wednesday, Oct 7, in class.

7. GENERATING SETS AND CAYLEY DIGRAPHS

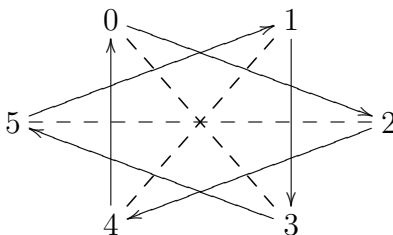
In a cyclic group G all elements are powers of a single element g which is called a *generator* of the group. Other groups such as the Klein four group V are not cyclic and require more than one generator.

Definition 7.1. *A set of elements of G is called a generating set and the elements are called **generators** if every element of G is a product of the generators and inverses of generators possibly with many repetitions. For example the elements of G look like: $b^5a^{-1}b^2a^{-9}b$ if a, b are the generators. The generators are said to “generate” the group. The product of no elements is by definition equal to the identity e .*

Examples:

- (1) The Klein four group $V = \{e, a, b, c\}$ has generating set $\{a, b\}$. Also b, c generate V and a, c are generators of V .
- (2) The set of all elements of a group G is a generating set.
- (3) $2, 3$ generate \mathbb{Z}_6 but neither element by itself is a generator. Whether or not “ g is a generator of G ” depends on what the other elements in the set are.

Given a generating set we can draw a directed graph called the *Cayley digraph* with one vertex for each element of the group and one arrow for each generators starting at each vertex. So, for example $G = \mathbb{Z}_6$ with generator 1 is a hexagon. With generating set $\{2, 3\}$ it would look like this:



The solid arrows indicate addition by 2 and the dotted lines are addition by 3. Since 3 is its own inverse there is no arrow direction on those dotted line. For example $2 +_6 3 = 5$ and $5 +_6 3 = 2$. So adding 3 modulo 6 will send 2 and 5 to each other, whereas adding 2 sends $0 \rightarrow 2 \rightarrow 4 \rightarrow 0$ and $1 \rightarrow 3 \rightarrow 5 \rightarrow 1$.

The Cayley digraph is always connected. Why?

Question: In what way is the square the Cayley digraph for the Klein four group?

Question: Do 12 and 14 generate \mathbb{Z} ? (The operation is addition.)

7.1. more about Cayley digraphs. The Cayley digraph is a directed graph with labels on the vertices and edges. A sequence of edges gives a **path** if the head (or target) of each edge is the tail (or source) of the next. The labels on the edges are composed *left to right*. Thus abc means a then b then c :

$$abc : \bullet \xrightarrow{a} \bullet \xrightarrow{b} \bullet \xrightarrow{c} \bullet$$

The labels on the vertices are group elements which change by multiplication on the right:

$$g \xrightarrow{a} ga \xrightarrow{b} gab \xrightarrow{c} gabc$$

8. PERMUTATION GROUPS

A *permutation* of a sequence of symbols is a rearrangement of the order of the symbols. The things being permuted are called “letters” even though they are usually numbers. For example 3241 is a permutation of the “letters” 1234. The symbols need to be different. Permutations can be described algebraically in two different ways.

- (1) As a movement of the letters. (In 3241, 1 moves to position 4.)
- (2) As a transformation of the letters. (In 3241, 1 changes into 3.)

Our book takes the second interpretation. Thus the permutation given by 3241 is the function which transforms 1 into 3, 2 to 2, 3 to 4 and 4 to 1:

$$\sigma(1) = 3, \quad \sigma(2) = 2, \quad \sigma(3) = 4, \quad \sigma(4) = 1$$

In other words, σ is a bijection of the set $\{1, 2, 3, 4\}$ to itself. One notation for this is the following.

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

or in general:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Since permutations are functions, you can compose them. For example if τ is the permutation

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

then $\tau\sigma$ means do σ then do τ . Permutations are composed *right to left*. If you remember that we are using the “transformation” interpretation (instead of the “movement” interpretation) then the composition is easy to calculate. In the example, σ gives 3241. Then τ will transform 2 into 3 and 3 into two changing the first two symbols into 23. So $\tau\sigma = 2341$ or:

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

The formula would be:

$$\begin{aligned} \tau\sigma(1) &= \tau(3) = 2, & \tau\sigma(2) &= \tau(2) = 3 \\ \tau\sigma(3) &= \tau(4) = 4, & \tau\sigma(4) &= \tau(1) = 1. \end{aligned}$$

A permutations of $A = \{1, 2, 3, 4\}$ is therefore a bijection $\sigma : A \rightarrow A$ and the set of all permutation of A forms a group under composition. (To be continued.)

8.1. symmetric group.

Definition 8.1. If A is any set then the **permutation group** of A , denoted S_A , is the group of bijections $\sigma : A \rightarrow A$ under composition. Subgroups of S_A are also called permutation groups (or groups of permutations to avoid confusion).

This is both a definition and a theorem. It states that the set of all bijections $A \rightarrow A$ forms a group under composition. Why is that?

A special case:

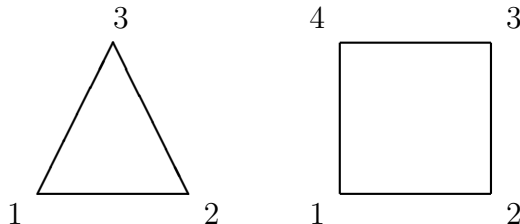
Definition 8.2. The permutation group of the set $A = \{1, 2, \dots, n\}$ is called the **symmetric group** on n letters and is denoted S_n .

Problem: Show that S_n has order $n!$.

For example: $|S_3| = 3! = 6$.

8.2. dihedral groups.

Definition 8.3. The **dihedral group** D_n is the group of symmetries of the regular n -gon. These include n rotations and n reflections. So $|D_n| = 2n$.



If we represent these geometric symmetries as permutations then we see that D_n is isomorphic to a group of permutations of n letters. Composition of geometric movements corresponds to the second interpretation of permutation (the one we are using!) For example,

$$s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

This is given by doing the movement corresponding to s followed by the movement corresponding to t .

8.3. Cayley's theorem.

Theorem 8.4 (Cayley). Every group is isomorphic to a group of permutations.

Proof. For any group G there is a mapping

$$\rho : G \rightarrow S_G$$

given by $\rho(g) =$ left multiplication by g :

$$\rho(g)(h) = gh$$

I make the following claims:

- (1) $\rho(g)$ is a permutation of G .
- (2) $H = \{\rho(g) \mid g \in G\}$ is a subgroup of S_G .
- (3) $\rho : G \rightarrow H$ is a bijection.
- (4) ρ satisfies the homomorphism property.

The first step is to understand that this list will complete the proof. (1) says that ρ is in fact a mapping from the set G to the set S_G . (2) says that $H = \rho(G)$ is a subgroup of S_G and therefore ρ gives a surjective mapping

$$\rho : G \rightarrow H$$

The next two conditions say that this mapping is an isomorphism of groups.

Next we verify this one step at a time.

(1) To show that $\rho(g)$ is a bijection, we just note that $\rho(g^{-1})$ is the inverse of $\rho(g)$:

$$\rho(g^{-1})\rho(g)(h) = g^{-1}gh = eh = h$$

and similarly, $\rho(g)\rho(g^{-1}) = id_G$. This proves (1).

(4) Now let us go to (4). The homomorphism property is:

$$\rho(g)\rho(h) = \rho(gh)$$

This is obvious once we know what it says:

$$\rho(g)\rho(h)(k) = g(hk) = (gh)k = \rho(gh)(k)$$

(2) To show that H is a subgroup we need to show three things and we have already done two of them! The last one (the one that we should have done first is to show that it contains the identity of S_G which is the identity mapping $\rho(e) = id_G$ since

$$\rho(e)(h) = eh = h.$$

We already know that $H = \rho(G)$ has inverses: $\rho(g)^{-1} = \rho(g^{-1}) \in H$ and is closed under composition since $\rho(g)\rho(h) = \rho(gh)$.

