Math 330-1: Abstract Algebra

Fall 2020, Northwestern University

Shuyi Weng

Disclaimer: These lecture notes are written for class-planning purposes only. They are not meant to be a substitution for the textbook. It is likely that the notes contain typos and mistakes. You are encouraged to let me know when you see any of those.

Last modified: Friday, November 20, 2020, 4:45pm

Contents

0 Introduction

Class 1
2020/09/16

0.1 As the title of the course suggest, we are going to study algebra in the abstract. To be more specific,

- **Abstraction** is when we shift from specifics to general. One characteristic of modern mathematics is to identify the structures and properties which some mathematical objects share in common. Abstraction occurs when we stop focusing too much on these objects and start to work with the shared structures and properties, sometimes without even knowing what the underlying objects are. This is also called the *axiomatic approach to mathematics*. The mentality of studying things without knowing what one is talking about is an incredible cognitive leap, and it is arguably the foundation of abstract mathematics.
- **Algebra** is an ancient subject that can be traced back to the Babylonians. It is the leap from playing with numbers to playing with letters representing numbers (probably your first encounter of abstraction) in grade school. Modern algebra studies *algebraic structures*. An algebraic structure is a set equipped with some number of operations, satisfying certain properties.

0.2 Example (*Vector spaces*)
You have already seen one algebraic structure before in linear algebra. A **vector space** is a set of vectors together with two operations: addition and scalar multiplication, satisfying various properties which we call the axioms of vector spaces.

0.3 In Math 330, the algebraic structures that we will focus on are *groups*, *rings*, and *fields*. Each quarter will be dedicated to one algebraic structure.

LaTeX TIPS
$\mathbb{Z}$ `\mathbb{Z}`
$\mathbb{Q}$ `\mathbb{Q}`
$\mathbb{R}$ `\mathbb{R}`
$\mathbb{C}$ `\mathbb{C}`

- **Groups** are sets that models symmetries of objects. For example, the set of rotations and reflections of a square forms the group D_8. Most groups that arise in mathematics are sets of symmetry transformations.
- **Fields** are sets with addition and multiplication, which obey all of the usual rules of elementary algebra. Specifically, subtraction and division by a non-zero element are well-defined "reverse operations" of addition and multiplication, respectively. The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are familiar examples of fields.
- **Rings** are algebraic structures more general than fields. Similar with fields, rings are sets with addition and multiplication. However, multiplication in a ring is not required to be commutative, and elements of a ring are not required to have multiplicative inverses. In another word, there may not be a good notion of division in a ring. The integers $\mathbb{Z}$ is an elementary example of a ring.

1 Arithmetics

1.1 Modular arithmetic

1.1 Theorem (*Division algorithm*)
Let a and b be integers with $b > 0$. Then there exist unique integers q and r with $0 \leq r < b$, such that $a = bq + r$. The integer q is called the **quotient** of a when divided by b, and the integer r is called the **remainder** of a when divided by b. If the remainder of a when divided by b is zero, we say b **divides** a, and we write $b \mid a$. Otherwise, we say b does not divide a, and we write $b \nmid a$.

LaTeX TIPS
$\mid$ `\mid`
$\nmid$ `\nmid`
$\equiv$ `\equiv`
$(\mathrm{mod}\ n)$ `\pmod{n}`

1.2 Definition (*Congruence*)
Let a and b be integers, and let $n > 0$. We say a is **congurent** to b **modulo** n if $n \mid (a - b)$, and we write $a \equiv b \pmod{n}$.

1.3 Theorem (*Some properties of modular congruence*)
Let $n > 0$. Then

(1) Congruence modulo n is an equivalence relation on the integers $\mathbb{Z}$.

(2) Congruence modulo n respects addition, subtraction, and multiplication; that is, if $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$, then $a + b \equiv c + d \pmod{n}$, $a - b \equiv c - d \pmod{n}$, and $ab \equiv cd \pmod{n}$,

1.4 Definition (*Modular arithmetic*)
Fix $n > 0$. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$; this is the set of equivalence classes of $\mathbb{Z}$ by congruence modulo n. Define operations $+_n$, $-_n$, and $\cdot_n$ on $\mathbb{Z}_n$ by

LaTeX TIPS
$+_n$ `+_n`
$-_n$ `-_n`
$\cdot_n$ `\cdot_n`

$$a +_n b \equiv a + b \pmod{n}, \quad a -_n b \equiv a - b \pmod{n}, \quad a \cdot_n b \equiv ab \pmod{n}.$$

We call these operations **addition modulo** n, **subtraction modulo** n, and **multiplication modulo** n, respectively.

1.5 Example
The following are the addition and multiplication tables in $\mathbb{Z}_6$.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1.6 Example
We can also solve algebraic equations under modular arithmetic. For example, we may look for an $x \in \mathbb{Z}_6$ that satisfies

$$x +_6 5 = 2.$$

Looking up the addition table, we deduce that $x = 3$.

We may also look for an $x \in \mathbb{Z}_6$ that satisfies

$$3 \cdot_6 x -_6 4 = 5.$$

First, we deduce that $3 \cdot_6 x = 5 +_6 4 = 3$. We may be tempted to conclude that $x = 1$. However, looking up the multiplication table, we see that $x = 3$ and $x = 5$ are both valid solutions. This is an example that "division modulo n" is not always well-defined.

1.7 Notation

When the modulo class is specified and the context is clear, we may omit the subscripts and just write as we would for regular number systems. For example, "we want to solve for $3x - 4 = 5$ in $\mathbb{Z}_6$."

1.8 We still want to know when we are able to do division modulo n. In another word, we want to know when do multiplicative inverses modulo n exist. Observing the multiplication table in $\mathbb{Z}_6$, we see that $1^{-1} = 1$ and $5^{-1} = 5$, but 2, 3, and 4 do not have multiplicative inverses.

1.9 Definition *(Greatest common divisor, relatively prime integers)*

Given integers $a, b > 0$, the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is the largest of all common divisors of a and b. When $\gcd(a, b) = 1$, we say a and b are **relatively prime**.

1.10 Theorem *(Bézout's identity)*

Given integers $a, b > 0$, there exist integers m and n such that

$$ma + nb = \gcd(a, b).$$

Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $ma + nb$.

This identity is an elementary fact in number theory. We will not show the proof here, but we will make use of this identity many times throughout the course.

1.11 Theorem

Class 2
2020/09/18

Let $n > 0$ be an integer, and let $k \in \mathbb{Z}_n$. Then k has a multiplicative inverse in $\mathbb{Z}_n$ if and only if n and k are relatively prime.

Proof

Suppose n and k are relatively prime. By definition, $\gcd(n, k) = 1$. By Bézout's identity, there exist $x, y \in \mathbb{Z}$ such that $nx + ky = 1$. Reading this equality modulo n, we have

$$nx + ky \equiv ky \equiv 1 \pmod{n}.$$

We see that $y \pmod{n}$ is an inverse of k in $\mathbb{Z}_n$.

Conversely, if k has a multiplicative inverse in $\mathbb{Z}_n$, we call its multiplicative inverse ℓ. Then $k\ell \equiv 1 \pmod{n}$. Thus 1 is an integer of the form $nx + ky$. By the second part of Bézout's identity, $\gcd(n, k) = 1$. □

1.2 Complex numbers

One of the most important number system in mathematics is the complex numbers $\mathbb{C}$. It arises from solving algebraic equations like $x^2 + 1 = 0$.

1.12 Definition (*Complex numbers*)
The symbol i is used to denote the **imaginary unit**, which is a solution to the quadratic equation $x^2 + 1 = 0$. A **complex number** is an expression of the form $a + bi$, where $a, b \in \mathbb{R}$. The set of all complex numbers is denoted by $\mathbb{C}$. Given a complex number $z = a + bi$, we say a is the **real part** of z, denoted by $\mathrm{Re}(z)$, and b is the **imaginary part** of z, denoted by $\mathrm{Im}(z)$. The **complex conjugate** of z, denoted by $\overline{z}$ and pronounced "z-bar", is $a - bi$.

LaTeX TIPS
$\overline{z}$ `\overline{z}`

The relation $i^2 = -1$ allows us to multiply complex numbers together.

1.13 Definition
The operation of **addition** $(+)$ and **multiplication** $(\cdot)$ of complex numbers are defined by

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

and

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i,$$

respectively.

1.14 From the definitions above, we can work out the rules for subtraction and division by a non-zero complex number. Subtraction is straightforward:

LaTeX TIPS
$\frac{a}{b}$ `\frac{a}{b}`

$$(a + bi) - (c + di) = (a - c) + (b - d)i.$$

Division is slightly trickier. The trick to division is to multiply both the divident and the divisor by the complex conjugate of the divisor:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2}.$$

Of course, division does not work if and only if $c+di = 0$, where the denominator above $c^2 + d^2 = 0$.

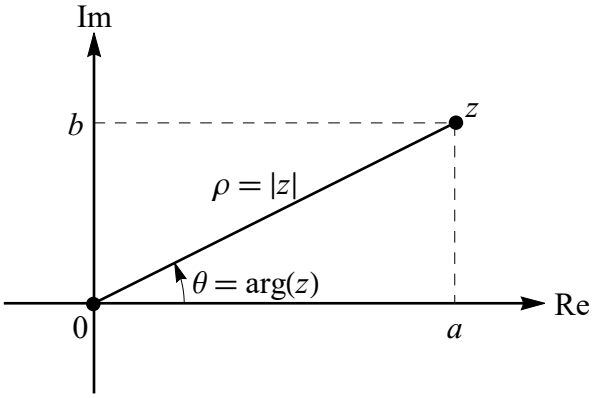
1.15 Example
Compute $(3 + 4i) \cdot (1 - i)$ and $(5 + 5i)/(2 + i)$.

$$(3 + 4i) \cdot (1 - i) = (3 + 4) + (4 - 3)i = 7 + i,$$

$$\frac{5 + 5i}{2 + i} = \frac{(5 + 5i)(2 - i)}{(2 + i)(2 - i)} = \frac{(10 + 5) + (10 - 5)i}{2^2 + 1^2} = \frac{15 + 5i}{5} = 3 + i.$$

1.16 Geometrically speaking, the complex number $a + bi \in \mathbb{C}$ can be identified with the point $(a, b) \in \mathbb{R}^2$. This is in fact a one-to-one correspondence between $\mathbb{C}$ and $\mathbb{R}^2$. The identification gives rise to the *complex plane*.

1.17 Definition *(Modulus and argument)*
Given a complex number $z = a+bi \in \mathbb{C}$, the **absolute value** (or the **modulus**) of z, denoted by $|z|$, is given by the distance from z to the origin in the complex plane. The **argument** of z, denoted by $\arg(z)$, is the angle that the line segment from 0 to z makes with the positive real axis.



Thus $\rho = |z| = \sqrt{a^2+b^2}$ and $\tan(\theta) = b/a$. This gives rise to the *polar form* of complex numbers:

$$z = \rho(\cos(\theta) + i\sin(\theta)),$$

where $\rho = |z|$ and $\theta = \arg(z)$.

LaTeX TIPS
$\sqrt{x}$ `\sqrt{x}`

The *Euler's formula* provides a compact notation for the polar form of complex numbers.

LaTeX TIPS
Greek letters:
α `\alpha`
β `\beta`
ζ `\zeta`
θ `\theta`
π `\pi`
ρ `\rho`
etc.

1.18 Theorem *(Euler's formula)*
For all $\theta \in \mathbb{R}$, we have $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.

PROOF
This is Problem 2(a) of Homework #1. □

With Euler's formula, we can write

$$z = |z|e^{i\arg(z)}.$$

It gives us the extra insight that when two complex numbers z and w are multiplied, the modulus of the product is the product of the moduli of z and w, and the argument of the product is the sum of the arguments of z and w. It also allows us to conveniently solve the *root of unity* problem.

1.19 Definition *(Root of unity)*
Fix a positive integer n. A complex number $z \in \mathbb{C}$ is an **n-th root of unity** if it satisfies $z^n = 1$.

1.20 Example
The imaginary unit i is a fourth root of unity because $i^4 = (i^2)^2 = (-1)^2 = 1$.

1.21 Example

With Euler's formula, we can see that all n-th roots of unity are

$$1, e^{2\pi i/n}, e^{4\pi i/n}, e^{6\pi i/n}, \ldots, e^{2(n-1)\pi i/n}.$$

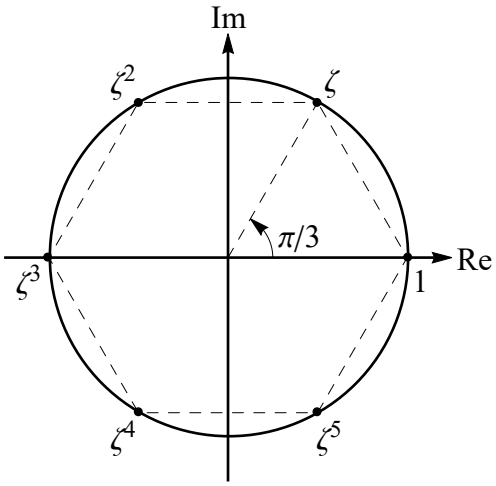
In many contexts, we let $\zeta = e^{2\pi i/n}$ and write all n-th roots of unity as

$$1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}.$$

1.22 Example

Class 3
2020/09/21

All sixth roots of unity are located on the unit circle:



The product of two sixth roots of unity is again a sixth root of unity. This can be shown with the relation

$$(\zeta^k \cdot \zeta^\ell)^6 = (\zeta^{k+\ell})^6 = (\zeta^6)^{k+\ell} = 1^{k+\ell} = 1.$$

Additionally, we can construct a multiplication table for sixth roots of unity.

$\cdot$	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
1	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
ζ	ζ	ζ^2	ζ^3	ζ^4	ζ^5	1
ζ^2	ζ^2	ζ^3	ζ^4	ζ^5	1	ζ
ζ^3	ζ^3	ζ^4	ζ^5	1	ζ	ζ^2
ζ^4	ζ^4	ζ^5	1	ζ	ζ^2	ζ^3
ζ^5	ζ^5	1	ζ	ζ^2	ζ^3	ζ^4

If we look closely enough, we notice that this table is essentially the same with the addition table of $\mathbb{Z}_6$ in Example 1.5. The only difference is the names we have assigned to the elements of $\mathbb{Z}_6$ and the sixth roots of unity. This means that multiplication of sixth roots of unity behaves like addition modulo 6.

In fact, the same argument could be said about any positive integer n. This is an example of an *isomorphism*, the name which derived from "equal-form-ness" in Greek. We will see more about it very soon.

2 Binary Structures

2.1 Binary operations

2.1 Definition (*Operations*)
Given a set S. An **operation** on S is a function $*\colon S^n \to S$. In plain language, it is a function that takes n inputs in S and outputs one element in S. We say an operation is **unary**, **binary**, **ternary** if the number n is 1, 2, 3, respectively.

LaTeX TIPS
$f\colon A \to B$
`f \colon A \to B`

2.2 Example
You have already seen many familiar examples of operations.

LaTeX TIPS
$M \mapsto M^{-1}$
`M \mapsto M^{-1}`

- Addition ($+$) and multiplication ($\times$) are binary operations on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, as well as on $\mathbb{Z}_n$.
- Negation ($x \mapsto -x$) is a unary operation on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
- Division is a binary operation on $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, but not on the entire $\mathbb{Q}$ because we cannot divide by 0.
- Division is not a binary operation on $\mathbb{Z}$ because $\mathbb{Z}$ does not contain fractions.
- The logic operators `AND`, `OR`, `XOR` are binary operations on $\{\texttt{True}, \texttt{False}\}$, while `NOT` is a unary operation on $\{\texttt{True}, \texttt{False}\}$.
- The cross product is a binary operation on $\mathbb{R}^3$, but the dot product is not because its output is a scalar rather than a vector.
- Matrix inversion ($M \mapsto M^{-1}$) is a unary operation on the set of all invertible $n \times n$ matrices with real entries.

In this course, we will mostly focus on binary operations on sets. For a set S together with a binary operation $*$ on S, we call the pair $(S, *)$ a **binary structure**. For finite sets, the most straightforward method to define a binary operation is to use a *Cayley table*.

2.3 Example
Let $S = \{a, b, c\}$ be a set of three letters, and let $*$ be a binary operation on S be defined by the following table:

$*$	a	b	c
a	a	b	c
b	b	b	b
c	c	a	c

Reading off the table, we know that $a * a = a$, $c * b = a$, and $b * c = b$, *etc.*

2.4 Remark
There are a few requirements and conventions in regard to Cayley tables.

- Each element appears exactly once in the top row; each element appears exactly once in the leftmost column.

- The elements of S should be listed as heads across the top in the same order as heads down the leftmost column.
- The entry in the i-th row and j-th column of the table body is

  (i-th entry in the leftmost column) $*$ (j-th entry in the top row),

  which must be an element of S.

2.2 Structural properties

We can define however many binary operations as we wish. But it would be nicer to recognize when some of them are "similar" or even "the same" (like we observed in Examples 1.5 and 1.22). *Structural properties* are properties of binary operations that must be shared between binary operations which are essentially the same. Three structural properties that we are going to focus on in this section are *associativity*, *commutativity*, and *unitality*.

2.5 Definition (*Associativity*)
A binary operation $*$ on a set S is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

2.6 Example
Many familiar examples of binary structures are associative.

- Addition is associative on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$. In each of these sets, we have $(a + b) + c = a + (b + c)$ for all a, b, c.
- Multiplication is associative on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$. In each of these sets, we have $(ab)c = a(bc)$ for all a, b, c.
- Matrix multiplication is associative on the set $\mathsf{Mat}_n(\mathbb{R})$ of $n \times n$ matrices over $\mathbb{R}$, because $(AB)C = A(BC)$ if A, B, and C are all $n \times n$ matrices.

Subtraction on $\mathbb{R}$ is not associative. For example, $(3-2)-1 = 0$ but $3-(2-1) = 2 \neq 0$.

2.7 Definition (*Commutativity*)
A binary operation $*$ on a set S is **commutative** if $a * b = b * a$ for all $a, b \in S$.

2.8 Example
Again, many familiar examples of binary structures are commutative.

- Addition is commutative on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$. In each of these sets, we have $a + b = b + a$ for all a, b.
- Multiplication is commutative on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$. In each of these sets, we have $ab = ba$ for all a, b.

Matrix multiplication is not commutative on $\mathsf{Mat}_n(\mathbb{R})$ for $n \geq 2$. For example, when $n = 2$,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ but } \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

LaTeX TIPS

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

```
\begin{bmatrix}
  1 & 0 \\
  0 & 1 \\
\end{bmatrix}
```

2.9 Definition (*Unitality*)
A binary operation $*$ on a set S is **unital** if there exists an element $e \in S$ such that $e * a = a * e = a$ for all $a \in S$. The element e here is called an **identity element** for the operation $*$.

2.10 Example
Many familiar examples of binary structures are unital.

- Addition is unital on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$. In each of these sets, 0 is the identity element because $0 + a = a + 0 = a$ for all a.
- Multiplication is unital on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$. In each of these sets, 1 is the identity element because $1 \cdot a = a \cdot 1 = a$ for all a.
- Matrix multiplication is associative on $\mathsf{Mat}_n(\mathbb{R})$, with the identity matrix $I \in \mathsf{Mat}_n(\mathbb{R})$ as the identity element as $IA = AI = A$ for all $A \in \mathsf{Mat}_n(\mathbb{R})$.

A non-example would be multiplication on the set $2\mathbb{Z}$ of even integers. In this case, $1 \notin 2\mathbb{Z}$, and we cannot find any even integer e which satisfies $e \cdot n = n \cdot e = n$ for all $n \in 2\mathbb{Z}$.

2.11 Theorem (*Uniqueness of identity*)
Let $(S, *)$ be a binary structure. If $*$ is unital, it has a unique identity element.

Proof
Let e_1, e_2 both be identity elements. Then $e_1 = e_1 * e_2 = e_2$ by definition. □

We are due for a less familiar example of binary structure.

2.12 Example
Let $C(\mathbb{R})$ be the set of continuous functions $f : \mathbb{R} \to \mathbb{R}$. Then function composition $\circ$ is a binary operation on $C(\mathbb{R})$ because the composition of two continuous functions is a continuous function as well. Moreover, it is associative and unital.

Associativity Let $f, g, h \in C(\mathbb{R})$. Then for all $x \in \mathbb{R}$, we have

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

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

Unitality Let $e(x) = x$. We will show e is the identity element in $C(\mathbb{R})$. Let $f \in C(\mathbb{R})$. Then for all $x \in \mathbb{R}$, we have

$$(f \circ e)(x) = f(e(x)) = f(x), \text{ and } (e \circ f)(x) = e(f(x)) = f(x).$$

Therefore, $f \circ e = e \circ f = f$.

However, $\circ$ is not commutative on $C(\mathbb{R})$. For example, if $f(x) = x^2$ and $g(x) = x + 1$, then

$$(g \circ f)(x) = x^2 + 1, \text{ but } (f \circ g)(x) = (x + 1)^2,$$

and so $g \circ f \neq f \circ g$.

2.13 Remark

Class 4
2020/09/23

Given a binary structure $(S, *)$, by definition of binary operation, $a * b \in S$ for every $a, b \in S$. We say S is *closed* under the operation $*$, and call this the *closure property* of binary structures. In some text, closure is also considered as a structural property, although it is axiomatic in the sense that it is a direct consequence of how we defined binary operations. However, closure can be used to describe subsets of binary structures.

2.14 Definition (*Closure*)

Let $(S, *)$ be a binary structure, and let H be a subset of S. We say H is **closed** under $*$ if $a * b \in H$ for all $a, b \in H$. In this case, we obtain a new binary structure $(H, *)$ **induced** from $(S, *)$.

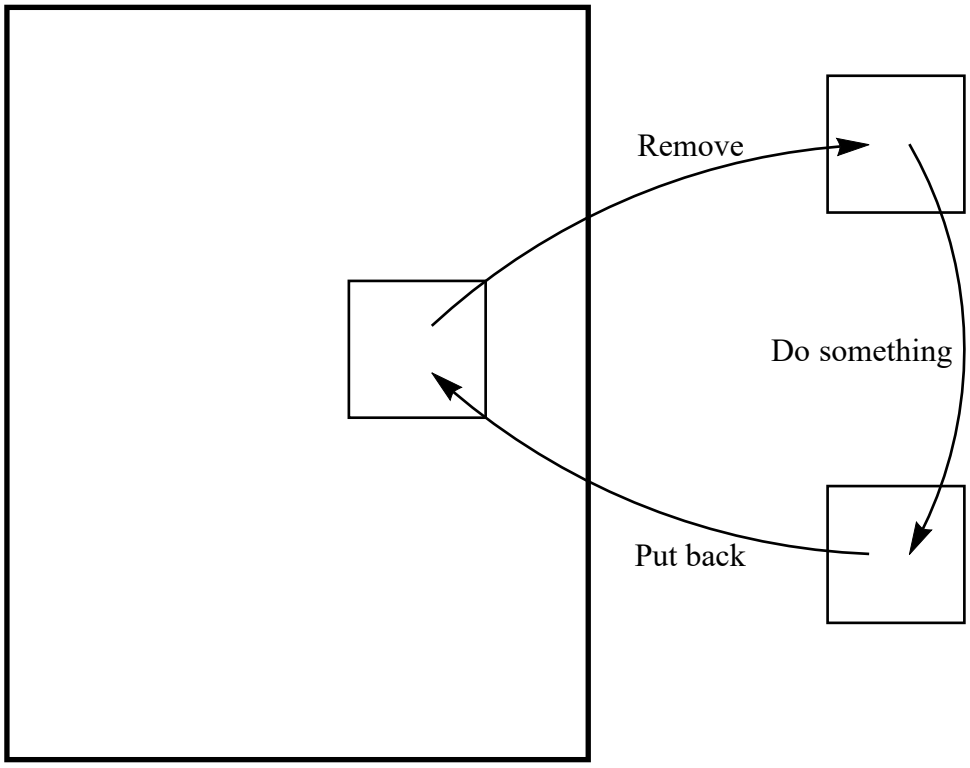
2.15 Example

Addition on complex numbers $(\mathbb{C}, +)$ is a binary structure. The subsets $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $2\mathbb{Z}$ (even integers), and $\mathbb{N}$ (natural numbers) of $\mathbb{C}$ are all closed under $+$. However, the set of odd integers is not closed under $+$ because the sum of two odd integers is an even integer.

3 Groups and Subgroups

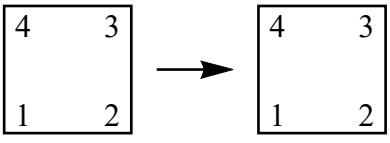
3.1 Case study: symmetries of a square

Suppose we remove a square region on a piece of printer paper. How many ways are there can we put it back into the hole it has left on the paper? More specifically, we want to describe the possible changes in the orientation of the square in terms of motions that result in these changes.

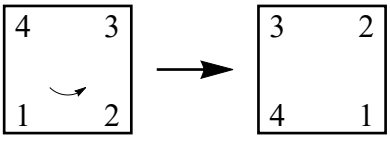


To visualize the change of orientation, we may label the corners with 1, 2, 3, and 4. This makes it easy to distinguish between motions that changes the orientation of the square in different ways. It is worth noting that we regard a 90° counterclockwise rotation the same as a 270° clockwise rotation, because the resulting orientations of the square are the same. With some experimentation, we can find eight motions that result in distinct orientations of the square.

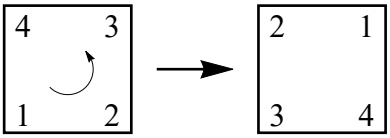
R_0 = rotation of 0°



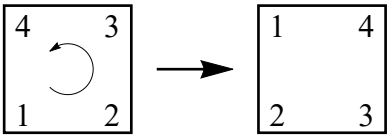
R_{90} = rotation of 90° (counterclockwise)



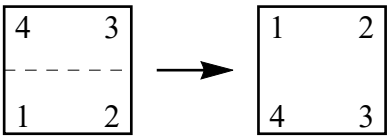
R_{180} = rotation of 180°



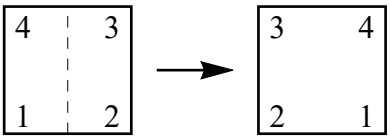
R_{270} = rotation of 270°



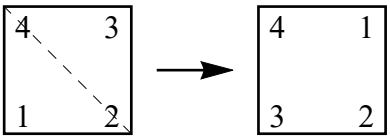
H = horizontal reflection



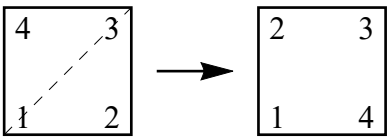
V = vertical reflection



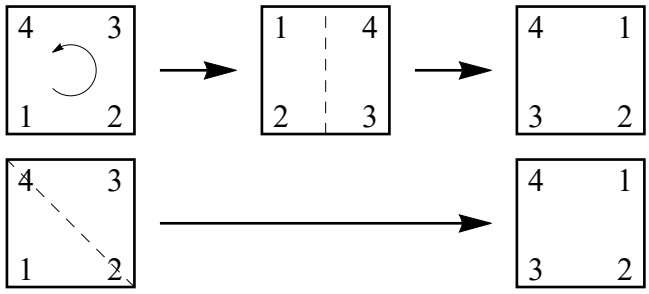
D = reflection across the main diagonal



A = reflection across the anti-diagonal



Further, if two motions are done one after the other, the result is once again one of the eight motions above. For example, if we rotate the square counterclockwise by 270°, then flip it across the vertical axis of symmetry, the resulting orientation of the square is the same with the result of reflection across the main diagonal.



This defines a binary operation $\star$ on the set

$$S = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, A\}$$

of distinct motions of the square, where the binary operation $\star$ could be interpreted as "following". The example above shows that doing V following R_{270} is the same with doing D alone. Symbolically, we could write $V \star R_{270} = D$.

3.1 Remark

We recall from Math 300 that, when we compose two functions, $f \circ g$ means "f following g". The order of computation is from the right to the left. We adopt this convention when we combine two motions of the square. In a later part of the course, we will see that these motions are indeed functions defined on appropriate spaces.