Finally, (3), ρ is a 1-1 by the cancellation property:

$$\rho(g) = \rho(h) \Rightarrow \rho(g)(x) = gx = hx = \rho(h)(x) \Rightarrow g = h$$

ρ is onto by definition (since H is the image of ρ). □

8.4. example of Cayley's theorem. The theorem is that every groups is isomorphic to a permutation group. The proof was that we have a monomorphism:

$$\rho : G \rightarrow S_G$$

called the regular representation which sends $g \in G$ to $\rho(g)$ which is multiplication on the left with g :

$$\rho(g)(h) = gh$$

Here is a simple example. Take $G = \mathbb{Z}_3 = \{0, 1, 2\}$. The binary operation is understood to be addition modulo 3. So, the regular representation is:

$$\rho(g)(h) = g +_3 h$$

So, $\rho(0)$ is the identity mapping, $\rho(1)$ adds 1:

$$\rho(1) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

and $\rho(2) = \rho(1)^2$ adds 2:

$$\rho(2) = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

Questions: Can you do the same for $G = V$ and $G = S_2$ using orbit notation (as explained in the next section)?

9. ORBITS, CYCLES AND A_n

First, I will do the example to explain the concepts. Then we will go over the rigorous definitions. A permutation of n letters $\sigma \in S_n$ has “orbits” and “cycles”. These are essentially the same thing except that orbits are sets and therefore *unordered* whereas cycles are “cyclically ordered”. Here is an example similar to the one in the book. $\sigma \in S_8$ is given by

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

This permutation has two cycles:

- (1) $1 \rightarrow 8 \rightarrow 3 \rightarrow 6 \rightarrow 1$. This is a 4-cycle and is written: (1836).
- (2) $2 \rightarrow 2$. This is a 1-cycle written: (2) and 1-cycles don't count!!
- (3) $4 \rightarrow 7 \rightarrow 5 \rightarrow 4$. This is the 3-cycle (475).

9.1. **orbits.** The orbits of σ are the three sets:

- (1) $\mathcal{O}_1 = \{1, 3, 6, 8\}$
- (2) $\mathcal{O}_2 = \{2\}$. This is a *singleton*.
- (3) $\mathcal{O}_3 = \{4, 5, 7\}$

The orbits are disjoint sets whose union is the set being permuted, namely the set $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$:

$$A = \mathcal{O}_1 \amalg \mathcal{O}_2 \amalg \mathcal{O}_3$$

This is a *partition* of the set A . The parts are called *cells* of the partition and they are given by an equivalence relation “lying in the same orbit”

Definition 9.1. If σ is a permutation of the set A and $a, b \in A$ are two elements, we say that a, b are in the same orbit if there exists an integer n so that $\sigma^n(a) = b$. This is an equivalence relation and the equivalence classes are called the **orbits** of σ . The orbit of any $a \in A$ is therefore the set:

$$\{\sigma^n(a) \mid n \in \mathbb{Z}\}$$

In the example, $\sigma(1) = 8, \sigma^2(1) = 3, \sigma^3(1) = 6, \sigma^4(1) = \sigma^0(1) = 1$. So the orbit of 1 is the set $\{1, 8, 3, 6\} = \{1, 3, 6, 8\}$. This is also the orbit of 3.

Problem: Show that the orbits of a permutation σ are either disjoint or equal.

9.2. **cycles.** Going back to the example, the first orbit $\{1, 3, 6, 8\}$ comes in the order 1836. We interpret this as a separate permutation where the other “letters” 2,4,5,7 are fixed:

$$(1836) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 4 & 5 & 1 & 7 & 3 \end{pmatrix}$$

Definition 9.2. A *cycle* is defined to be a permutation having at most one orbit which is not a singleton. The length of a cycle is the number of elements in the largest orbit.

The *support* of any permutation σ is defined to be the set of all letters x so that $\sigma(x) \neq x$. This is the set of letters *moved* by σ . The length of a cycle is the size of its support except if it is a 1-cycle.

Problem: How many 1-cycles does S_n have? How many 2-cycles does S_n have? How many 3-cycles does it have?

Definition 9.3. 2-cycles are called **transpositions**.

Problem: Show that disjoint cycles commute. (Why is it obvious that they commute?)

Here is an example that shows that cycles can commute even if they are not disjoint:

$$\sigma = (12345), \quad \tau = (13524)$$

What does it mean that these commute? Why do you think they commute?

Theorem 9.4. Every permutation of n letters can be written as a product² of disjoint cycles of length ≥ 2 . These disjoint cycles are uniquely determined. But the product can be written in any order.

Proof. Suppose that $\sigma \in S_n$. For each orbit \mathcal{O} of σ which is not a singleton, the permutation σ permutes the elements of \mathcal{O} in one cycle $\sigma_{\mathcal{O}}$:

$$\sigma_{\mathcal{O}}(x) = \begin{cases} \sigma(x) & \text{if } x \in \mathcal{O} \\ x & \text{otherwise} \end{cases}$$

Do this for every orbit of σ which is not a singleton. Then σ is a product of the cycles $\sigma_{\mathcal{O}_1}, \sigma_{\mathcal{O}_2}, \dots, \sigma_{\mathcal{O}_k}$ since, for any letter x lies in exactly on orbit, say \mathcal{O}_i and $y = \sigma(x)$ also lies in \mathcal{O}_i . Then $\sigma_{\mathcal{O}_j}(x) = x$ and $\sigma_{\mathcal{O}_i}(x) = y$. So, $\sigma_{\mathcal{O}_1}, \sigma_{\mathcal{O}_2}, \dots, \sigma_{\mathcal{O}_k}$ sends x to y .

To show uniqueness, suppose that σ is written as a product of disjoint cycles. Then the supports of these cycles must be the orbits of σ which are not singletons. Then the cycles must be $\sigma_{\mathcal{O}}$ as above. \square

²The product of no elements of a group is defined to be the identity e .

9.3. more about cycles. Problems: Write the following permutation of 8 as a product of disjoint cycles.

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

What is the order of an n -cycle? What is the order of σ ?

Lemma 9.5. *Every n -cycle can be written as a product of $n - 1$ transpositions³*

Proof. Here is the formula:

$$(a_1 a_2 a_3 \cdots a_n) = (a_1 a_2)(a_2 a_3)(a_3 a_4) \cdots (a_{n-1} a_n)$$

for example a 4-cycle can be written as a product of 3 transpositions:

$$(1357) = (13)(35)(57)$$

□

Since every permutation of n can be written as a product of disjoint cycles and every cycle is a product of transpositions, we get the following.

Theorem 9.6. *Every permutation of n can be written as a product of transpositions.*

How many transpositions do you need? Suppose that σ is a permutation of 100 with 4 orbits of size 10,20,30,40. Then, in the cycle decomposition, σ is a product of 4 cycles of size 10,20,30,40. These cycles can be written as a product of 9,19,29,39. So, σ can be written as a product of

$$9 + 19 + 29 + 39 = 96$$

transpositions. The formula is $100 - 4$ or $n - k$ where k is the number of orbits. What is k for the identity permutation?

9.4. sign of a permutation.

Definition 9.7. *The sign of a permutation σ of n letters is defined to be $(-1)^{n-k}$ where k is the number of orbits of σ . The permutation σ is defined to be odd if $n - k$ is odd (and the sign is -1) and σ is even if $n - k$ is even.*

Notice that σ can be written as a product of $n - k$ transpositions. So, an even permutation is a product of an even number of transpositions and an odd permutation is a product of an odd number of transpositions.

³Research problem: Show that there are exactly n^{n-2} different ways to write an n cycle as a product of $n - 1$ transpositions.

Theorem 9.8. *A permutation of n which is a product of m transpositions is even if m is even and odd if m is odd.*

Proof. Suppose that σ can be written as a product of m transpositions. Then we want to show that m has the same parity as $n - k$, i.e., that $n - k - m$ is always an even integer. We will prove this by induction on m .

Suppose that $m = 1$. Then σ is a 2-cycle. So it has one orbit of size 2 and the remaining $n - 2$ letters form the other orbits which are singletons. So, σ has $k = n - 1$ orbits and $n - k - m = n - (n - 1) - 1 = 0$ is even.