3.2 The Cayley table of the binary structure $(S, \star)$ is constructed below.

$\star$	R_0	R_{90}	R_{180}	R_{270}	H	V	D	A
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	A
R_{90}	R_{90}	R_{180}	R_{270}	R_0	A	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	A	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	A	V	H
H	H	D	V	A	R_0	R_{180}	R_{90}	R_{270}
V	V	A	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	A	H	R_{270}	R_{90}	R_0	R_{180}
A	A	H	D	V	R_{90}	R_{270}	R_{180}	R_0

From the Cayley table, we observe that $(S, \star)$ is unital, with R_0 as the identity element. We also observe that $(S, \star)$ is not commutative, because $R_{270} \star V = A$, while we have previously noticed that $V \star R_{270} = D \neq A$. Associativity is less obvious from the Cayley table. But if we consider these motions as functions, associativity is a direct consequence.

Independent of the structural properties we noted above, we also observe that each motion in $(S, \star)$ is a physical action on the cut-off square, and they could be "undone" by another motion. For example, we can undo a counterclockwise 90° rotation R_{90} by a clockwise 90° rotation, or equivalently, a counterclockwise 270° rotation R_{270}. In fact, we observe that each column of the Cayley table above has an identity element R_0, meaning that every motion in S could be undone by some motion in S. We can state a similar statement about each row of the Cayley table: every motion could undo some motion in S. It turns out that "being able to undo" is also a structural property of binary operations.

3.3 Definition *(Invertibility)*

Let $\star$ be a binary operation on S that is associative and unital with identity element $e \in S$. An element $a \in S$ is **invertible** (under the operation $\star$) if there exists $b \in S$ such that $a \star b = b \star a = e$. In this case, we say b is an **inverse** of a.

3.4 Example

In the binary structure $(S, \star)$ of motions of a square, each motion has an inverse, and they are matched in the following table.

Motion	R_0	R_{90}	R_{180}	R_{270}	H	V	D	A
Inverse	R_0	R_{270}	R_{180}	R_{90}	H	V	D	A

3.5 Example
In $(\mathbb{Z}, +)$, each integer n is invertible, and the inverse is the negation $-n$:

$$n + (-n) = (-n) + n = 0.$$

However, not every integer in $(\mathbb{Z}, \cdot)$ is invertible, because $\mathbb{Z}$ does not contain fractions. In fact, only ± 1 are invertible in $(\mathbb{Z}, \cdot)$.

3.6 Example
Consider the binary structure $(\mathbb{Z}_8, \cdot_8)$. We have proved in Theorem 1.11 that $k \in \mathbb{Z}_8$ is invertible if and only if k and 8 are relatively prime. Thus $1, 3, 5, 7 \in \mathbb{Z}_8$ are invertible under multiplication.

3.7 Notation
In a binary operation $(S, \star)$, we often write $S^* = \{a \in S \mid a \text{ is invertible}\}$ for the set of invertible elements. This notation is typically reserved for contexts where the binary operation $\star$ is some kind of *multiplication* or *composition*, rather than addition. Hence, we write $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ to mean the invertible elements in $(\mathbb{Z}_8, \cdot_8)$, not in $(\mathbb{Z}_8, +_8)$.

LaTeX TIPS
Set notation:
$\{a \in S \mid a \text{ is invertible}\}$
`\{a \in S \mid a \text{is invertible}\}`

3.8 Theorem (*Uniqueness of inverse*)
Let $\star$ be a binary operation on S that is associative and unital. If $a \in S$ is invertible, then it has a unique inverse in S.

Proof
Let e be the identity element of $(S, \star)$, and let $b_1, b_2 \in S$ be inverses of a. Then

$$b_1 = b_1 \star e = b_1 \star (a \star b_2) = (b_1 \star a) \star b_2 = e \star b_2 = b_2$$

as required. □

3.9 Notation
The standard notations for the (unique) inverse of an element a is either a^{-1} or $-a$, depending on the nature of the operation. If the operation is understood to be some kind of multiplication or composition, we use the notation a^{-1}; on the other hand, if the operation is some kind of addition, we use $-a$.

3.2 Groups and some elementary properties

We are now ready to give the definition of a *group*, which is the central topic of this course.

3.10 Definition (*Groups*)
A **group** is a set G together with a binary operation $\star\colon G^2 \to G$ that satisfies the following properties:

Associativity axiom: $(g \star h) \star k = g \star (h \star k)$ for all $g, h, k \in G$;

Identity axiom: There exists $e \in G$ such that $e \star g = g \star e = g$ for all $g \in G$;

Inverse axiom: For all $g \in G$, there exists $h \in G$ such that $g \star h = h \star g = e$.

In addition, if the binary operation of a group G is commutative, we say G is an **abelian group**.

3.11 Remark
By Theorems 2.11 and 3.8, every group $(G, \star)$ has a unique identity element $e \in G$, and every element $a \in G$ has a unique inverse $a^{-1} \in G$ (or $-a \in G$ in additive contexts).

3.12 Example
The familiar addition operations on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$, and $\mathbb{Z}_n$ gives rise to abelian groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^n, +)$, and $(\mathbb{Z}_n, +_n)$. The identity element is 0 in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$, and the zero vector $\mathbf{0} \in \mathbb{R}^n$, and the inverse of a number x (or a vector $\mathbf{x} \in \mathbb{R}^n$) is the negation $-x$ (or $-\mathbf{x} \in \mathbb{R}^n$).

LaTeX TIPS
Vectors:
$\mathbf{0}$ `\mathbf{0}`
$\mathbf{x}$ `\mathbf{x}`

3.13 Example
The set of positive integers $\mathbb{Z}_{>0} = \{1, 2, 3, 4, \dots\}$ is not a group under addition. There is no identity element in $\mathbb{Z}_{>0}$, nor is any element invertible.

3.14 Example
The set of positive integers $\mathbb{Z}_{>0} = \{1, 2, 3, 4, \dots\}$ is not a group under multiplication, either. There is an identity element $1 \in \mathbb{Z}_{>0}$, but none of the other elements are invertible.

3.15 Example
The set of (multiplicatively) invertible elements in $\mathbb{Z}_8$ is a group under multiplication modulo 8. Recall that $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. Observe that

$$1 \cdot 1 \equiv 3 \cdot 3 \equiv 5 \cdot 5 \equiv 7 \cdot 7 \equiv 1 \pmod 8.$$

Hence, every element is its own inverse in this group.

3.16 Example
The set of symmetries of a square

$$S = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, A\}$$

is a group under the binary operation $\star$. This is our first example of a non-abelian group. In fact, this is the *dihedral group* of order 8, denoted by D_8. We will study dihedral groups in more details very soon.

3.17 Example
The set S of invertible 2×2 matrices is a group under matrix multiplication. Being invertible is equivalent to having a non-zero determinant. If $\det(A) \neq 0$ and $\det(B) \neq 0$, then $\det(AB) = \det(A)\det(B) \neq 0$. Thus the matrix product AB is also invertible. This shows that the set of invertible 2×2 matrices is closed under matrix multiplication.

Matrix multiplication is an associative operation, and the identity matrix I is the identity element in this binary structure. By construction, every matrix in S has a multiplicative inverse. In fact, there is a nice formula for the inverse:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

We see that S is indeed a group under matrix multiplication. This group is not abelian.

3.18 Notation

Class 5
2020/09/25

This is a good place to simplify our notations a little bit.

- First, we will usually just refer to a group as G, rather than $(G, \star)$. The binary operation is left implicit, as it can usually be inferred from context.
- Second, we will typically omit the binary operation symbol altogether, and write gh instead of $g \star h$. One exception is when the binary operation is some kind of addition, then we still keep the $+$ sign for the operation involved.
- Lastly, if we want to write the result of combining a few copies of the same element $g \in G$, instead of a long sequence such as $gg \dots g$, we will simply write g^n. Again, the exception is when the binary operation is some kind of addition. When the context is clear, the notation ng is sometimes employed.

The following lemma is extremely useful in finding the inverse of elements within a group. We will also have our first practice with the simplified notations.

3.19 Lemma

Let G be a group. If $a, b \in G$, then the inverse of ab is $b^{-1}a^{-1}$.

Proof

Let $e \in G$ be the identity of G. Then

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

Likewise, $(b^{-1}a^{-1})(ab) = e$. Hence, $b^{-1}a^{-1}$ is an inverse of ab. By uniqueness of inverse, we conclude that $(ab)^{-1} = b^{-1}a^{-1}$. □

Recall our main theme is to identify the "same-shape-ness" (isomorphism) within binary structures. As a start, two groups must have the same size in order to have the same structure. The notion of *order* captures the size of a group.

3.20 Definition (*Order of a group*)

The **order** of a group G is the cardinality of G. We say a group G is of order n if $|G| = n$. A **finite group** is when the order of the group is finite, while an **infinite** group is when the order of the group is infinite.

3.21 Example (*Groups of order 0*)

There is no group of order 0. The identity axiom asserts that any group must contain at least an identity element.

3.22 Example (*Groups of order 1*)

Once again, the identity axiom asserts that any group must contain at least an identity element. So a group G of order 1 must be one that only contains the identity element, *i.e.*, $G = \{e\}$. This is called the **trivial group**.

3.23 Example (*Groups of order 2*)
A group $(G, \star)$ of order 2 must contain the identity element and one other element. Its Cayley table must take the form

$\star$	e	a
e	e	a
a	a	?

There are only two options for the entry at the question mark: e and a. But we cannot fill it in with a, otherwise a would not have an inverse in G. So we must have $a^2 = e$.

Since the binary operation $\star$ is entirely determined by the group axioms, it follows that there is a unique group of order 2. This group is isomorphic to $\mathbb{Z}_2$.

The process of completing the unknown part of a Cayley table is very useful in determining group structure. The following lemma is helpful for this process.

3.24 Lemma
If G is a group and $a, b \in G$, then there is a unique solution $x \in G$ to the equation $ax = b$, and there is a unique solution $y \in G$ to the equation $ya = b$.

PROOF
Note that $ax = b$ if and only if $x = a^{-1}b$, and $ya = b$ if and only if $y = ba^{-1}$. □

3.25 Remark
Lemma 3.24 implies that the Cayley table for groups must contain every element of the group exactly once in every row and in every column. It also implies that the left and right cancellation laws hold in groups.

3.26 Example (*Groups of order 4*)
We have already seen some examples of groups of order 4, two of which are $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_8^*, \cdot_8)$, whose Cayley tables are shown below.

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

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

We observe that these two groups have different structures. In particular, every $x \in Z_8^*$ satisfies $x \cdot_8 x = 1$, the identity element in Z_8^*, whereas only $0, 2 \in Z_4$ satisfy the analogous equations $0 +_4 0 = 0$ and $2 +_4 2 = 0$. So there are at least two different groups of order 4 up to isomorphism. You will prove that there are exactly two groups of order 4 up to isomorphism on Homework #2.

The isomorphism class of the group $(\mathbb{Z}_8^*, \cdot_8)$ is often referred to as the **Klein 4-group**, denoted by K_4 or V. It is the group $K_4 = \{e, a, b, c\}$ that satisfies $c = ab$ and $a^2 = b^2 = c^2 = e$.

3.3 Subgroups

If we forget all the structures of a group G, to the bare bones, G is a set of items. Just like sets with subsets contained in them, groups also have *subgroups* as structures within themselves.

3.27 Definition (*Subgroups*)
Let G be a group. A **subgroup** of G is a subset $H \subseteq G$ that is closed under the operation of G and satisfies the group axioms itself. We write $H \leq G$ if H is a subgroup of G. If $H \leq G$ and $H \neq G$, we say H is a **proper subgroup** of G.

LaTeX TIPS
$\subseteq$ \subseteq
$\supseteq$ \supseteq
$\leq$ \leq
$\geq$ \geq
$\neq$ \neq

3.28 Example (*Trivial subgroups*)
Every non-trivial group G has at least two subgroups: the group G itself, and the trivial subgroup $H = \{e\}$.

3.29 Example
The set $2\mathbb{Z}$ of even integers is a subgroup of $\mathbb{Z}$.

Proof
First, we observe that $2\mathbb{Z}$ is closed under addition because the sum of even integers is an even integer.

- (Associativity) Addition is associative, which is inherited from $\mathbb{Z}$.
- (Identity) The additive identity 0 is in $2\mathbb{Z}$.
- (Inverse) The negation of an even integer n is still even.

We can conclude that $2\mathbb{Z} \leq \mathbb{Z}$. □

Class 6
2020/09/28

Checking all four structural properties for a subgroup can get tedious very quickly. We usually appeal to the following *one-step subgroup test* to check whether a subset of a group is a subgroup.

3.30 Theorem (*The one-step subgroup test*)
Let G be a group, and let H be a non-empty subset of G. Then $H \leq G$ if and only if $xy^{-1} \in H$ for all $x, y \in H$.

Proof
Suppose $H \leq G$. Let $x, y \in H$, then $xy^{-1} \in H$ because H is a group itself.

Now suppose that $xy^{-1} \in H$ for all $x, y \in H$. We verify the group axioms and closure on H.

LaTeX TIPS
$\varnothing$ \varnothing

- (Associativity) The operation on H is the same as the operation on G, thus inherits associativity.
- (Identity) Because $H \neq \varnothing$, there exists $x \in H$. Thus $xx^{-1} = e \in H$.
- (Inverse) Let $x \in H$. Then $ex^{-1} = x^{-1} \in H$.
- (Closure) Let $x, y \in H$. Then $y^{-1} \in H$ by the inverse axiom. Thus $x(y^{-1})^{-1} = xy \in H$.

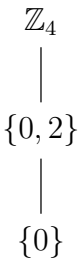
Hence, $H \leq G$. □

If two groups have the same structure, they should have the same subgroup structure as well. We can use this fact to distinguish between non-isomorphic group by showing that they have different subgroups.

3.31 Example (*Subgroups of $\mathbb{Z}_4$*)
We know that $\{0\} \leq \mathbb{Z}_4$ and $\mathbb{Z}_4 \leq \mathbb{Z}_4$. Furthermore, $\{0, 2\} \leq \mathbb{Z}_4$, as can be verified by the one-step subgroup test.