Now suppose the statement holds for m . Then we will prove it for $m + 1$. This means we assume that σ is a product of $m + 1$ transpositions:

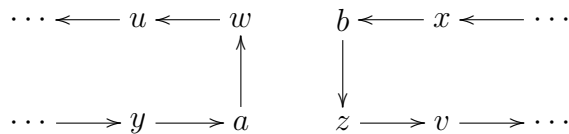
$$\sigma = \underbrace{\tau_1 \tau_2 \cdots \tau_m}_{\rho} \tau_{m+1} = \rho \tau_{m+1}$$

Since ρ is a product of m transpositions, we know by induction on m that $n - k - m$ is even where k is the number of orbits of ρ . To show that our statement holds for $m + 1$ it is enough to show that σ has either $k + 1$ or $k - 1$ orbits. Then

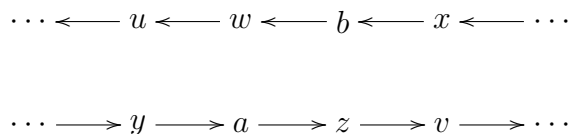
$$n - (\text{number of orbits of } \sigma) - (m + 1) = n - (k \pm 1) - (m - 1)$$

will be even.

The transposition τ_{m+1} is a 2-cycle, say $\tau_{m+1} = (ab)$. There are two cases: either a, b lie in different orbits of ρ or they lie in the same orbit of ρ . In the first case, the two orbits will “fuse” and become one orbit. So $\rho\tau_{m+1}$ will have $k - 1$ orbits. In the second case the orbit containing a, b will split into two orbits making $k + 1$ orbits for $\rho\tau_{m+1}$. Here is a diagram which illustrates both cases.



becomes:



□

9.5. the alternating group A_n .

Definition 9.9. *The alternating group on n letters, denoted A_n , is defined to be the subgroup of S_n consisting of all even permutations of n .*

To show that this is a subgroup:

- (1) A_n contains the identity since the identity has $k = n$ orbits.
- (2) A_n is closed under composition: If σ, τ are even then they can be written as a product of even numbers of transpositions, say $2s$ and $2t$. Multiplying them we get $\sigma\tau$ written as a product of $2s + 2t$ transpositions. So, it is even.
- (3) If σ is a product of $2s$ transpositions $\sigma = t_1 t_2 \cdots t_{2s}$ then the inverse is the product of the same $2s$ transpositions written backwards:

$$\sigma^{-1} = t_{2s} t_{2s-1} \cdots t_2 t_1$$

Why is that?

Problem: Show that the order of A_n is $n!/2$, i.e., A_n has exactly half the elements of S_n . Do the other elements of S_n form another subgroup?

Show that (for $n \geq 2$) S_n is the disjoint union of A_n and the set

$$(12)A_n = \{(12)\sigma \mid \sigma \in A_n\}$$

The alternating group A_4 contains a group isomorphic to the Klein 4-group V . It is

$$K = \{e, (12)(34), (13)(24), (14)(23)\}$$

Problem: show that any product of 3-cycles is even.

10. COSETS

In the symmetric group S_n , half the elements are odd and half are even. The even permutations form a subgroup A_n . The odd ones form a subset which is not a subgroup. It is called a *coset* of A_n . The important point is that a coset is a *subset* of a group.

Definition 10.1. *Suppose that H is a subgroup of a group G and $a \in G$. Then*

$$aH := \{ah \mid h \in H\}$$

*is called a **left coset** of H in G and*

$$Ha := \{ha \mid h \in H\}$$

*is called a **right coset** of H in G .*

If the group is additive then the cosets of H in G are

$$a + H = H + a = \{a + h \mid h \in H\}$$

10.1. examples. I will give you three examples for now. The first example will show that the same coset can be written in different ways. The second example will show that left cosets and right cosets can be different. The third example shows that infinite cosets also have conceptual meaning.

10.1.1. $G = \mathbb{Z}_4, H = \langle 2 \rangle$. This is an additive group. So, by definition, the cosets of H in G are given by adding⁴ elements of G to H . So, naively, there appear to be four cosets: $0 + H, 1 + H, 2 + H, 3 + H$. But, remember, these are just the *names* of the cosets. Since $H = \{0, 2\}$,

$$1 + H = \{1, 3\}$$

What are the other cosets?

10.1.2. $G = S_3, H = \langle (12) \rangle$. This example will show that the left cosets are not the same sets as the right cosets. There are three left cosets of $H = \{e, (12)\}$ in S_3 :

$$H = \{e, (12)\}, \quad (13)H = \{(13), (123)\}, \quad (23)H = \{(23), (132)\}$$

There are three right cosets:

$$H = \{e, (12)\}, \quad H(13) = \{(13), (132)\}, \quad H(23) = \{(23), (123)\}$$

⁴Note that the book and I are both writing $+$ instead of $+_4$ at this point. It is not as precise but it is standard notation.

So, left and right cosets are different. This picture might help.

$H :$	$e \quad (12)$	$H :$	$e \quad (12)$	$H(23)$				
$(13)H :$	$(13) \quad (123)$	$H(13) :$	<table style="border-collapse: collapse; width: 100%;"> <tr> <td style="border-right: 1px solid black; padding: 5px; text-align: center;">(13)</td> <td style="padding: 5px; text-align: center;">(123)</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px; text-align: center;">(132)</td> <td style="padding: 5px; text-align: center;">(23)</td> </tr> </table>	(13)	(123)	(132)	(23)	
(13)	(123)							
(132)	(23)							
$(23)H :$	$(132) \quad (23)$							

Can you explain why this happens? If we take the subgroup $A_3 = \{e, (123), (132)\}$, the left and right cosets are the same. What do you think is the difference?

10.1.3. $G = \mathbb{R}^2$, $H = \text{line}$. If G is the additive group \mathbb{R}^2 then a straight line through the origin is a subgroup. If you choose one nonzero vector v in the line then

$$H = \mathbb{R}v = \{rv \mid r \in \mathbb{R}\}$$

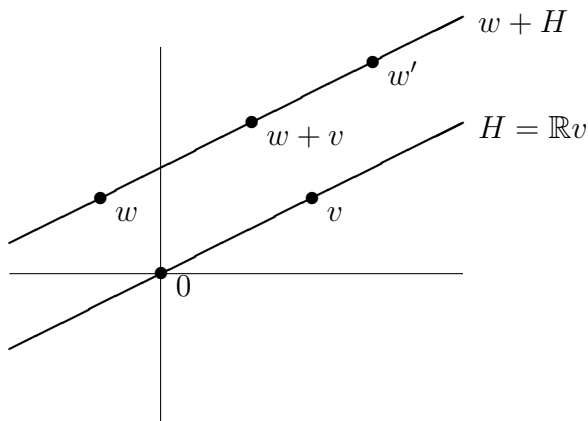
Show that this is an additive subgroup of \mathbb{R}^2 .

The cosets of the line are

$$w + H = w + \mathbb{R}v$$

This is the straight line parallel to H which passes through the point w . If w' any other point in the same line then you get the equation

$$w + H = w' + H.$$



The key point is that parallel lines do not meet unless they are the same line. (A line is parallel to itself.)

10.2. properties of cosets. The main property is that cosets of H do not meet unless they are equal. And two cosets may be equal even though they look different.

10.2.1. *different ways to write the same coset.*

Theorem 10.2. *Two left cosets aH, bH of H in G are equal if and only if $a^{-1}b \in H$. This is also equivalent to the statement $b \in aH$.*

Proof. ($aH = bH \Rightarrow a^{-1}b \in H$) Suppose that $aH = bH$. Then $b = be \in bH$. So, b will also be an element of aH . So, $b = ah$ for some $h \in H$. But, solving for h , we get $h = a^{-1}b \in H$.

($a^{-1}b \in H \Rightarrow aH = bH$) Conversely, if $a^{-1}b \in H$ then we want to show that $aH = bH$. To show this we have to show that each set is contained in the other. So, take any $bh \in bH$. Then

$$bh = a \underbrace{(a^{-1}b)h}_{\in H} \in aH$$

So, $bH \subseteq aH$. Now take any $ah \in aH$. Then $ah = b(a^{-1}b)^{-1}h \in bH$. So, $aH \subseteq bH$ and we conclude that $aH = bH$. \square

This theorem means the following. If C is a left coset of H in G then the possible ways to write C are:

$$C = cH$$

where c is any element of C . In example 10.1.2, The left coset $C = \{(12), (123)\}$ can be written as

$$C = (12)H \quad C = (123)H$$

You take one of the two elements of C and put them next to H on the left.