These are the only subgroups of $\mathbb{Z}_4$. If $G \leq \mathbb{Z}_4$, and if $1 \in G$, then $1+1 = 2 \in G$ by closure, and $1 + 2 = 3 \in G$ by closure, and $1 + 2 = 3 \in G$ by closure as well. So $G = \mathbb{Z}_4$. Likewise, if $3 \in G$, then $3 + 3 = 2 \in G$ by closure, and a similar argument would give $G = \mathbb{Z}_4$ as well.

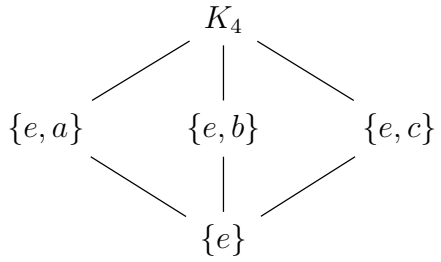
We can represent the subgroup structure of a group using a *subgroup diagram*. The subgroup diagram of $\mathbb{Z}_4$ is the following.



3.32 Example (*Subgroups of K_4*)
Recall that $K_4 = \{e, a, b, c\}$ that satisfies $c = ab$ and $a^2 = b^2 = c^2 = e$. Once again, we know $\{e\} \leq K_4$ and $K_4 \leq K_4$ as a start. Furthermore, $\{e, a\}$, $\{e, b\}$, and $\{e, c\}$ all form subgroups of V.

These are the only subgroups of K_4. If $G \leq K_4$ and if $a, b \in G$, then $ab = c \in G$ by closure, and $a^2 = e \in G$ by closure. So $G = K_4$. Likewise, if $b, c \in G$ or if $a, c \in G$, we get $G = K_4$.

The subgroup diagram of K_4 is the following.



We see from the subgroup diagrams that $\mathbb{Z}_4$ only has one subgroup of order 2, but K_4 has three subgroups of order 2. Therefore, they are not isomorphic.

4 Homomorphisms

We have been using the word "isomorphic" loosely to indicate two groups having the same overall structure. In this section, we make precise the notion of when two groups "look alike." We first define the notion of a *homomorphism*, which we will have a lot more to say about in later topics.

4.1 Definition (*Morphisms*)
Let G and H be groups. A function $\varphi\colon G \to H$ is a **homomorphism** if

$$\varphi(ab) = \varphi(a)\varphi(b)$$

for all $a, b \in G$. A homomorphism $\varphi\colon G \to H$ is an **isomorphism** if φ is also bijective. We say that G and H are **isomorphic** if there exists an isomorphism between them, and we write $G \cong H$.

A homomorphism $\varphi\colon G \to G$ of a group G with itself is an **endomorphism** of G. A bijective endomorphism of G (or, equivalently, an isomorphism of G with itself) is an **automorphism** of G.

LaTeX TIPS
$\cong$ `\cong`

4.2 Example (*Trivial homomorphism*)
For any groups G and H, there always exists the **trivial homomorphism** $\varphi\colon G \to H$ defined by $\varphi(g) = e_H$ for all $g \in G$, where e_H is the identity element in H.

Evidently, no structural information can be recovered from the trivial homomorphism. The homomorphism in the next example is less trivial, but also does not provide much information.

4.3 Example
For any group G, the identity map $\iota\colon G \to G$ defined by $\iota(g) = g$ for all $g \in G$ is an automorphism of G. This shows $G \cong G$. In fact, "being isomorphic" is an equivalence relation on any non-empty collection of groups, and the equivalence classes are called *isomorphism classes*.

The following example shows the relation between $\mathbb{Z}$ and $\mathbb{Z}_n$.

4.4 Example
Let $n \geq 1$ be an integer. Define $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$ by setting $\varphi(a)$ to be the remainder of a modulo n for all $a \in \mathbb{Z}$. This is a homomorphism. Given $a, b \in \mathbb{Z}$, let $r, s \in \mathbb{Z}_n$ be such that $a \equiv r \pmod{n}$ and $b \equiv s \pmod{n}$. Then

$$\varphi(a) +_n \varphi(b) = r +_n s = \varphi(a + b).$$

4.5 Example
A linear transformation $T\colon V \to W$ between two vector spaces V and W is a homomorphism if we consider the additive group structure of vector spaces.

The next example will show that the binary operations in Examples 1.5 and 1.22 are in fact isomorphic as groups.

4.6 Example

Class 7
2020/09/30

For any positive integer n, the integer classes $\mathbb{Z}_n$ modulo n is isomorphic to the set U_n of all n-th roots of unity.

Let $\varphi\colon \mathbb{Z}_n \to U_n$ be a map given by $\varphi(k) = e^{2\pi ik/n}$. Then

$$\varphi(k+\ell) = e^{2\pi i(k+\ell)/n} = e^{2\pi ik/n}e^{2\pi i\ell/n} = \varphi(k)\varphi(\ell).$$

Thus φ is a homomorphism. It is relatively straightforward to verify that φ is also injective and surjective.

The next lemma specifies what we mean when we say that the homomorphisms are "structural-preserving maps" between groups.

4.7 Lemma (*Identity and inverse are preserved under a homomorphism*)
If $\varphi\colon G \to H$ is a group homomorphism, then

- $\varphi(e_G) = e_H$;
- $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.

PROOF
Suppose $\varphi\colon G \to H$ is a homomorphism between the groups G and H. Then

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G).$$

By the cancellation property, we have $\varphi(e_G) = e_H$.

Let $g \in G$. Then

$$\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_H,$$

and

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H.$$

Thus $\varphi(g^{-1})$ is the inverse of $\varphi(g)$ in H. □

4.8 Remark
We will have many more examples of homomorphisms and isomorphisms throughout our discussion. One of the central topics in mathematics is to find the properties of a structure that determines its isomorphism type. Theorems of this type are referred to as *classification theorems*. For example, the statement

"any group G of order 4 is isomorphic to either $\mathbb{Z}_4$ or K_4"

is one of this kind. In this case, the defining property is that the group G is of order 4, and this property leads to the isomorphism types of $\mathbb{Z}_4$ and K_4. From this classification theorem, we know that either $\mathbb{Z}_8^* \cong \mathbb{Z}_4$ or $\mathbb{Z}_8^* \cong K_4$ without having to find explicit isomorphisms between these groups.

Generally speaking, it is difficult to determine whether two groups are isomorphic or not. Constructing an isomorphism between two arbitrary groups, or

proving no such map exists, is computationally impossible in most cases. This is like in calculus, it is almost impossible to write down a closed-form expression for the integral of an arbitrary continuous function. But it does not stop us from studying integrals, since the concept is so important and so fruitful in many fields of mathematics and physics.

4.9 Definition

Let $\varphi\colon G \to H$. The **image** of φ, denoted by $\varphi(G)$, is the set

$$\varphi(G) = \{h \in H \mid h = \varphi(g) \text{ for some } g \in G\}.$$

The **kernel** of φ, denoted by $\ker(\varphi)$, is the set

$$\ker(\varphi) = \varphi^{-1}(e_H) = \{g \in G \mid \varphi(g) = e_H\}.$$

4.10 Example

Let's consider the homomorphism $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$ in Example 4.4. The image $\varphi(G)$ is the entire group $\mathbb{Z}_n$. The kernel $\ker(\varphi) = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ is precisely the set $n\mathbb{Z}$ of integer multiples of n. This is a *surjective* homomorphism.

4.11 Example

Fix an integer n. Consider the function $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = nx$. After verifying that f is indeed a homomorphism, we see that the image $f(\mathbb{Z}) = |n|\mathbb{Z}$, and the kernel $\ker(\varphi) = \{0\}$ is trivial if $n \neq 0$.

4.12 Theorem

Let G and H be groups, and let $\varphi\colon G \to H$ be a homomorphism.

(1) $\varphi(G)$ is a subgroup of H.

(2) $\ker(\varphi)$ is a subgroup of G.

(3) φ is injective if and only if $\ker(\varphi)$ is trivial.

Proof of Part (1)

We will prove part (1) here, and leave parts (2) and (3) of this theorem as an exercise in Homework #2.

First of all, $\varphi(G) \neq \varnothing$ because $G \neq \varnothing$. We can apply the one-step subgroup test (Theorem 3.30) on $\varphi(G)$. Let $x, y \in \varphi(G)$. Then $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in G$. Thus

$$xy^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(G). \qquad \square$$

4.13 Example

If G is a group of matrices, then determinant $\det\colon G \to \mathbb{R}^*$ is a homomorphism because of the relation $\det(A)\det(B) = \det(AB)$. Let's take a look at the image and the kernel if G is one the following matrix groups:

- $G = \mathsf{GL}_n(\mathbb{R})$. The image $\det(G)$ is the whole group $\mathbb{R}^*$. In another word, the determinant is surjective. The kernel is

$$\ker(\det) = \{A \in \mathsf{GL}_n(\mathbb{R}) \mid \det(A) = 1\} = \mathsf{SL}_n(\mathbb{R}).$$

- $G = \mathsf{SL}_n(\mathbb{R})$. The image $\det(G)$ is the singleton $\{1\}$. Hence, the determinant is the trivial homomorphism on $\mathsf{SL}_n(\mathbb{R})$, and the kernel is the full domain $\mathsf{SL}_n(\mathbb{R})$.
- $G = \mathsf{O}(n)$. The image $\det(G) = \{\pm 1\}$, and the kernel

$$\ker(\det) = \{A \in \mathsf{O}(n) \mid \det(A) = 1\} =: \mathsf{SO}(n).$$

  This is called the **special orthogonal group**.

5 Cyclic Groups

5.1 Elementary properties of cyclic groups

We define a new way to construct subgroups.

5.1 Definition (*Cyclic subgroup and order of an element*)
Let G be a group, and let $a \in G$. The **cyclic subgroup of G generated by a** is the subgroup

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}.$$

If $\langle a \rangle$ is a finite group of order n, we say that the **order of a** is n, and we write $|a| = n$. If $\langle a \rangle$ an infinite group, we say that a has **infinite order**.

LaTeX TIPS
$\langle a \rangle$
`\langle a \rangle`

5.2 Remark
In the additive context, we usually write ka instead of a^k for a sequence of k copies of a under the operation of G.

Of course, we are due for a lemma that says $\langle a \rangle$ is indeed a subgroup of G.

5.3 Lemma
Let G be a group, and let $a \in G$. If $H = \langle a \rangle$, then $H \leq G$.

Proof
First, $a^0 = e \in H$, so $H \neq \varnothing$. Let $x, y \in H$. Then there exists $k, \ell \in \mathbb{Z}$ such that $x = a^k$ and $y = a^\ell$. Thus $xy^{-1} = a^k a^{-\ell} = a^{k-\ell} \in \langle a \rangle = H$. By the one-step subgroup test, $H \leq G$. □

5.4 Definition (*Cyclic groups*)
We say that an element a is a **generator** for G if $G = \langle a \rangle$. A group is **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$.

5.5 Example
The integers $\mathbb{Z}$ is generated by 1. Translating Definition 5.1 to the additive context, we get

$$\langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\} = \mathbb{Z}.$$

Further, -1 is also a generator of $\mathbb{Z}$, as

$$\langle -1 \rangle = \{k \cdot (-1) \mid k \in \mathbb{Z}\} = \mathbb{Z}.$$

If we consider an integer $n \in \mathbb{Z}$, we have

$$\langle n \rangle = \{k \cdot n \mid k \in \mathbb{Z}\} = n\mathbb{Z}.$$

5.6 Example ($\mathbb{Z}_4$ *and* K_4)
$\mathbb{Z}_4$ is cyclic with generators 1 and 3. That is, $\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle$.

Class 8
2020/10/02

K_4 is not cyclic. The subgroups $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are all proper subgroups of order 2, and $\langle e \rangle$ is trivial.

This is yet another proof that $\mathbb{Z}_4$ and K_4 are not isomorphic.

5.7 Example
For every integer $n \geq 2$, the group $\mathbb{Z}_n$ is generated by 1. When $n = 1$, the group $\mathbb{Z}_1$ is isomorphic to the trivial group, which is trivially cyclic.

At this point, we have actually exhausted all possible cyclic groups. The following *classification theorem* (cf. Remark 4.8) tells us all cyclic groups are of a few certain types.

5.8 Theorem (*Classification theorem of cyclic groups*)
Every cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$ for some $n \geq 1$.

Before attempting the proof, we mention the well-ordering principle of the natural numbers, which is very useful throughout the discussion on cyclic groups.

5.9 Theorem (*Well-ordering principle*)
Every non-empty subset of positive integers contains a smallest member.

We will use the well-ordering principle in the next few proofs.

Proof of Theorem 5.8
Let G be a cyclic group generated by a. There are only two possibilities: either $a^m = e$ for some $m \geq 1$, or $a^m \neq e$ for any $m \geq 1$.

- If $a^m = e$ for some $m \geq 1$, let $n \geq 1$ be the least number among such integers. Then $a^n = e$ and $a^k \neq e$ for all $1 \leq k \leq n-1$. Define $\varphi\colon \mathbb{Z}_n \to G$ by $\varphi(k) = a^k$ for all $k \in \mathbb{Z}_n$. We want to show that φ is an isomorphism.
  - (Injectivity) Let $k, \ell \in \mathbb{Z}_n$. Without loss of generality, let $k \geq \ell$. Assume that $\varphi(k) = \varphi(\ell)$. Then $a^k = a^\ell$. Thus $a^{k-\ell} = e$. But $0 \leq k - \ell \leq n - 1$. This means $k - \ell = 0$. Thus $k = \ell$.
  - (Surjectivity) Let $x \in G$. Then $x = a^k$ for some $k \in \mathbb{Z}$. By the division algorithm (Theorem 1.1), we can write $k = qn + r$, where $q \in \mathbb{Z}$ and $0 \leq r < n$. Thus $x = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r = \varphi(r)$.
  - (Homomorphism) let $k, \ell \in \mathbb{Z}_n$. Then
$$\varphi(k + \ell) = a^{k+\ell} = a^k a^\ell = \varphi(k)\varphi(\ell).$$
  So $G \cong \mathbb{Z}_n$ in this case.
- If $a^m \neq e$ for all $m \geq 1$, define $\varphi\colon \mathbb{Z} \to G$ by $\varphi(k) = a^k$ for all $k \in \mathbb{Z}$. We want to show that φ is an isomorphism.
  - (Injectivity) Let $k, \ell \in \mathbb{Z}$. Without loss of generality, let $k \geq \ell$. Assume that $\varphi(k) = \varphi(\ell)$. Then $a^k = a^\ell$. Thus $a^{k-\ell} = e$. But $a^m \neq e$ for all $m \geq 1$. This means $k - \ell = 0$. Thus $k = \ell$.
  - (Surjectivity) This follows directly from the definitions:
$$\varphi(\mathbb{Z}) = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle = G.$$
  - (Homomorphism) Let $k, \ell \in \mathbb{Z}$. Then
$$\varphi(k + \ell) = a^{k+\ell} = a^k a^\ell = \varphi(k)\varphi(\ell).$$

So $G \cong \mathbb{Z}$ in this case. □

5.10 Remark

Theorem 5.8 tells us all the isomorphism classes of cyclic groups. Every cyclic group is abelian. Furthermore, it tells us that two cyclic groups are isomorphic if and only if they have the same order. This justify the notation of using $\mathbb{Z}$ to represent an infinite cyclic group, and $\mathbb{Z}_n$ to represent an arbitrary cyclic group of order n.