10.2.2. *different cosets are disjoint.*

Theorem 10.3. *If $aH \neq bH$ then aH, bH are disjoint.*

Proof. If $c \in aH \cap bH$ then $aH = cH = bH$. \square

Another way to say this: If two left cosets overlap then they are equal. Since every element of the group $g \in G$ is contained in the left coset gH , this theorem implies:

Corollary 10.4. *G is divided up (as in the figure in Example 10.1.2) into a disjoint union of left cosets.*

10.2.3. *cosets have the same cardinality.*

Theorem 10.5. *Every left coset aH of H is in 1-1 correspondence with H . In particular, all left cosets have the same number of elements.*

Proof. The correspondence is that $h \in H$ corresponds to $ah \in aH$ and $x \in aH$ corresponds to $a^{-1}x \in H$. \square

10.3. **Lagrange theorem.** If we put this together we get:

Theorem 10.6 (Lagrange). *If H is a subgroup of a finite group G then the order of H divides the order of G and the quotient*

$$|G|/|H|$$

*is equal to the number of left cosets of H in G . This is called the **index** of H in G and denoted $|G : H|$.*

Lagrange's theorem says that the order of a subgroup divides the order of the group. Here are some immediate consequences.

Corollary 10.7. *If $g \in G$ then the order of g divides the order of G .*

Proof. The order of g is equal to the order of the cyclic subgroup $\langle g \rangle$: $|g| = |\langle g \rangle|$ which divides $|G|$ by Lagrange. \square

Corollary 10.8. *If $|G| = n$ then $g^n = e$ for all $g \in G$.*

Proof. The previous corollary said that $n = mk$ if $|g| = m$. Then

$$g^n = g^{mk} = (g^m)^k = e^k = e$$

Or, you can just use the rule that $g^n = e$ iff n is a multiple of $|g|$. \square

Corollary 10.9. *If p is a prime then*

$$x^p \equiv x \pmod{p}$$

for any integer x .

Proof. Here the group is $U(p) = \{1, 2, \dots, p-1\}$ which has order $p-1$. The previous corollary implies that

$$x^{p-1} \equiv 1 \pmod{p}$$

if x is not divisible by p . So, $x^p \equiv x$ in those cases. If $p|x$ then $x^p \equiv 0 \equiv x$. So, the formula also holds in that case. So, it holds in all cases. \square

11. DIRECT PRODUCT

The **Cartesian product** of sets $S_1 \times S_2 \times \cdots \times S_n$ is the set of all ordered n -tuples (x_1, x_2, \cdots, x_n) where $x_i \in S_i$.

Question: How many elements does $S_1 \times S_2 \times \cdots \times S_n$ have?

Definition 11.1. If G_1, \cdots, G_n are groups then the **direct product**

$$G_1 \times G_2 \times \cdots \times G_n$$

is the group of all ordered n -tuples (a_1, \cdots, a_n) under coordinate-wise multiplication:

$$(a_1, \cdots, a_n)(b_1, \cdots, b_n) = (a_1b_1, \cdots, a_nb_n)$$

This may be more familiar when the group operation is addition:

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n)$$

In the additive case, when n is finite, the direct product of additive groups is called the **direct sum** and is sometimes written

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$

For example:

$$\mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}$$

Problem: If $g \in G$ has order 4 and $h \in H$ has order 6 then show that the element $(g, h) \in G \times H$ has order 12 (the least common multiple of 4 and 6).

Problem: If $o(g) = n$ and $o(h) = m$ are relatively prime then show that (g, h) has order nm .

Theorem 11.2. If n, m are relatively prime then $\mathbb{Z}_n \times \mathbb{Z}_m$ is a cyclic group of order nm . I.e.,

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

where \cong means isomorphic.

The rest of this section will be covered by Bong Lian next week.

Also, we will skip section 12. A more useful application of group theory is RSA: You choose a group G , write your message as an element $g \in G$ and raise it to a power, say g^3 . This is the coded form of your message. It is impossible to find the cube root of g^3 without knowing the order of the group. For example, if you know that your group has order 220 then you just raise to the 147-th power to get the original message:

$$(g^3)^{147} = g^{441} = (g^{220})^2 g = g.$$

The time it takes to raise to the n -th power is on the order of $\log n$.

13. HOMOMORPHISMS

Definition 13.1. A homomorphism $\phi : G \rightarrow H$ is a mapping between groups satisfying the condition

$$\phi(gh) = \phi(g)\phi(h)$$

for all $g, h \in G$.

We will look at examples and study the elementary properties (in terms of elements) and the structural properties in terms of subgroups. The difference between homomorphisms and isomorphisms is that homomorphisms need not be surjective nor do they have to be injective (1-1) and this leads to some very interesting properties which lie at the heart of the structural theory of groups.

Example 13.2. Examples of homomorphisms:

- (1) $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ where $\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$ is the multiplicative group of nonzero real numbers. This homomorphism is surjective but not injective.
- (2) If G is any group and $g \in G$ then the mapping $\phi : \mathbb{Z} \rightarrow G$ given by $\phi(n) = g^n$ is a homomorphism which is neither surjective nor injective.
- (3) $\text{sgn} : S_n \rightarrow \{1, -1\}$. This example defines the alternating group: $A_n := \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\}$.

Basic properties of homomorphisms:

- (1) $\phi(e_G) = e_H$. Proof: Take $g = h = e$ then

$$\phi(e)e_H = \phi(e) = \phi(ee) = \phi(e)\phi(e)$$

By cancellation we get $\phi(e) = e$.

- (2) $\phi(g^{-1}) = \phi(g)^{-1}$. Proof:

$$e = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}).$$

- (3) $\phi(g^n) = \phi(g)^n$. Pf: By induction on n .

Structural properties of homomorphisms depend on the following definitions and theorems.

Definition 13.3. A subgroup $N \leq G$ is called normal if

$$gNg^{-1} = N$$

for all $g \in G$. The notation is $N \trianglelefteq G$.

The equation $gNg^{-1} = N$ is the same as the equation

$$gN = Ng$$

In other words, left cosets are the same as right cosets. From this interpretation we know from the example that we had earlier that $H = \{e, (12)\}$ is not a normal subgroup of S_3 since the left cosets are different from right cosets. Let's examine the definition. Put $g = (13)$. Then $g^{-1} = (13)$ so

$$gHg^{-1} = (13)H(13) = \{(13)(13), (13)(12)(13)\} = \{e, (23)\}$$

This is not equal to $H = \{e, (12)\}$. So, H is not normal.

Normal subgroups are related to homomorphisms in the following way. This is a definition and a theorem.

Theorem 13.4. *If $\phi : G \rightarrow H$ is a homomorphism then the set of all $g \in G$ which go to e in H is a normal subgroup. It is called the **kernel** of ϕ .*

$$\ker \phi := \{g \in G \mid \phi(g) = e\} \trianglelefteq G.$$

Proof. The kernel of ϕ is a subgroup of G since

- (1) it contains e since $\phi(e) = e$
- (2) If $g \in \ker \phi$ then $\phi(g^{-1}) = \phi(g)^{-1} = e^{-1} = e$. So, $g^{-1} \in \ker \phi$.
- (3) If $g, h \in \ker \phi$ then $\phi(gh) = \phi(g)\phi(h) = ee = e$. So, $gh \in \ker \phi$.

To prove normality suppose that $h \in \ker \phi$. Then $\phi(h) = e$ so

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)e\phi(g)^{-1} = e$$

so $ghg^{-1} \in \ker \phi$ for all $g \in G$. So $\ker \phi$ is normal in G . \square

- (1) The kernel of $\det : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^\times$ is

$$\ker \det = \{A \in GL(n, \mathbb{R}) \mid \det A = 1\} = SL(n, \mathbb{R})$$

- (3) The kernel of $\text{sgn} : S_n \rightarrow \{1, -1\}$ is A_n .
- (2) What is the kernel of $\phi : \mathbb{Z} \rightarrow G$ given by $\phi(n) = g^n$?

Theorem 13.5. *The image of any homomorphism $\phi : G \rightarrow H$ is a subgroup of H .*

Proof. The image $\text{im } \phi$ is the set of all $\phi(g)$ where $g \in G$.

- (1) $\text{im } \phi$ contains $\phi(e) = e$.
- (2) Any element of $\text{im } \phi$ has the form $\phi(g)$. So, $\phi(g)^{-1} = \phi(g^{-1}) \in \text{im } \phi$.
- (3) The product of any two elements of $\text{im } \phi$ is: $\phi(g)\phi(h) = \phi(gh) \in \text{im } \phi$.

So, $\text{im } \phi$ is a subgroup of H . \square

The image of $\det : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^\times$ is \mathbb{R}^\times since any nonzero real number x is the determinant of the diagonal matrix with diagonal entries $x, 1, 1, \dots, 1$. What are the images in the other two examples?

One point which I forgot to make.

Lemma 13.6. *A subgroup N of G is normal if*

$$gNg^{-1} \subseteq N$$

for all $g \in G$.

This was used in the proof of Theorem 13.4. (We started with an element $h \in \ker \phi$ and showed that $ghg^{-1} \in \ker \phi$. This only proves that $gKg^{-1} \subseteq K$ for $K = \ker \phi$.

Proof. If $gNg^{-1} \subseteq N$ for all g then, in particular, this equation is true for g^{-1} . So

$$(g^{-1})N(g^{-1})^{-1} = g^{-1}Ng \subseteq N$$

Multiply by g on the left and g^{-1} on the right to get:

$$N \subseteq gNg^{-1}.$$

So, the two sets N, gNg^{-1} are contained in each other. So they are equal. \square

Problems

- (1) Use Lagrange to show that any group of prime order is cyclic.
- (2) If $|G| = pq$ where p, q are prime then any proper subgroup is cyclic.
- (3) If $o(g) = 2$ and g is the only element of G of order 2, then $\langle g \rangle$ is a normal subgroup of G .
- (4) If G is a finite group of order $2n$ then any subgroup of order n is normal.

Conjugation In class we talked about what happens when H is a subgroup of G which is not normal. Then gHg^{-1} is a subgroup of G which is different from H for some g . (It could be the same, for example $eHe^{-1} = H$.)

The groups H and gHg^{-1} are isomorphic. The isomorphism

$$\phi_g : H \rightarrow gHg^{-1}$$

is given by $\phi_g(h) = ghg^{-1}$. This is a homomorphism since

$$\phi_g(h)\phi_g(k) = ghg^{-1}gkg^{-1} = ghkg^{-1} = \phi_g(hk)$$

and it has an inverse given by $\phi_{g^{-1}}$:

$$\phi_{g^{-1}}\phi_g(h) = \phi_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}(g^{-1})^{-1} = h$$

The isomorphism ϕ_g is called **conjugation by g** and gHg^{-1} is called a **conjugate** of H . So, N is normal if N is “invariant under conjugation.”

14. FACTOR GROUPS

Factor groups are an example of the creative side of mathematics. Out of a group G and a normal subgroup N we make a new group G/N . We call this a “construction.”

If $N \triangleleft G$ then the set of cosets of N form a group with multiplication defined by

$$(aN)(bN) := abN$$

The additive notation is:

$$(a + N) + (b + N) := (a + b) + N$$

This group, whose elements are the cosets of N with operation defined by one of the two formulas above, is denoted G/N . To check that this is a group the only thing we have to check is that the multiplication is “well-defined” because the other conditions are obvious. (E.g., $eN = N$ is the identity, $(aN)^{-1} = a^{-1}N$.)

Well-defined means *independent of all choices*. But what choices did we make?

As I pointed out before, you get the same left coset in many ways.

$$a_1N = a_2N \iff a_1^{-1}a_2 \in N$$

So, suppose that $a_1N = a_2N$ and $b_1N = b_2N$. Then we have two different formulas for the product and we need to show:

$$a_1b_1N = a_2b_2N$$

In other words, we need to check that $(a_1b_1)^{-1}a_2b_2 \in N$. But:

$$(a_1b_1)^{-1}a_2b_2 = b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}(a_1^{-1}a_2)b_1(b_1^{-1}b_2) \in b_1^{-1}Nb_1N = NN = N$$

Theorem 14.1. *If N is a normal subgroup of a group G then the set G/N of cosets of N in G is a group with operation $(aN)(bN) = abN$.*

Proof. The verification of the definition of a group is very straightforward:

(1) $N = eN$ is the identity: $(eN)(aN) = eaN = aN$ and $(aN)(eN) = aeN = aN$.

(2) Multiplication of cosets is associative:

$$[(aN)(bN)](cN) = (abN)(cN) = abcN = (aN)(bcN) = (aN)[(bN)(cN)]$$

(3) The inverse of aN is $a^{-1}N$:

$$(aN)(a^{-1}N) = aa^{-1}N = eN$$

Therefore G/N is a group. □

Theorem 14.2. *If N is a normal subgroup of G then the mapping*

$$\gamma : G \rightarrow G/N$$

given by $\gamma(g) = gN$ is a surjective homomorphism.

Proof. This is obvious from the definition. □

14.1. **Example:** \mathbb{Z}/n . Take the additive group $G = \mathbb{Z}$. Since this is abelian, all subgroups are normal. Take the subgroup $4\mathbb{Z}$. There are 4 cosets:

$$\mathbb{Z}, 1 + \mathbb{Z}, 2 + \mathbb{Z}, 3 + \mathbb{Z}$$

If we use the notation

$$\bar{x} := x + 4\mathbb{Z}$$

then the 4 cosets: $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ and $\bar{0} = \bar{4} = \bar{8} = \bar{12} = \dots$ and similarly, the other cosets have many names. Addition is given by:

$$\bar{x} + \bar{y} = \overline{x + y}$$

This is just addition modulo 4. So,

$$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$$

The group $\mathbb{Z}/n\mathbb{Z}$ is often just written \mathbb{Z}/n .

14.2. Isomorphism theorems.

Theorem 14.3. *If $\phi : G \rightarrow H$ is a homomorphism of groups with kernel K then the factor group G/K is isomorphic to the image of ϕ and the isomorphism $\bar{\phi} : G/K \rightarrow \text{im } \phi$ is given by*

$$\bar{\phi}(gK) = \phi(g)$$

Proof. (1) This is well defined (independent of the choice of g) since $gK = hK$ iff $h^{-1}g \in K$ which implies that

$$\phi(h^{-1}g) = e = \phi(h)^{-1}\phi(g)$$

So, $\phi(h) = \phi(g)$.

(2) $\bar{\phi}$ is clearly onto. (Why?)

(3) To show that $\bar{\phi}$ is 1-1 suppose that $\bar{\phi}(gK) = \bar{\phi}(hK)$. Then $\phi(g) = \phi(h)$ So,

$$\phi(g^{-1}h) = \phi(g)^{-1}\phi(h) = e$$

In other words, $g^{-1}h \in K$. But this is the same as saying that $gK = hK$. So, $\bar{\phi}$ is 1-1.

(4) The homomorphism property:

$$\bar{\phi}(gKhK) = \bar{\phi}(ghK) = \phi(gh) = \phi(g)\phi(h) = \bar{\phi}(gK)\bar{\phi}(hK)$$

□

The original homomorphism $\phi : G \rightarrow H$ is factored as a composition of three homomorphisms:

$$\phi = \iota \circ \bar{\phi} \circ \gamma : G \xrightarrow{\gamma} G/N \xrightarrow{\bar{\phi}} \text{im } \phi \xrightarrow{\iota} H$$

Problem: If $N \triangleleft G$ what is the order of gN as an element in the group G/N ? How is the order of gN related to the order of g ? Take as an example $G = \mathbb{Z}_{12}$, $N = \langle 4 \rangle$, $g = 2$.

Answer: The order of gN is equal to the smallest positive integer k so that $g^k \in N$. In the example $g = 2$, $k = 2$ since $2 + 2 = 4 \in N$. This is related to the order of g : $o(g) = n$ by the fact that k divides n . In the example, $n = 6$ since $6 \cdot 2 = 0$.⁵

⁵The additive group notation is $kg = g + g + \cdots + g$ instead of $g^k = gg \cdots g$. An additive group often has other operations defined and we want to make sure we are talking about the group operation which is addition and not the other operations which are usually not a group operations.