5.11 Theorem

Every subgroup of a cyclic group is cyclic.

Proof

Let $G = \langle a \rangle$ be a cyclic group, and let $H \leq G$. If H is trivial, then $H = \langle e \rangle$ is cyclic. If H is non-trivial, then $a^m \in H$ for some positive integer m. Let $n \geq 1$ be the least number among such integers. Then $a^n \in H$ and $a^k \notin H$ for all $1 \leq k \leq n-1$. By definition, $\langle a^n \rangle \leq H$. We will show that $H \subseteq \langle a^n \rangle$ as well. Let $x \in H$. Then $x \in G$, and $x = a^\ell$ for some $\ell \in \mathbb{Z}$. By the division algorithm, we can write $\ell = qn + r$, where $q \in \mathbb{Z}$ and $0 \leq r < n$. Thus $x = a^{qn+r}$. Hence, $(a^n)^{-q}x = a^{-qn}a^{qn+r} = a^r \in H$. But $a^r \notin H$ for all $1 \leq r \leq n-1$. Therefore, $r = 0$, and $x = a^{qn} = (a^n)^q \in \langle a^n \rangle$. This shows that $H = \langle a^n \rangle$. □

5.12 Example

The subgroups of $\mathbb{Z}$ are the groups $n\mathbb{Z}$ for $n \in \mathbb{Z}$. They are cyclic with $n\mathbb{Z} = \langle n \rangle$.

Class 9
2020/10/05

We are able to say more about subgroups of finite cyclic groups with the help of some tools in number theory.

5.13 Theorem (*Generators of cyclic groups*)

$k \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if k and n are relatively prime.

Proof

We have shown in Theorem 1.11 that $k \in \mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if k and n are relatively prime. We will make use of this result.

Assume that k and n are relatively prime. Then k has a multiplicative inverse in $\mathbb{Z}_n$. That is, there exist $\ell \in \mathbb{Z}_n$ such that $\ell k = 1$ in $\mathbb{Z}_n$. Let $m \in \mathbb{Z}_n$. Then we can write $m = m(\ell k) = (m\ell)k$ in $\mathbb{Z}_n$. Regard m and ℓ as integers, it follows that any $m \in \mathbb{Z}_n$ is the sum of $m\ell$ copies of k. Hence, $\mathbb{Z}_n$ is generated by k.

Now assume that $\mathbb{Z}_n$ is generated by k. That is, for all $m \in \mathbb{Z}_n$, we have $m = \ell k$ for some $\ell \in \mathbb{Z}$. Let $m = 1$ and read this equality modulo n, we obtain $1 = \ell k$ in $\mathbb{Z}_n$. Thus k has a multiplicative inverse in $\mathbb{Z}_n$. It follows that k and n are relatively prime. □

We can rephrase Theorem 5.13 in terms of an arbitrary finite cyclic group as the following corollary.

5.14 Corollary

In a cyclic group $G = \langle a \rangle$ of order n, all generators of G are of the form a^k,

where k and n are relatively prime.

5.15 Example

Let's consider $\mathbb{Z}_{12}$ as a cyclic group of order 12. The generators of $\mathbb{Z}_{12}$ are elements in $\mathbb{Z}_{12}$ relatively prime to 12, and they are elements in

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}.$$

For instance, if we use 5 to generate a subgroup of $\mathbb{Z}_{12}$, we get

$$\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbb{Z}_{12}.$$

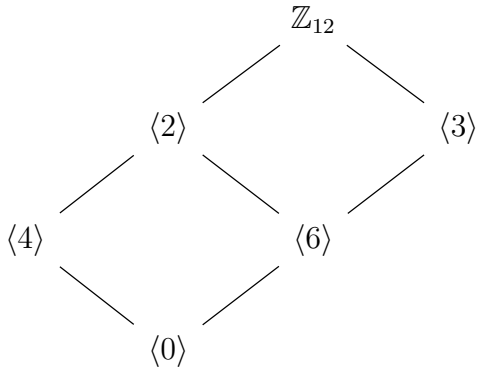
If we use 4, which is not a generator of $\mathbb{Z}_{12}$, to generate a subgroup, we get

$$\langle 4 \rangle = \{0, 4, 8\} \lneq \mathbb{Z}_{12}.$$

Notice that $\langle 4 \rangle = \langle 8 \rangle$. Using all other elements of $\mathbb{Z}_{12}$ to generate subgroups, we get three extra non-trivial subgroups of $\mathbb{Z}_{12}$:

$$\begin{aligned}
\langle 2 \rangle &= \langle 10 \rangle = \{0, 2, 4, 6, 8, 10\}, \\
\langle 3 \rangle &= \langle 9 \rangle = \{0, 3, 6, 9\}, \\
\langle 6 \rangle &= \{0, 6\}.
\end{aligned}$$

The subgroup diagram of $\mathbb{Z}_{12}$ looks like the following.



5.16 Remark

Observing the example above in detail, we notice that the order of each element, which is the order of the subgroup generated by that element, is the following

$$\begin{aligned}
|1| = |5| = |7| = |11| = |\langle 1 \rangle| &= 12, \\
|2| = |10| = |\langle 2 \rangle| &= 6, \\
|3| = |9| = |\langle 3 \rangle| &= 4, \\
|4| = |8| = |\langle 4 \rangle| &= 3, \\
|6| = |\langle 6 \rangle| &= 2, \\
|0| = |\langle 0 \rangle| &= 1.
\end{aligned}$$

All of the above satisfy that $|k| = \dfrac{12}{\gcd(k, 12)}$ (In the case of $k = 0$, every positive integer is a divisor of k). The following theorem generalizes Theorem 5.13.

5.17 Theorem (*Order of elements in a cyclic group*)
Let $k \in \mathbb{Z}_n$, and let $H = \langle \ell \rangle \leq \mathbb{Z}_n$. Then

(1) k has order $\dfrac{n}{\gcd(k,n)}$, and

(2) $H = \langle k \rangle$ if and only if $\gcd(k,n) = \gcd(\ell,n)$.

PROOF (not covered in class, non-examinable)
Omitted. □

5.2 Subgroup generated by a subset

5.18 Definition (*Subgroup generated by a subset*)
Let G be a group, and let $S \subseteq G$. The **subgroup of G generated by S**, denoted by $\langle S \rangle$ is the intersection of all subgroups of G containing S. That is,

$$\langle S \rangle = \bigcap \{H \leq G \mid S \subseteq H\}.$$

LATEX TIPS
$\cap$ \cap
$\cup$ \cup
$\bigcap$ \bigcap
$\bigcup$ \bigcup

If $\langle S \rangle = G$, we say that S is a **generating set** for G, and that the elements of S are **generators** of G. A group G is **finitely generated** if there exists a finite subset $S \subseteq G$ such that $G = \langle S \rangle$.

There are a few justifications needed for this definition. First, we must convince ourselves that the (possibly infinite) intersection in the definition is indeed a subgroup of G. Second, it had better be the case that when $S = \{a\}$ is a singleton, the definition agrees with our previous definition of a cyclic subgroup.

5.19 Lemma
Let G be a group, and let H_α be a family of subgroups of G, indexed by $\alpha \in \mathcal{A}$. Then $\bigcap_{\alpha \in \mathcal{A}} H_\alpha$ is a subgroup of G.

PROOF
The proof is essentially the same with Problem 2(a) on Homework #2. □

5.20 Lemma
Let G be a group and let $a \in G$. Then $\langle a \rangle = \bigcap \{H \leq G \mid a \in H\}$.

PROOF
The cyclic subgroup $\langle a \rangle$ itself is a subgroup of G containing a. Thus

$$\bigcap \{H \leq G \mid a \in H\} \leq \langle a \rangle.$$

On the other hand, any subgroup H of G containing a must also contain a^k for all $k \in \mathbb{Z}$. Thus

$$\langle a \rangle \leq \bigcap \{H \leq G \mid a \in H\}.$$ □

5.21 Example
Every group is trivially generated by itself. This also tells us that every finite group is finitely generated.

5.22 Example

Recall the definition of the Klein 4-group $K_4 = \{e, a, b, c\}$, where $ab = c$ and $a^2 = b^2 = c^2 = e$. We know from Example 5.6 that any single element cannot generate the entire K_4. However, we do have $K_4 = \langle\{a, b\}\rangle$, because the only subgroup of K_4 that contains both a and b is K_4 itself.

5.23 Notation

When we have an explicit enumeration of the generating set $S = \{s_1, s_2, \dots\}$, instead of $\langle\{s_1, s_2, \dots\}\rangle$, we will often write it concisely as $\langle s_1, s_2, \dots\rangle$.

The definition of a subgroup generated by a subset does not explicitly tell us whether a specific element belongs to the subset. For example, we do not know $c \in \langle a, b\rangle \leq K_4$ *unless* we know that $K_4 = \langle a, b\rangle$. In this case, the group in consideration is relatively small, hence not difficult to figure out. But this is far from generality. The following theorem characterize all the elements of $\langle S\rangle$ in terms of the generators.

5.24 Theorem

Let G be a group. If $S \subseteq G$ is a generating set for G, then every element of G is a finite product of elements in S and their inverses.

PROOF (not covered in class, non-examinable)

Assume that $G = \langle S\rangle$. Let H be the set of finite products of elements in S and their inverses. Then $H \subseteq G$ by closure of G under the group operation. By definition, $S \subseteq H$. If we can show $H \leq G$, we would be done with the proof.

To see $H \leq G$, let $x, y \in H$. Then

$$x = s_1^{\pm 1} s_2^{\pm 1} \cdots s_m^{\pm 1}, \text{ and } y = t_1^{\pm 1} t_2^{\pm 1} \cdots t_n^{\pm 1},$$

for some elements $s_i, t_j \in S$ and some choices of ± 1. Thus

$$xy^{-1} = (s_1^{\pm 1} s_2^{\pm 1} \cdots s_m^{\pm 1})(t_1^{\pm 1} t_2^{\pm 1} \cdots t_n^{\pm 1})^{-1} = s_1^{\pm 1} s_2^{\pm 1} \cdots s_m^{\pm 1} t_n^{\mp 1} \cdots t_2^{\mp 1} t_1^{\mp 1},$$

which is again a finite product of elements in S and their inverses. By the one-step subgroup test, $H \leq G$ and $S \subseteq H$. Because H is one of the subgroups in the intersection that defines $\langle S\rangle = G$, we must have $H = G$. □

5.25 Remark

In the proof of Theorem 5.24, adjacent factors s_i could be the same generator. Products of the form $ssss^{-1}sss^{-1}s^{-1}$ could be simplified s^2. This further tells us that

$$\langle S\rangle = \{s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \mid n \in \mathbb{Z}_{>0}, \text{ and } s_i \in S, k_i \in \mathbb{Z}, s_i \neq s_{i+1} \text{ for all } i.\}$$

5.26 Example

In the case where $K_4 = \langle a, b\rangle$, we can write $c = ab$ as how the generators a and b "generate" the element c under the group operation.

5.3 Dihedral groups

Class 10
2020/10/07

The idea of using a subset to generate a subgroup provides us with many interesting examples of finite groups. We will use this idea to further study *dihedral groups*.

5.27 Example
Let's consider the subgroup G of $\mathsf{GL}_2(\mathbb{R})$ generated by the matrices

$$R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

We first notice that R is the rotation matrix by $\pi/2$. Thus G must contain all powers of R, which correspond to rotations by $\pi/2$, π, $3\pi/2$, and 2π (a full rotation back to the original state), respectively. These are the matrices

$$R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, R^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, R^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \text{ and } R^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

With S being the reflection across the x-axis, $S^2 = I$, and the subgroup $\langle S \rangle = \{I, S\}$. For the subgroup $\langle R, S \rangle$, all elements are finite products of powers of R and S. This allows us to find a few more elements of G.

$$RS = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, R^2S = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ and } R^3S = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$

While we compute the products of R and S, we also notice that

$$RS = SR^3, R^2S = SR^2, \text{ and } R^3S = SR.$$

We claim that the subgroup G of $\mathsf{GL}_2(\mathbb{R})$ is the following group of order 8:

$$G = \langle R, S \rangle = \{I, R, R^2, R^3, S, RS, R^2S, R^3S\}$$

with Cayley table

	I	R	R^2	R^3	S	RS	R^2S	R^3S
I	I	R	R^2	R^3	S	RS	R^2S	R^3S
R	R	R^2	R^3	I	RS	R^2S	R^3S	S
R^2	R^2	R^3	I	R	R^2S	R^3S	S	RS
R^3	R^3	I	R	R^2	R^3S	S	RS	R^2S
S	S	R^3S	R^2S	RS	I	R^3	R^2	R
RS	RS	S	R^3S	R^2S	R	I	R^3	R^2
R^2S	R^2S	RS	S	R^3S	R^2	R	I	R^3
R^3S	R^3S	R^2S	RS	S	R^3	R^2	R	I

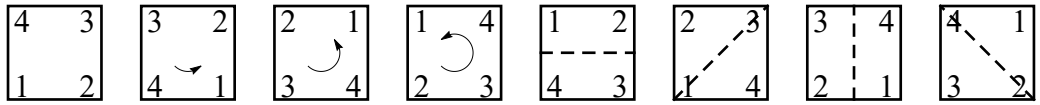
Connecting back to Section 3.1, we see that G is isomorphic to the symmetries of a square. Indeed, the matrices in G correspond to eight linear transformations that preserves the unit square centered at the origin.