15. SIMPLE GROUPS

If G is a group then the trivial group $\{e\}$ and the whole group G are normal subgroups of G . The group G is defined to be **simple** if there are no other normal subgroups and $G \neq \{e\}$. (You could rephrase this to say G is simple if it has exactly two normal subgroups.)

Theorem 15.1. *The cyclic group \mathbb{Z}_n is prime if and only if n is prime.*

Proof. Suppose $n = p$ is prime and H is a subgroup of \mathbb{Z}_p then $m = |H|$ divides p . So $m = p$ or $m = 1$. So, $H = G$ or $H = \{0\}$. So, \mathbb{Z}_p is simple.

Conversely, suppose that $G = \mathbb{Z}_n$ where n is not prime, say $n = pq$ where $1 < p < n$. Then

$$H = p\mathbb{Z}_n = \{0, p, 2p, \dots, (q-1)p\}$$

is a proper normal subgroup of G . So, \mathbb{Z}_n is not simple. \square

Problem: Suppose that n is a positive integer. What is $\mathbb{R}/n\mathbb{R}$?

Problem: Does this mean that $(\mathbb{R}, +)$ is a simple group?

Problem: Compute: $\mathbb{Z}_4 \times \mathbb{Z}_6 / \langle (2, 3) \rangle$. Here $\langle (2, 3) \rangle$ is the cyclic subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_6$ generated by the element $(2, 3)$. [Hint: Consider the homomorphism $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \rightarrow \mathbb{Z}_{12}$ given by $\phi(a, b) = 3a +_{12} 2b$. What are the kernel and image of ϕ ?]

Theorem 15.2. *The alternating group A_n is simple for all $n \geq 5$.*

I won't explain the proof of this (it is in the book). I want to explain instead why we care about simple groups.

The concept is that the simple groups are the "building blocks" out of which all finite groups can be constructed. If a group G is not simple, then G has a normal subgroup N with factor group G/N and we can reconstruct G out of these two pieces: $N, G/N$.

Definition 15.3. *We say that G is an **extension** of N by Q if N is a normal subgroup of G and Q is isomorphic to the quotient group G/N .*

Analogy: Simple groups are the "atoms" and all other finite group are "molecules" built out of these atoms.

15.1. Center of a group. If G is a nonabelian group then it has elements a, b which do not commute: $ab \neq ba$. But, it may have an element c which commutes with everything: $cg = gc$ for all $g \in G$. (Can you think of such an element?) Such an element is called *central*.

Definition 15.4. *The **center** $Z(G)$ of G is defined to be the set of all $c \in G$ which commutes with every element of G :*

$$Z(G) = \{c \in G \mid cg = gc \ \forall g \in G\}$$

Theorem 15.5. *The center of G is a normal subgroup of G .*

Example 15.6. *For example, the center of $GL(2, \mathbb{R})$ is given by:*

$$Z(GL(2, \mathbb{R})) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} : x \in \mathbb{R}^\times \right\}$$

Example 15.7. *The center of D_4 is the subgroup generated by t^2 , the 180° rotation. Since D_4 has only 8 elements you can go through the list and see that only e and t^2 are central.*

Proving that $Z(G)$ is a normal subgroup is very straightforward. You know how to show it is a subgroup. How do you show it is normal?

Problem: Show that the center of S_n is trivial for $n \geq 3$. [Hint: Suppose that $\sigma \in S_n$ is central and nontrivial. Then σ moves at least one letter, say $\sigma(x) = y$ where $x \neq y$. Now find another permutation τ so that $\sigma\tau \neq \tau\sigma$.]

15.2. Commutator subgroup. If $a, b \in G$ then the **commutator** of a and b is given by:

$$[a, b] := aba^{-1}b^{-1}$$

Problem: Show that a, b commute if and only if their commutator is trivial (equal to the identity e).

Two key points about commutators are

- (1) If the normal subgroup N contains all the commutators of G then G/N is abelian: $aba^{-1}b^{-1} \in N$ means

$$N = aba^{-1}b^{-1}N$$

Multiply both of these on the right by baN to get

$$(bN)(aN) = baN = aba^{-1}b^{-1}NbaN = abN = (aN)(bN)$$

- (2) Conjugates of commutators are commutators:

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$$

Definition 15.8. *The **commutator subgroup** G' of G is defined to be the subgroup of G generated by the commutators. This is a normal subgroup of G with abelian quotient G/G' .*

Example 15.9. A_n is the commutator subgroup of S_n for all $n \geq 1$.

Example 15.10. $SL(n, \mathbb{R})$ is the commutator subgroup of $GL(n, \mathbb{R})$ for all $n \geq 2$.

Theorem 15.11. *If N is a normal subgroup of G then G/N is abelian if and only if N contains G' .*

16. GROUP ACTIONS ON SETS

(Lecture by Bong Lian, notes by Maxim Starobinets.)

We try to analyze a group G by representing it as a symmetry of a set (in particular the dihedral group D_n and symmetric group S_n). That is, elements of G are represented as bijections of a particular set X (to itself: $X \rightarrow X$) in such a way that the group *multiplication* corresponds to composition of bijections and group *inversion* corresponds to taking the inverses of bijections.

16.1. Definition.

Definition 16.1. If G is a group and X is a set, a G -action on X (also called an action of G on the set X) is a mapping

$$* : G \times X \rightarrow X \quad (g, x) \mapsto gx$$

so that

- (1) $ex = x$ for all $x \in X$
- (2) $(g_1g_2)x = g_1(g_2x) \quad \forall x \in X, \forall g_1, g_2 \in G.$

In that case we say that X is a G -set

Example 16.2. Take any set X and recall that S_X is the set of all bijections of X to itself. So, $\sigma \in S_X$ iff σ is a map $\sigma : X \rightarrow X$, which is 1-1 and onto. S_X is a group under composition and S_X acts on X by $S_X \times X \rightarrow X$, $(\sigma, x) \mapsto \sigma(x)$. Note that

- (1) $(e, x) \mapsto e(x) = x$ since the identity element of S_X is the identity mapping on X .
- (2) $(\sigma\tau)(x) = (\sigma \circ \tau)(x) = \sigma(\tau(x))$ since multiplication in S_X is given by composition of maps.

Example 16.3. Choose $X = \mathbb{Z}_n$. Then $S_X = S_n$ is the group of permutation of n letters.

Let X be any G -set and $H \leq G$. Then X is also an H -set. So:

Any subgroup $H \leq S_X$ acts on the set X .

Definition: If X is a G -set then for all $g \in G$ define

$$\sigma_g : X \rightarrow X \quad x \mapsto gx \quad \forall x \in X$$

In other words, $\sigma_g(x) = gx$.

Claim: σ_g is a bijection ($\sigma_g \in S_X$).

Proof. $\sigma_{g^{-1}}$ is the inverse of σ_g :

$$(\sigma_{g^{-1}} \circ \sigma_g)(x) = g^{-1}gx = x \quad \text{and} \quad (\sigma_g \circ \sigma_{g^{-1}})(x) = x$$

So, σ_g is a bijection. □

So, from any G -set X we get a mapping

$$\phi : G \rightarrow S_X, \quad g \mapsto \sigma_g$$

Are the following equal?

$$\phi(g_1)\phi(g_2) = \sigma_{g_1} \circ \sigma_{g_2} \quad \phi(g_1g_2) = \sigma_{g_1g_2}$$

Take any $x \in X$. Then

$$\sigma_{g_1g_2}(x) = (g_1g_2)(x) = g_1(g_2(x)) = g_1\sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x)) = (\sigma_{g_1} \circ \sigma_{g_2})(x)$$

So, ϕ is a homomorphism. This proves the following theorem.

Theorem 16.4. *Let X be a G -set. For $g \in G$, the map $\sigma_g : X \rightarrow X$, $x \mapsto gx$ is a bijection of X to itself. The map $\phi : G \rightarrow S_X$, $g \mapsto \sigma_g$ is a group homomorphism.*

Question: Can we recover the G -action on X from the homomorphism $\phi : G \rightarrow S_X$? Does ϕ always come from a G -action on X ?