5.28 Definition *(Dihedral groups)*
The **dihedral group** D_{2n} is the group of symmetries of the regular n-gon. The group is generated by a rotation r and a reflection s.

5.29 Notation
The opinion is divided among mathematicians whether to use the notations D_n or D_{2n} to represent the dihedral group of the regular n-gon. Geometers prefers D_n to emphasize the underlying n-gon, while the notation D_{2n}, where the subscript gives the order of the group, is more commonly-used in the group theory literature. We will employ the D_{2n} notation in this course.

5.30 Example
As we have discussed above, the dihedral group D_8 is the group of symmetries of a square.

$$D_8 = \langle r, s \rangle = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$$



e r r^2 r^3 s rs r^2s r^3s

5.31 Example
For the general construction of a dihedral group, fix a regular n-gon centered at the origin in the plane. Assume that one of the vertices is on the positive x-axis. Let $r \in D_{2n}$ be the counterclockwise rotation of $2\pi/n$ radian, and let $s \in D_{2n}$ be the reflection about the x-axis. Then

$$D_{2n} = \langle r, s \rangle = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

5.32 Lemma
Let $n \geq 3$ be a positive integer. Let D_{2n} be the dihedral group on a regular n-gon with generators r and s. Then

(1) $e, r, r^2, \ldots, r^{n-1}$ are all distinct, and $r^n = e$, so $|r| = n$.

(2) $|s| = 2$.

(3) $|s| \neq r^k$ for any k.

(4) $s, rs, r^2s, \ldots, r^{n-1}s$ are all distinct.

(5) $sr = r^{-1}s$.

(6) $sr^k = r^{-k}s$ for all $0 \leq k \leq n-1$.

(7) Each element in D_{2n} can be *uniquely* written in the form $r^k s^\ell$ for some $0 \leq k \leq n-1$ and $\ell \in \{0, 1\}$.

5.33 All of the statements above can be proved by realizing elements of D_{2n} as matrices in $\mathsf{GL}_2(\mathbb{R})$. That is, we can construct an injective homomorphism $\varphi\colon D_{2n} \to \mathsf{GL}_2(\mathbb{R})$ and work with the group $\varphi(D_{2n})$. You will prove some of these statements in discussion.

5.34 Example

From Theorem 5.24 and Remark 5.25, we know that every element of the dihedral group $D_{2n} = \langle r, s \rangle$ is a finite product of powers of r and s. We will see in this example how to write any such product in the form $r^k s^\ell$ for some $0 \leq k \leq n-1$ and $\ell \in \{0, 1\}$. Consider the element $x = s^7 r^3 s^{-2} r^6 s r^{-2} s^5 \in D_8$.

$$
\begin{aligned}
x &= s^7 r^3 s^{-2} r^6 s r^{-2} s^5 \\
&= s r^3 r^6 s r^{-2} s && \text{because } s^2 = e \\
&= s r^9 s r^{-2} s \\
&= s r s r^2 s && \text{because } r^4 = e \\
&= r^{-1} s s r^2 s && \text{because } sr = r^{-1} s \\
&= r^{-1} r^2 s && \text{because } s^2 = e \\
&= r s
\end{aligned}
$$

6 Symmetric Groups

We started our course by claiming that groups are algebraic structures that model *symmetries* of objects. We will make this claim more precise in this section.

A symmetry of an object can be viewed as a transformation of the object that preserves its fundamental properties. However, depending on our interpretation of the word "fundamental", we may include or exclude certain transformations from a particular discussion of symmetry.

For example, the symmetries of a square forms the dihedral group D_8, which includes all rigid motions of the square that preserves the shape of the square. In this case, the fundamental properties preserved under D_8 are shape and structural integrity. If we want to include orientation as a fundamental property of the square, we must exclude the reflections, because they do not preserve orientation. On the other hand, if we wish to relax the fundamental property of structural integrity, thus allowing deformation within the square, we are including many more transformations that preserves only the shape of the square. For the topologists in the audience, the group under consideration would become $\mathsf{Homeo}(\square)$, the homeomorphism group of the square.

The simplest object in mathematics is a set. This is the underlying object for all the algebraic structures in mathematics. We will study symmetries of sets.

6.1 Permutations

Class 11
2020/10/09

6.1 Definition *(Permutations)*
Let X be a set. A **permutation** of X is a bijective function $\pi\colon X \to X$. If X is finite, we can write $X = \{x_1, x_2, \ldots, x_n\}$, and write

$$\pi = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \pi(x_1) & \pi(x_2) & \cdots & \pi(x_n) \end{pmatrix}$$

to pair up each element in X with its corresponding image under the permutation π. We denote the set of all permutations of X by $\mathrm{Sym}(X)$ or S_X, and call it the **symmetric group** on X.

First of all, we justify the use of the term "group" on the set of all permutations.

6.2 Lemma
Let X be a set. Then $\mathrm{Sym}(X)$ is a group under function composition.

Sketch of proof
We need to check closure and the group axioms.

- Closure: the composition of two bijective functions is bijective.
- Associativity: function composition is associative.

- Identity: the identity function $\iota(x) = x$ serves as the identity.
- Inverse: bijective functions are invertible. □

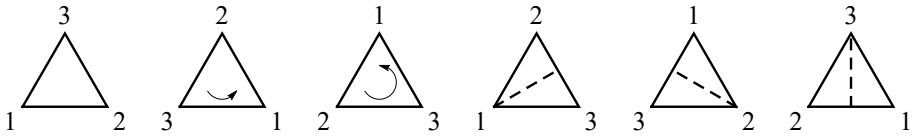
6.3 Definition (*The n-th symmetric group*)
If $X = \{1, 2, \ldots, n\}$, then $\mathrm{Sym}(X)$ is the **symmetric group on n letters**, denoted by S_n.

6.4 Example
Given $n \geq 1$, there are $n!$ permutations of the set $\{1, 2, \cdots, n\}$. Thus $|S_n| = n!$. For example, S_3 has 6 elements:

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Incidentally, S_3 is isomorphic to the dihedral group D_6 on an equilateral triangle.



While symmetric groups are interesting to study in their own right, we are also interested in subgroups of symmetric groups.

6.5 Definition (*Permutation group*)
A **permutation group** is a subgroup of $\mathrm{Sym}(X)$ for some set X.

6.6 Example
The additive group $\mathbb{Z}_n$ cyclically permutes $\{0, 1, \ldots, n-1\}$. It can be regarded as a subgroup of S_n.

6.7 Example
The dihedral group D_{2n} permutes the vertices of a regular n-gon. It can be regarded as a subgroup of S_n.

The following lemma justifies why we can regard each of the above examples as a subgroup of S_n, while their underlying sets are not exactly $\{1, 2, \ldots, n\}$.

6.8 Lemma
Let G and H be groups, and let $\varphi\colon G \to H$ be an injective homomorphism. Then $G \cong \varphi(G)$.

Proof
We have proved in Theorem 4.12 that $\varphi(G) \leq H$. Note that $\varphi\colon G \to \varphi(G)$ is bijective. It is injective by assumption and surjective by restricting the codomain to its image. Thus φ is an isomorphism onto its image, and $G \cong \varphi(G)$. □

6.9 Theorem (*Cayley's theorem*)
Every group is isomorphic to a permutation group.

PROOF
Let G be an arbitrary group. With Lemma 6.8, all we need to do is to find an injective homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$ for some appropriate choice of X.

Class 12
2020/10/12

Let $X = G$, and define $\varphi\colon G \to \mathrm{Sym}(G)$ by $\varphi(g) = \lambda_g$, where $\lambda_g\colon G \to G$ is the function of left multiplication by g given by $\lambda_g(x) = gx$. The function λ_g is bijective for all $g \in G$, because $gx = y$ has a unique solution $x \in G$ for every $y \in G$ by Lemma 3.24. Thus each λ_g is a permutation of G. We now show that φ is an injective homomorphism.

- (Homomorphism) Let $g, h \in G$. Then
$$\begin{aligned}\varphi(gh)(x) &= \lambda_{gh}(x) = (gh)x = g(hx)\\ &= \lambda_g(\lambda_h(x)) = (\lambda_g \circ \lambda_h)(x) = [\varphi(g) \circ \varphi(h)](x)\end{aligned}$$
for all $x \in G$. Thus $\varphi(gh) = \varphi(g) \circ \varphi(h)$.
- (Injectivity) If G is trivial, then φ is trivially injective. Let $g, h \in G$ be distinct. Then $\lambda_g(e) = g \neq h = \lambda_h(e)$. Thus $\lambda_g \neq \lambda_h$.

We conclude that $G \cong \varphi(G) \leq \mathrm{Sym}(G)$. □

6.10 Notation
Although permutations are functions, and the operation on permutation groups is function composition, we will omit the composition sign $\circ$ from now on and use multiplicative notation. For example, we will write $\pi\sigma$ instead of $\pi \circ \sigma$, and π^2 instead of $\pi \circ \pi$.

6.11 Example
By Cayley's Theorem, there is an injective homomorphism $\varphi\colon K_4 \to \mathrm{Sym}(K_4)$.

- $ee = e$, $ea = a$, $eb = b$, and $ec = c$, so
$$\lambda_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}.$$
- $ae = a$, $aa = e$, $ab = c$, and $ac = b$, so
$$\lambda_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}.$$
- $be = b$, $ba = c$, $bb = e$, and $bc = a$, so
$$\lambda_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}.$$
- $ce = c$, $ca = b$, $cb = a$, and $cc = e$, so
$$\lambda_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}.$$

Note that these permutations satisfy $\lambda_a^2 = \lambda_b^2 = \lambda_c^2 = \lambda_e$ and $\lambda_a\lambda_b = \lambda_c$. These are the defining properties of K_4, and thus $\varphi(K_4) \cong K_4$.

6.12 Remark

Permutations on n objects can be modeled by the *permutation matrices*, whose columns are the standard basis vectors in $\mathbb{R}^n$ in any order. This gives a homomorphism $\rho\colon S_n \to \mathsf{GL}_n(\mathbb{R})$. By Cayley's theorem, any finite group G injectively maps into some S_n through φ. The composition $\rho \circ \varphi$ yields a homomorphism from G to $\mathsf{GL}_n(\mathbb{R})$. This is an example of a *representation*, the central object of study of representation theory.

6.2 Orbits and cycles

The table notation to describe a permutation is somewhat cumbersome. Especially considering the fact that for a permutation that simply exchanges two elements, we still need to enumerate all elements of the set and their images. We would like a more efficient notation for permutations.

6.13 Definition *(Orbits)*

Let X be a set, let $\sigma \in \mathrm{Sym}(X)$, and let $a \in X$. The **orbit** of a under σ is the subset of X given by

$$\mathcal{O}_\sigma(a) = \{\sigma^k(a) \mid k \in \mathbb{Z}\}.$$

LaTeX TIPS
$\mathcal{O}$ `\mathcal{O}`

6.14 Example

Let $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 0 \end{pmatrix} \in \mathrm{Sym}(\mathbb{Z}_6)$. Then σ corresponds to the permutation by adding 1. Thus the orbit of every $k \in \mathbb{Z}_6$ is

$$\mathcal{O}_\sigma(k) = \{0, 1, 2, 3, 4, 5\}$$

6.15 Example

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix} \in S_6$. Iterating σ on $\{1, 2, 3, 4, 5, 6\}$ gives

$$\begin{aligned} \cdots &\mapsto 1 \mapsto 2 \mapsto 4 \mapsto 1 \mapsto \cdots \\ \cdots &\mapsto 3 \mapsto 6 \mapsto 3 \mapsto 6 \mapsto \cdots \\ \cdots &\mapsto 5 \mapsto 5 \mapsto 5 \mapsto 5 \mapsto \cdots \end{aligned}$$

Then we have three disjoint orbits:

$$\begin{aligned} \mathcal{O}_\sigma(1) = \mathcal{O}_\sigma(2) = \mathcal{O}_\sigma(4) &= \{1, 2, 4\}, \\ \mathcal{O}_\sigma(3) = \mathcal{O}_\sigma(6) &= \{3, 6\}, \\ \mathcal{O}_\sigma(5) &= \{5\}. \end{aligned}$$

For the remainder of this section, we will only consider permutations on the finite set $X = \{1, 2, 3, \ldots, n\}$ for some integer $n \geq 1$. Hence, the only symmetric groups of concern will be S_n.

6.16 Definition *(Cycles)*

A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the size of its largest orbit. A cycle of length k is called an **k-cycle**. Two cycles are **disjoint** if their orbits of length at least 2 are disjoint.

6.17 Notation

The identity element in S_n is the unique 1-cycle. Given a cycle $\sigma \in S_n$ of length $k \geq 2$, we write

$$\sigma = (a_1\ a_2\ \ldots\ a_k),$$

where $\{a_1, a_2, \ldots, a_k\}$ is the orbit under σ that contains k elements, and with $\sigma(a_i) = a_{i+1}$ for all $1 \leq i \leq k-1$ and $\sigma(a_k) = a_1$. This is the *cycle notation*.

6.18 Example

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \in S_4$. Then the cycle notation for σ is

$$(1\ 3\ 4) = (3\ 4\ 1) = (4\ 1\ 3).$$

LaTeX TIPS
Cycle notation:
(1 2 3) `(1 \ 2 \ 3)`

Note that (1 4 3) is not the cycle notation for σ because

$$(1\ 4\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \neq \sigma.$$

6.19 Example

We may take products of cycles to form more complicated permutations. For example, consider (1 2) and (1 3) in S_3. The product

$$(1\ 2)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2).$$

However, the product

$$(1\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3).$$

So the cycles (1 2) and (1 3) do not commute.

6.20 Example

Consider (1 2 4) and (3 6) in S_6, and their product is

Class 13
2020/10/14

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

We also see in this example that (1 2 4)(3 6) = (3 6)(1 2 4). In fact, any two disjoint cycles commute with each other.

6.21 Lemma

If $\sigma, \tau \in S_n$ are disjoint cycles, then $\sigma\tau = \tau\sigma$.