Yes: The corresponding action is given by

$$* : G \times X \rightarrow X, \quad (g, x) \mapsto gx := \phi(g)(x)$$

$$(1) \quad ex =_? x \quad \forall x \in X$$

$$ex := \phi(e)(x) = id_X(x) = x$$

$$(\phi(e) = e = id \text{ in } S_X \text{ because } \phi \text{ is a homomorphism.})$$

$$(2) \quad (g_1g_2)(x) =_? g_1(g_2(x)):$$

$$(g_1g_2)(x) = \phi(g_1g_2)(x) = [\phi(g_1)\phi(g_2)](x)$$

$$= \phi(g_1)[\phi(g_2)(x)] = \phi(g_1)(g_2x) = g_1(g_2(x))$$

So, we get an action $*$ which is completely specified by the homomorphism ϕ . By the theorem, an action gives a homomorphism. So, specifying a G -action on X is equivalent to specifying a group homomorphism $\phi : G \rightarrow S_X$.

16.2. Substructures of G -actions on X . Let X be a G -set and let $\phi : G \rightarrow S_X$ be the corresponding group homomorphism. Then

$$\{g \in G \mid gx = x \ \forall x \in X\} \leq G$$

But, $gx = x \iff \phi(g)(x) = x$. So, $\phi(g) = id_X$ (identity bijection). So, the set above is

$$\{g \in G \mid \phi(g) = id_X\} = \ker \phi$$

is a normal subgroup of G . By the Isomorphism Theorem 14.3, ϕ induces a new group homomorphism

$$\bar{\phi} : G/\ker(\phi) \rightarrow S_X, \quad g\ker(\phi) \mapsto \phi(g)$$

(Wednesday, first review:)

X is a G -set

$\phi : G \rightarrow S_X$ is the associated group homomorphism

$\ker \phi \trianglelefteq G$ is a normal subgroup

The induced map

$$\mu = \bar{\phi} : G/\ker \phi \rightarrow S_X$$

makes X a $(G/\ker \phi)$ -set.

Definition 16.5. (1) A G -action on X is **faithful** if $\ker(\phi) = \{e\}$.

(2) A G -action on X is **transitive** if $\forall x_1, x_2 \in X \exists g \in G$ so that $gx_1 = x_2$.

Fact: G acts transitively on X iff $\phi(G)$ acts transitively on X .

Proof. Suppose G acts transitively on X . Take $x_1, x_2 \in X$. By supposition, $\exists g \in G$ s.t. $gx_1 = x_2$. But $gx_1 = \phi(g)x_1$, so $\exists \phi(g)$ s.t. $\phi(g)x_1 = x_2$. The other direction is analogous. \square

Example 16.6. The dihedral group $D_4 = \{e, t, t^2, t^3, s, st, st^2, st^3\}$ acts on $X = \{1, 2, 3, 4\}$ (the set of vertices of a square). D_4 also acts on the set of edges $E = \{s_1, s_2, s_3, s_4\}$ on the set of meridians $M = \{m_1, m_2\}$ diagonals $D = \{d_1, d_2\}$ and the center point C by:

	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C
σ_t	2	3	4	1	s_4	s_1	s_2	s_3	m_2	m_1	d_2	d_1	C
σ_s	2	1	4	3	s_1	s_4	s_3	s_2	m_1	m_2	d_2	d_1	C
σ_{st}	1	4	3	2	s_2	s_1	s_4	s_3	m_2	m_1	d_1	d_2	C

(See Figure 16.9 on page 156.) The action of D_4 on X and E are faithful and transitive. The action of D_4 on M, D, C are not faithful (t^2 is in the kernel of all 3 of these actions) but they are transitive actions.

16.2.1. *isotropy subgroup.*

Definition 16.7. Let X be a G -set and $g \in G$. Define:

$$X_g := \{x \in X \mid gx = x\} \subseteq X$$

This is the **g -fixed subset** of X . For $x \in X$ define:

$$G_x := \{g \in G \mid gx = x\}$$

This is the **stabilizer** or isotropy subgroup of x in G .

Theorem 16.8. If X is a G -set, given $x \in X$, $G_x \leq G$.

Proof. Let $g_1, g_2, g \in G_x$ Then

- (1) $e \in G_x$ since $ex = x$
- (2) $g_1g_2 \in G_x$ since $g_1g_2(x) = g_1x = x$
- (3) $g^{-1} \in G_x$? we know that $gx = x$ and we want to know⁶ that $g^{-1}x = x$. So, take the equation we know and act on both sides by g^{-1} :

$$g^{-1}(gx) = x = g^{-1}x.$$

□

16.2.2. *orbits.*

Definition 16.9. Let X be a G -set. A **G -orbit** in X is a subset of X given by

$$Gx = \{gx \mid g \in G\}$$

for some $x \in X$.

The same orbit can be written in different ways. For $x, y \in X$ when is $Gx = Gy$?

Lemma 16.10. $Gx = Gy$ iff $y \in Gx$

Proof. Suppose that $y \in Gx$. Then $y = gx$ for some $g \in G$. For any $g'y \in Gy$ we have

$$\underbrace{g'y}_{\in Gy} = \underbrace{g'g}_{\in G} x$$

So $Gy \subseteq Gx$. Also, $y = gx \Rightarrow g^{-1}y = x$. So, $x \in Gy$ which implies $Gx \subseteq Gy$. So, $Gx = Gy$.

Conversely suppose that $Gx = Gy$. Then $y \in Gy$ since $y = ey$. So, $y \in Gx$. □

⁶Many times we explain things by starting with what we don't know and ending up with something we know. That is not a proof. You need to rewrite the equation backwards starting with what we know.

Theorem 16.11 (Orbit-cosets correspondence). *Let X be a G -set and $x \in X$. Then there is a bijection:*

$$Gx \xrightarrow{\cong} G/G_x$$

from the G -orbit of x to the set of all left cosets of G_x . In particular, if G is finite then $|Gx|$ divides $|G|$.

Proof. The second assertion follows from the first assertion and Lagrange's theorem.

The first assertion: the bijection is given by $gx \mapsto gG_x$. This is well defined since (follow arrows to the right)

$$gx = hx \iff h^{-1}gx = x \iff h^{-1}g \in G_x \iff gG_x = hG_x$$

This also shows the mapping is 1-1 and onto. (Follow arrows to the left to show 1-1. Onto is obvious.) \square

Theorem 16.12 (Partition property of orbits). *Let X be a G -set. Then any two distinct G -orbits in the G -set are disjoint.*

Proof. The *contrapositive* of the theorem is: $Gx \cap Gy \neq \emptyset \Rightarrow Gx = Gy$. So, suppose $Gx \cap Gy$ is nonempty and $z \in Gx \cap Gy$. Then $z \in Gx$ and $z \in Gy$. So, by the lemma, $Gz = Gx$ and $Gz = Gy$. So, $Gx = Gy$. \square

So the different orbits of X are disjoint and give a partition of X :

$$X = \coprod Gx_i$$

(Disjoint union of different orbits Gx_i .)

Example 16.13. $D_4 = \{e, t, t^2, t^3, s, st, st^2, st^3\}$, $X = \{1, 2, 3, 4\}$ Take $x = 1 \in X$. The stabilizer of 1 is

$$G_1 = \{e, st\}$$

The orbit is $G1 = X$ with $|G1| = 4 = 8/2 = |G : G_1|$ elements since G_1 has the same cardinality as the set of left cosets of G_1 in G .

17. GROUP ACTIONS, CONTINUED

This is a review of group actions and an application to the theory of p -group. Details on p. 328 in the book.

17.1. orbit-stabilizer.

Theorem 17.1 (orbit-stabilizer formula). *If G acts on a set X and $x \in X$ then the size of the orbit of x is the index of the stabilizer:*

$$|Gx| = |G : G_x|$$

Proof. There is a bijection between the set of left cosets of $H = G_x$ and the orbit of x given by $\phi(gH) = gx$. To see that this is a bijection note that

$$gx = hx \iff x = g^{-1}hx \iff g^{-1}h \in G_x \iff gG_x = hG_x.$$

□

For example, suppose that the set $X = G$ with action of G given by conjugation:

$$g \cdot x = gxg^{-1}$$

Let's verify that this is an action.

- (1) $e \cdot x = exe^{-1} = x$
- (2) $(gh) \cdot x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g \cdot hxh^{-1} = g \cdot h \cdot x$.