Proof

Let $\sigma, \tau \in S_n$ be disjoint cycles. Write $\sigma = (a_1\ a_2\ \dots\ a_k)$ and $\tau = (b_1\ b_2\ \dots\ b_\ell)$. Then $a_i \neq b_j$ for all choices of i and j. Let $x \in \{1, 2, \dots, n\}$. Then

- If $x \neq a_i$ and $x \neq b_j$ for any i and j, then x is unchanged under σ and τ. Thus
$$\sigma(\tau(x)) = \sigma(x) = x = \tau(x) = \tau(\sigma(x)).$$
- If $x = a_i$ for some i, then $x \neq b_j$ for any j. Thus τ fixes x, and $\sigma(x) = a_{i+1}$ (where we understand a_{k+1} to mean a_1). Hence,
$$\sigma(\tau(x)) = \sigma(x) = a_{i+1} = \tau(a_{i+1}) = \tau(\sigma(x)).$$
- Similarly, if $x = b_j$ for some j, then $\sigma(\tau(x)) = b_{j+1} = \tau(\sigma(x))$.

In any case, $\sigma(\tau(x)) = \tau(\sigma(x))$ for all x. Thus $\sigma\tau = \tau\sigma$. □

6.22 Theorem (*Cycle decomposition*)

Every permutation $\sigma \in S_n$ is a product of disjoint cycles.

Proof (not covered in class, non-examinable)

Let $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$ be orbits under σ. We first show that these orbits are disjoint. Define a relation $\sim$ on $\{1, 2, \dots, n\}$ by $a \sim b$ if $b = \sigma^\ell(a)$ for some $\ell \in \mathbb{Z}$. Informally, $a \sim b$ means a and b are in the same orbit under σ. Then

- $\sim$ is reflexive, because $a = \sigma^0(a)$ for all a.
- $\sim$ is symmetric, because if $b = \sigma^\ell(a)$ for some $\ell \in \mathbb{Z}$, then $a = \sigma^{-\ell}(b)$.
- $\sim$ is transitive, because if $b = \sigma^\ell(a)$ and $c = \sigma^m(b)$ for some $\ell, m \in \mathbb{Z}$, then $c = \sigma^m(\sigma^\ell(a)) = \sigma^{m+\ell}(a)$.

Therefore, $\sim$ is an equivalence relation, and $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$ are equivalence classes that partitions $\{1, 2, \dots, n\}$, and they must be disjoint.

Let σ_i be permutations defined by

$$\sigma_i(x) = \begin{cases} \sigma(x), & \text{if } x \in \mathcal{O}_i, \\ x, & \text{otherwise.} \end{cases}$$

Then each σ_i is a cycle, because it acts as σ on a single orbit $\mathcal{O}_i$, but it leaves all other orbits unchanged. Then we have

$$\sigma = \sigma_1\sigma_2\cdots\sigma_k,$$

with all the cycles in this product disjoint. □

6.23 Example

Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 7 & 3 & 1 & 4 & 9 & 8 & 6 \end{pmatrix} \in S_9$. The disjoint orbits under σ are

$$\cdots \mapsto 1 \mapsto 2 \mapsto 5 \mapsto 1 \mapsto \cdots$$
$$\cdots \mapsto 3 \mapsto 7 \mapsto 9 \mapsto 6 \mapsto 4 \mapsto 3 \mapsto \cdots$$
$$\cdots \mapsto 8 \mapsto 8 \mapsto \cdots$$

So we can express σ as a product of disjoint cycles as $\sigma = (1\ 2\ 5)(3\ 7\ 9\ 6\ 4)$. Note that the cycle (8) of length 1 does not appear in the product, because it is essentially the identity permutation in S_9.

6.3 Parity of permutations and the alternating groups

It is reasonable to claim that any permutation of the sequence $1, 2, \ldots, n$ can be achieved by successively exchanging a pair of numbers. A single such exchange is called a *transposition*.

6.24 Definition
In S_n, a cycle of length 2 is a **transposition**.

6.25 A transposition is a cycle written as $(a\ b)$ in cycle notation. A computation can show that cycles of any length is a product of transpositions:

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

We then have the following result as a corollary of Theorem 6.22.

6.26 Corollary
The symmetric group S_n is generated by transpositions. That is, every $\sigma = S_n$ is a finite product of transpositions.

6.27 Theorem
Let $\sigma \in S_n$. If $\sigma = \tau_1\tau_2 \ldots \tau_k$ and $\sigma = \tau_1'\tau_2' \ldots \tau_\ell'$ are two ways to write σ as products of transpositions, then k and ℓ are either both even or both odd.

PROOF (non-examinable)
Per Remark 6.12, let $\varphi\colon S_n \to \mathsf{GL}_n(\mathbb{R})$ be the homomorphism defined by letting $\varphi(\sigma) = T_\sigma$ be the linear transformation that permutes the coordinate axes according to σ. For example, if $n = 3$ and $\sigma = (1\ 2\ 3)$, then

$$T_\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \text{ and } T_\sigma \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \end{bmatrix} = \begin{bmatrix} x_{\sigma(1)} \\ x_{\sigma(2)} \\ x_{\sigma(3)} \end{bmatrix}.$$

If $\tau \in S_n$ is a transposition, then T_τ interchanges two coordinates, and the matrix of T_τ swaps two columns of the identity matrix. Thus $\det(T_\tau) = -1$. We have

$$\begin{aligned}(-1)^k &= \det(T_{\tau_1} T_{\tau_2} \cdots T_{\tau_k}) = \det(T_{\tau_1\tau_2\ldots\tau_k}) \\ &= \det(T_{\tau_1'\tau_2'\ldots\tau_\ell'}) = \det(T_{\tau_1'} T_{\tau_2'} \cdots T_{\tau_\ell}) = (-1)^\ell.\end{aligned}$$

Thus k and ℓ must be either both even or both odd. □

The following definition is made meaningful by Theorem 6.27.

6.28 Definition
A permutation $\sigma \in S_n$ is **even** if it can be expressed as a product of an even

number of transpositions, and **odd** if it can be expressed as a product of an odd number of transpositions.

6.29 Example

Recall that we can write every k-cycle as a product of $k-1$ transpositions:

$$(a_1\ a_2\ a_3\ \ldots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_4)(a_1\ a_3)(a_1\ a_2).$$

This means that a k-cycle is even if k is odd, and odd if k is even.

6.30 Algorithm

Given a permutation $\sigma \in S_n$, we can find the parity of σ through the following process.

- Write $\sigma = \sigma_1\sigma_2\ldots\sigma_m$ as a product of (not necessarily disjoint) cycles.
- Count the number of cycles of even length among $\sigma_1, \sigma_2, \ldots, \sigma_m$.
- If there are an even number of them, then σ is even; if there are an odd number of them, then σ is odd.

6.31 Example

The permutation

$$(1\ 2\ 3\ 4)(2\ 3)(5\ 6\ 7)(4\ 5\ 6\ 7\ 8)(8\ 9)$$

has three cycles of even length, so it is odd.

6.32 Example

A permutation with cycle structure

$$(*\ *\ *)(*\ *\ *\ *\ *)(*\ *\ *)$$

has no cycles of even length, so it is even.

6.33 Definition *(Alternating groups)*

If $n \geq 2$, the subgroup of S_n consisting of the even permutations is called the **alternating group on n letters**, denoted by A_n.

6.34 Lemma

$A_n \leq S_n$.

Proof

First of all, $e \in A_n$ because $e = (1\ 2)(1\ 2)$, so $A_n \neq \varnothing$. Now let $\rho, \sigma \in A_n$. Write $\rho = \tau_1\tau_2\ldots\tau_k$ and $\sigma = \tau_1'\tau_2'\ldots\tau_\ell'$, where $\tau_1, \tau_2, \ldots, \tau_k, \tau_1', \tau_2', \ldots, \tau_\ell'$ are transpositions, and k and ℓ are both even. Because transpositions are their own inverses,

$$\rho\sigma^{-1} = (\tau_1\tau_2\ldots\tau_k)(\tau_1'\tau_2'\ldots\tau_\ell')^{-1} = \tau_1\tau_2\ldots\tau_k\tau_\ell'\ldots\tau_2'\tau_1'.$$

This is a product of $k+\ell$ transpositions. Because k and ℓ are even, so is $k+\ell$. Thus $\rho\sigma^{-1} \in A_n$. By the one-step subgroup test, $A_n \leq S_n$. □

6.35 Example

For some small values of n,

- $A_2 = \{e\}$.
- $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$. The only other permutations of $\{1, 2, 3\}$ are all transpositions.
- S_4 contains elements of the following cycle structure:
  - e,
  - $(* *)$,
  - $(* * *)$,
  - $(* * * *)$,
  - $(* *)(* *)$,

  among which $(* *)$ and $(* * * *)$ give odd permutations, and e, $(* * *)$, and $(* *)(* *)$ give even permutations. Thus

$$A_4 = \{e, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2),\\ (1\ 4\ 3), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

  with a total of 12 elements.

6.36 Theorem (*Order of alternating groups*)
If $n \geq 2$, then $|A_n| = n!/2$.

PROOF
Let $B_n \subseteq S_n$ be the set of all odd permutations. Define functions $f\colon A_n \to B_n$ and $g\colon B_n \to A_n$ by $f(\sigma) = (1\ 2)\sigma$ and $g(\sigma) = (1\ 2)\sigma$. Note that both f and g changes the parity of a permutation by adding a single transposition. Further, $f(g(\sigma)) = (1\ 2)(1\ 2)\sigma = \sigma$. Similarly, $g(f(\sigma)) = (1\ 2)(1\ 2)\sigma = \sigma$. Thus f is invertible, so it is bijective, which implies that $|A_n| = |B_n|$. But $|A_n| + |B_n| = |S_n| = n!$. It follows that $|A_n| = n!/2$. □

7 Quotient Groups

Recall the Cayley table for the Klein 4-group K_4:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The Cayley table, as shaded above, is in four blocks: two of them being $\begin{matrix} e & a \\ a & e \end{matrix}$, and the other two $\begin{matrix} b & c \\ c & b \end{matrix}$. This allows us to partition K_4 into two parts: $A = \{e, a\}$ and $B = \{b, c\}$, and multiplication of elements in A and B follows the Cayley table below.

	A	B
A	A	B
B	B	A

We will see later that this is an example of a *quotient group*. But first, we observe that A is a subgroup of K_4, and every two elements in B "differ by" an element of A, in the sense that for all $x, y \in B$, there exists $z \in A$ such that $xz = y$, or equivalently, $x^{-1}y \in A$ for all $x, y \in B$. In fact, we have $B = \{bz \mid z \in A\}$. This motivates us to first discuss the notion of *cosets*.

7.1 Cosets and Lagrange's theorem

7.1 Definition (*Cosets*)
Let G be a group, and let $H \leq G$. The **left cosets** of H in G are sets of the form

$$aH = \{ax \mid x \in H\}.$$

The **right cosets** of H in G are sets of the form

$$Ha = \{xa \mid x \in H\}.$$

Note that we have $y \in aH$ if and only if $a^{-1}y \in H$, and $y \in Ha$ if and only if $ya^{-1} \in H$.

7.2 Remark
Often times, we say "coset" to mean "left coset". If we want to talk about right cosets, we will do so explicitly. For abelian groups, this does not matter, as left and right cosets coincide.

In contexts where the group operation is understood as some kind of addition, we write $a + H$ and $H + a$ for left and right cosets. But only $a + H$ is getting used, as groups in all such contexts are assumed to be abelian.

7.3 Example
Let $H = \{e, a\} \leq K_4$. The cosets of H in K_4 are

$$eH = aH = \{e, a\}, \text{ and } bH = cH = \{b, c\}.$$

7.4 Example
Consider $n\mathbb{Z}$ as a subgroup of $\mathbb{Z}$. Here we employ the additive notation. The cosets of $n\mathbb{Z}$ are those of the form

$$r + n\mathbb{Z} = \{r + nq \mid q \in \mathbb{Z}\}$$

for $r \in \mathbb{Z}$. Note that $x \in r + n\mathbb{Z}$ if and only if $x - r \in n\mathbb{Z}$, which occurs if and only if $x \equiv r \pmod{n}$. Thus the cosets of $n\mathbb{Z}$, without repetition, are

$$r + n\mathbb{Z} = \{r + nq \mid q \in \mathbb{Z}\}$$

for $r \in \mathbb{Z}_n$.

7.5 Example
Consider $A_n \leq S_n$. Then A_n itself is the coset of A_n containing every even permutation, and B_n (see proof of Theorem 6.36) is the coset of A_n containing every odd permutation.

7.6 Example
When a group is non-abelian, the left and right cosets of a particular subgroup are not necessarily all the same. For example, consider the dihedral group D_8 and its subgroup $H = \langle s \rangle = \{e, s\}$. The left and right cosets containing r are

$$rH = \{r, rs\} \text{ and } Hr = \{r, sr\},$$

respectively. Because $sr = r^{-1}s = r^3 s \neq rs$, we see $rH \neq Hr$.

7.7 Theorem (*Cosets of a group partition the group*)
Let G be a group and let $H \leq G$. The left cosets of H form a partition of G; so do the right cosets of H.

Class 15
2020/10/19

Proof
Define a relation $\sim$ on G by $a \sim b$ if $b \in aH$. Then $a \sim b$ if and only if $a^{-1}b \in H$.

- $\sim$ is reflexive, because $a^{-1}a = e \in H$ for all $a \in G$.
- $\sim$ is symmetric, because if $a^{-1}b \in H$, then $b^{-1}a = (a^{-1}b)^{-1} \in H$.
- $\sim$ is transitive, because if $a^{-1}b, b^{-1}c \in H$, then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

Thus $\sim$ is an equivalence relation. Moreover, $a \sim b$ if and only if a and b belongs to the same coset. Thus the equivalence classes of $\sim$ are precisely the left cosets of H in G. Therefore, the left cosets of H partition G.

The proof for right cosets is essentially the same, except that the equivalence relation $\sim$ is defined by $a \sim b$ if $b \in Ha$, which occurs if and only if $ba^{-1} \in H$. □

7.8 Theorem (*Lagrange's Theorem*)
Let G be a finite group, and let $H \leq G$. Then the order of H divides the order of G.