The orbits of this action are called the **conjugacy classes** of G :

$$G \cdot x = \{gxg^{-1} \mid g \in G\}$$

The group G is a disjoint union of conjugacy classes and the number of conjugacy classes is called c .

$$G = \coprod_{i=1}^c G \cdot x_i$$

For example S_3 has $c = 3$ conjugacy classes. What are they?

Definition 17.2. *The **centralizer** of $x \in G$ is defined to be the stabilizer of x under this action:*

$$C(x) = \{g \in G \mid gxg^{-1} = x\}$$

The equation can also be written $gx = xg$. So this is the set of all elements of G which commute with x .

The orbit stabilizer formula in this case says that the size of the conjugacy class of $x \in G$ is equal to the index of the centralizer of x .

$$|G \cdot x| = |G : C(x)|$$

For example, $x = (12) \in S_3$ has 3 conjugates $(12), (23), (13)$ and its centralizer $C((12)) = \{e, (12)\}$ has 2 elements and these two numbers give $2 \cdot 3 = 6 = |S_3|$.

Putting these together we get:

$$|G| = \sum_{i=1}^c |G \cdot x_i| = \sum_{i=1}^c |G : C(x_i)|$$

In the case of $G = S_3$ this is:

$$\begin{aligned} |S_3| &= |S_3 : C(e)| + |S_3 : C((12))| + |S_3 : C((123))| \\ 6 &= 1 + 3 + 2 \end{aligned}$$

The first number is 1 since $C(e) = S_3$.

Problem: a) Show that $C(g) = G$ if and only if $g \in Z(G)$.

b) Show that every element of $Z(G)$ is in its own conjugacy class.

This implies that the number of times the index $|G : C(x_i)|$ is equal to 1 is the number of elements in the center $Z(G)$. Call this $z = |Z(G)|$. For example, $z = |G|$ if G is abelian.

Theorem 17.3 (class formula). *If G is a finite group then*

$$|G| = |Z(G)| + \sum_{\neq 1} \underbrace{|G : C(x_i)|}$$

Corollary 17.4. *If the order of G is a power of a prime: $|G| = p^k$, $k \geq 1$ then G has a nontrivial center.*

Proof. In the class formula, all the numbers divide p^k . So, the numbers which are not 1, such as $|G|$ and $|G : C(x_i)|$ are multiples of p . Therefore, $|Z(G)|$ is divisible by p . But $e \in Z(G)$. So $Z(G)$ must have at least p elements. \square

For example D_4 has $8 = 2^3$ elements and its center has $p = 2$ elements.

Corollary 17.5. *There are no nonabelian simple p -groups (groups whose order is a power of the prime p).*

Proof. Any nontrivial p -group P has a nontrivial center $Z(P)$ which we know is a normal subgroup of P . If P is simple then we must have $P = Z(P)$. So, P is abelian (which implies P has order p . Why?) \square

17.2. Burnside's theorem. This is a formula for counting the number of orbits of a finite group acting on a finite set. (From Maxim's notes on Bong Lian's lecture.)

Theorem 17.6 (Burnside). *If G is a finite group and X is a finite G -set then*

$$(\#G\text{-orbits in } X) \cdot |G| = \sum_{g \in G} |X_g|$$

Proof. We count the number of elements in the same set S in two different ways.

$$S = \{(g, x) \in G \times X \mid gx = x\}$$

(1) "Freeze" g . For $g_1 \in G$ put $S_{g_1} := \{(g_1, x) \in S\} \subseteq S$. Then

$$S = \coprod_{g \in G} S_g$$

since $S_{g_1} \cap S_{g_2} = \emptyset$ if $g_1 \neq g_2$. For each $g \in G$ there is a bijection:

$$S_g = \{(g, x) \in S\} \xleftrightarrow{1:1} X_g$$

given by

$$(g, x) \xleftrightarrow{1:1} x$$

So, the size of the set S is given by

$$|S| = \sum_{g \in G} |S_g| = \sum_{g \in G} |X_g|$$

(2) "Freeze" x . For $x \in X$ put

$$S^x := \{(g, x) \in S\} = \{(g, x) \mid gx = x\}$$

Then S is the disjoint union of S^x and we have a bijection

$$S^x \xleftrightarrow{1:1} G_x \quad (g, x) \xleftrightarrow{1:1} g$$

So, the size of S is also given by

$$|S| = \sum_{x \in X} |S^x| = \sum_{x \in X} |G_x|$$

(3) $|G|/|G_x| = |G_x|$ (orbit-coset correspondence). Solve for $|G_x|$ to get:

$$|G_x| = \frac{|G|}{|G_x|}$$

For any x we get an orbit Gx . But we get the same orbit for each $y \in Gx$. If r is the number of orbits and we name the orbits $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_r$. Then $X = \coprod \mathcal{O}_i$ and

$$\sum_{x \in X} \frac{1}{|Gx|} = \sum_{i=1}^r \underbrace{\sum_{x \in \mathcal{O}_i} \frac{1}{|Gx|}}_{=1 \text{ since } |Gx| = |\mathcal{O}_i|} = r$$

Putting (2), (3) together we get

$$|S| = \sum_{x \in X} |Gx| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \cdot \sum_{x \in X} \frac{1}{|Gx|} = |G| \cdot r$$

Compare with (1): $|S| = \sum_{g \in G} |X_g|$ to get

$$|G| \cdot (\# \text{ of orbits}) = \sum_{g \in G} |X_g|$$

□

Example 17.7. *How many different dice (6-face) can one make? (Consider any rotation of a die as the same.) The group of rotations of the cube has 24 elements. They form a subgroup of S_8 (since G acts faithfully on the set of vertices) and G forms a subgroup of S_6 since it acts faithfully on the set of faces.*

Let X be the set of all possible ways of marking the cube (with 1, 2, \dots , 6 spots on the 6 sides) including rotationally equivalent markings. Then $|X| = 6! = 720$. The number of distinguishable dice is

$$\begin{aligned} \# \text{ of orbits} &= \frac{1}{24} \sum_{g \in G} |X_g| \\ &= \frac{1}{24} |X_e| = \frac{1}{24} \cdot 720 = 30 \end{aligned}$$

since X_g is empty for $g \neq e$.

Example 17.8. *(From Homework 8 handout) Each of the 8 corners of a cube is to be tipped with one of four colors, each of which may be used on any number of corners. Find the number of distinguishable markings. Use the hint: the group of rotations of the cube has 24 elements consisting of the identity, 9 which leave a pair of opposite faces invariant, 8 which leave a pair of opposite vertices invariant and 6 leaving a pair of opposite edges invariant. (Invariant means staying in the same place but possibly rotated in that place.)*

The answer is:

$$\frac{1}{24} (8^4 + 3 \cdot 4^4 + 6 \cdot 2^4 + 8 \cdot 4^4 + 6 \cdot 4^4) = 356$$

This uses Burnside's formula:

$$r \cdot |G| = \sum_{g \in G} |X_g|$$

Where r is the answer to the question. G is the rotation group of the cube and $|G| = 24$ is given. X_g is the set of coloring of the cube which are fixed by the rotation g .

- (1) For $g = e$ all patterns are fixed. So, $X_e = X$ which has 8^4 elements since each of the 8 corners has 4 possible colors.
- (2) For g one of the 9 rotations which fix two opposite faces, there are 6 which are 90° rotations and 3 which are 180° rotations. The 3 which are 180° rotations have 4^4 possible colorings invariant under g since the 4 corners on the front must be the same color as the four in the back. This gives $|X_g| = 4^4$ three times. The 6 which are 90° rotations have 2^4 colorings giving $6 \cdot 2^4$ in the sum.
- (3) For g one of the 8 rotations which fix two opposite corners, these are 120° rotations which permute the other 6 corners in two 3-cycles. So, there are 4^4 ways to color this in a way fixed by the rotation. This gives $8 \cdot 4^4$ in the sum.
- (4) For g one of the 6 rotations which fix opposite edges, there are again 4^4 colorings fixed by g since the colors of the vertices on the front face determine the colors on the back face (if the fixed edges are pointing away from you). This gives the last term $6 \cdot 4^4$ in the sum.