PROOF
Let $a \in G$, and define a function $f\colon H \to aH$ by $f(x) = ax$ for all $x \in H$. Note that $ax \in aH$, so f is well-defined. Further, f is bijective, because $y = ax$ has a unique solution $x \in G$ for every $y \in aH$, and if $y \in aH$, the solution $x = a^{-1}y \in H$. Therefore, $|H| = |aH|$.

By Theorem 7.7, we can write $G = a_1H \cup a_2H \cup \cdots a_kH$ as a disjoint union for some $a_1, \ldots, a_k \in G$. Thus

$$|G| = \sum_{i=1}^{k} |a_kH| = \sum_{i=1}^{k} |H| = k|H|.$$

So $|H|$ divides $|G|$, as required. □

7.9 Example
If G is a group of order 4, it does not contain any subgroup of order 3, as we have seen already with $\mathbb{Z}_4$ and K_4.

7.10 Example
Recall the alternating group A_4 with the following enumeration of elements

Class 16
2020/10/21

$$A_4 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$$
$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

The subgroups of A_4 are

- $\{e\}$,
- $\langle(1\ 2)(3\ 4)\rangle$,
- $\langle(1\ 3)(2\ 4)\rangle$,
- $\langle(1\ 4)(2\ 3)\rangle$,
- $\langle(1\ 2\ 3)\rangle$,
- $\langle(1\ 2\ 4)\rangle$,
- $\langle(1\ 3\ 4)\rangle$,
- $\langle(2\ 3\ 4)\rangle$,
- $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$,
- A_4.

We see that the orders of these subgroups are 1, 2, 3, 4, and 12, all of which divide 12. We also see that A_4 does not have a subgroup of order 6. Hence the converse of Lagrange's theorem does not hold. We *cannot* say that if k divides $|G|$, then G must have a subgroup of order k.

We now present some interesting results that following readily from Lagrange's theorem.

7.11 Corollary
The order of an element of a finite group G divides the order of G.

PROOF
The order of an element is defined to be the order of the cyclic subgroup generated by the element. The statement then follows immediately from Lagrange's theorem. □

7.12 Corollary (*Classification of groups of prime order*)
Every finite group of prime order p is isomorphic to $\mathbb{Z}_p$.

PROOF
Let G be a finite group of order p, where p is prime. In particular, $p \geq 2$, so there exists a non-identity element $a \in G \backslash \{e\}$. Then $\langle a \rangle \leq G$, and $|\langle a \rangle| \geq 2$. By Lagrange's theorem, $|\langle a \rangle|$ divides p, hence $|\langle a \rangle| = p$. Thus $G = \langle a \rangle$ is cyclic. By Theorem 5.8, we conclude that $G \cong \mathbb{Z}_p$. □

We have seen *Fermat's little theorem* in Question 5 of Homework #1. We are now ready to present it as a corollary of Corollaries 7.11 and 7.12.

7.13 Corollary (*Fermat's little theorem*)
For every integer n and every prime p, we have $n^p \equiv n \pmod{p}$.

PROOF
By the division algorithm, we first write $n = pq + r$, where $q \in \mathbb{Z}$ and $0 \leq r < p$. Then $r \in \mathbb{Z}_p$, and we only need to show $r^p = r$ in $(\mathbb{Z}_p, \cdot_p)$. If $r = 0$, the statement follows trivially. If $r \neq 0$, then $r \in \mathbb{Z}_p^*$. Note that $\mathbb{Z}_p^*$ is a group of order $p - 1$ under multiplication. Hence, the order of r in $\mathbb{Z}_p^*$ divides $p - 1$. It follows that $r^{p-1} = 1$ in $\mathbb{Z}_p^*$. Multiply both sides by r, and we get the desired result. □

7.14 Definition (*Index of a subgroup*)
Let G be a group, and let $H \leq G$. Then **index of H in G**, denoted by $[G : H]$, is the cardinality of the set of left cosets of H in G.

7.15 Remark
The index of a subgroup, as defined above, may be finite or infinite. In the case that G is finite, it is clear that

$$[G : H] = \frac{|G|}{|H|}.$$

If G is an infinite group, its subgroups may or may not have finite indices, as demonstrated by the following example.

It is also worth noting that the index of a subgroup is defined to be the cardinality of the set of left cosets. We may as well define the index of a subgroup with its right cosets, and the two definitions agree with each other, as you will show in Homework #5.

7.16 Example
Consider $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$. The cosets of H in G are precisely

$$\begin{aligned} 2\mathbb{Z} &= \{\text{all even integers}\}, \text{ and} \\ 1 + 2\mathbb{Z} &= \{\text{all odd integers}\}. \end{aligned}$$

Thus $[G : H] = 2$. Consider $K = \{0\}$. Then every singleton subset of G is a coset of K in G. Thus $[G : K] = \infty$.

7.2 Normal subgroups and quotient groups

7.17 Definition (*Normal subgroups*)
A subgroup $H \leq G$ is **normal** if $gH = Hg$ for all $g \in G$. We write $H \trianglelefteq G$ to denote a normal subgroup relation.

LaTeX TIPS
$\trianglelefteq$ \unlhd

7.18 Example
For any group G, the trivial subgroup $\{e\} \leq G$ and the group G itself are normal subgroups of G.

7.19 Example
All subgroups of an abelian group are normal. If G is abelian and $H \leq G$, then

$$gH = \{gx \mid x \in H\} = \{xg \mid x \in H\} = Ha,$$

so that $H \trianglelefteq G$.

7.20 Proposition
A subgroup of index 2 is normal.

Proof
Let G be a group, and let $H \leq G$ with $[G : H] = 2$. Then the two left cosets of H in G are precisely H and $G\backslash H$. Because cosets partition the group, and the number of right cosets equals the number of left cosets, there are two right cosets of H in G, and they are H and $G\backslash H$ as well. Further, if $g \in H$, then $gH = H = Hg$, and if $g \notin H$, then $gH = G\backslash H = Hg$. It follows that $H \trianglelefteq G$. □

Class 17
2020/10/23

7.21 Example (*Index-2 subgroups*)
Here are some examples of index-2 subgroups. Note that some of them are finite, and some are infinite.

- The alternating group A_n is an index-2 subgroup of S_n.
- The cyclic subgroup $\langle r \rangle$ is an index-2 subgroup of D_{2n}.
- $(0, \infty)$ is an index-2 subgroup of $\mathbb{R}^*$ under multiplication.
- $\mathsf{SL}_n(3)$ is an index-2 subgroup of $\mathsf{GL}_n(3)$. This is because $\mathbb{Z}_3^* = \{1, 2\}$, and $2 \cong -1 \pmod 3$, so $\mathsf{SL}_n(3)$ contains all matrices whose determinant is 1, while $\mathsf{GL}_n(3)$ contains all matrices whose determinant is ± 1.

7.22 Theorem (*Equivalent definitions of normality*)
Let G be a group, and let $H \leq G$. The following statements are equivalent.

(1) H is a normal subgroup of G.

(2) For all $g \in G$, we have $g^{-1}Hg = H$, where $g^{-1}Hg = \{g^{-1}xg \mid x \in H\}$.

(3) H is the kernel of some group homomorphism $\varphi\colon G \to G'$.

We will prove the implication (3) $\Rightarrow$ (1), and leave the rest as an exercise in Problem 2 of Homework #5.

Proof of (3) $\Rightarrow$ (1)
Let $\varphi\colon G \to G'$ be a group homomorphism. Theorem 4.12 tells us $\ker(\varphi) \leq G$. To show normality of $H = \ker(\varphi)$, let $g \in G$. and let $x \in gH$. Then $g^{-1}x \in H$. Thus

$$e = \varphi(g^{-1}x) = \varphi(g^{-1})\varphi(x) = \varphi(x)\varphi(g^{-1}) = \varphi(xg^{-1}).$$

It follows that $xg^{-1} \in H$, hence $x \in Hg$. This implies $gH \subseteq Hg$.

Likewise, we can show $Hg \subseteq gH$. Therefore, $gH = Hg$, and $H \trianglelefteq G$. □

What we just proved can be summarized as the following corollary.

7.23 Corollary
If $\varphi\colon G \to H$ is a group homomorphism, then $\ker(\varphi) \trianglelefteq G$.

Recall the definition of a group: a group is a paring of a set G together with a binary operation $*\colon G \times G \to G$ that satisfies some properties which we call the group axioms. In the following discussion, we will define a binary operation on the collection of cosets. But first of all, we will define *class functions*.

7.24 Definition (*Class functions*)
A **class function** is a function $f\colon C \to S$, where C is a collection of equivalence classes.

7.25 Remark
There is nothing special about the definition of a class function. It is as simple as it sounds–a function. However, the way we define a class function often raises concerns for "well-defined-ness", as demonstrated in the following example.

7.26 Example
Let G be a group, and let $N \trianglelefteq G$. Then we know from normality that the left and right cosets of N in G coincide. Let $\mathcal{C} = \{g_iN\}_{i\in\mathcal{I}}$ be the collection of cosets of N in G. Thus $\mathcal{C}$ is a partition of G. We will define a class function $*_N\colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ by

$$*_N(aN, bN) = (ab)N.$$

An immediate concern about this definition is that, if $a'N = aN$ and $b'N = bN$, is it guaranteed that $*_N(aN, bN) = *_N(a'N, b'N)$, or in another word, is it always the case that if $a'N = aN$ and $b'N = bN$, then $(ab)N = (a'b')N$. This turns out to be true, as we will show in the next lemma. The validity of this

claim shows that the class function $*_N$ is *well-defined*; that is, if we choose any representative from the same equivalence class as the input of the function, the outcome is independent of our choice of representative.

7.27 Lemma

Let G be a group, and let $N \trianglelefteq G$. If $x \in aN$ and $y \in bN$, then $xy \in (ab)N$

PROOF

Assume that $x \in aN$ and $y \in bN = Nb$. Then $x = an_1$ and $y = n_2 b$ for some $n_1, n_2 \in N$. Thus $xy = (an_1)(n_2 b) = a(n_1 n_2)b$. Further, $n_1 n_2 \in N$, so $(n_1 n_2)b \in Nb = bN$, and thus $(n_1 n_2)b = bn_3$ for some $n_3 \in N$. It follows that

$$xy = a(n_1 n_2)b = abn_3 \in (ab)N. \qquad \square$$

The class function $*_N$ we just verified to be well-defined gives a binary operation on the collection of cosets of N in G. In fact, $(\mathcal{C}, *_N)$ forms a group.

7.28 Definition (*Quotient groups*)

Let G be a group, and let $N \trianglelefteq G$. The **quotient** of G by N, denoted by G/N, is the group

$$G/N = \{aN \mid a \in G\}$$

with group operations defined by $(aN)(bN) = (ab)N$ for all $aN, bN \in G/N$. Such a group G/N is called a **quotient group**, or a **factor group**.

7.29 Example

We first come back to the example at the beginning of the chapter. The Cayley table of K_4 can be subdivided into four blocks.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The subgroup $A = \{e, a\}$ is normal in K_4, because K_4 is an abelian group. The cosets of A in K_4 are precisely $A = eA = aA$ and $B = bA = cA$.

7.30 Example

Consider the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$. It is a normal subgroup because $\mathbb{Z}$ is abelian. The cosets of $n\mathbb{Z}$ satisfy the relation

$$a + n\mathbb{Z} = b + n\mathbb{Z} \text{ if and only if } a \equiv b \pmod{n}.$$

The operation on the quotient group $\mathbb{Z}/n\mathbb{Z}$ works as

$$(k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) = (k + \ell) + n\mathbb{Z}.$$

We notice that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. In fact, $\mathbb{Z}/n\mathbb{Z}$ is another commonly-used notation for the isomorphism class of cyclic groups of order n.

7.31 Example

Consider the subgroup $\mathbb{Z}$ of $\mathbb{R}$. It is a normal subgroup because $\mathbb{R}$ is abelian. The cosets of $\mathbb{Z}$ satisfy the relation

Class 18
2020/10/26

$$a + \mathbb{Z} = b + \mathbb{Z} \text{ if and only if } a - b \in \mathbb{Z}.$$

The operation on the quotient group $\mathbb{R}/\mathbb{Z}$ works as

$$(a + \mathbb{Z}) + (b + \mathbb{Z}) = (a + b) + \mathbb{Z}.$$

We notice that $\mathbb{R}/\mathbb{Z} \cong [0, 1)$, where the operation on $[0, 1)$ is addition modulo 1, or taking the non-integer part by

$$x +_1 y = x + y - \lfloor x + y \rfloor.$$

We can then define a function $f : \mathbb{R}/\mathbb{Z} \to [0, 1)$ by

$$f : x + \mathbb{Z} \mapsto x - \lfloor x \rfloor.$$

First of all, f is a class function, and it is well-defined because if $a - b \in \mathbb{Z}$, then a and b have the same non-integer part, thus $f(a+\mathbb{Z}) = f(b+\mathbb{Z})$. The converse statement, where if $a - b \notin \mathbb{Z}$, then a and b have different non-integer parts, thus $f(a + \mathbb{Z}) \neq f(b + \mathbb{Z})$, shows that f is injective. For any $x \in [0, 1)$, we have $f(x + \mathbb{Z}) = x$, and thus f is surjective. Lastly, f is a homomorphism because

$$\begin{aligned} f(a + \mathbb{Z}) +_1 f(b + \mathbb{Z}) &= \begin{cases} a + b, & \text{if } a + b < 1 \\ a + b - 1, & \text{if } a + b \geq 1 \end{cases} \\ &= f(a + b + \mathbb{Z}). \end{aligned}$$

7.3 The first isomorphism theorem

We defined quotient groups in the previous section, and saw some preliminary examples of quotient groups. In this section, we will prove the very powerful *fundamental theorem of group homomorphisms*, also called *the first isomorphism theorem* in many texts, which gives isomorphism classes of quotient groups.

7.32 Example

Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. We only concern the additive group structures on the vector spaces $\mathbb{R}^n$ and $\mathbb{R}^m$. This makes T a group homomorphism. Given a vector $\boldsymbol{b} \in \mathbb{R}^m$, the following algorithm could be employed to solve $T\boldsymbol{x} = \boldsymbol{b}$ for all solutions $\boldsymbol{x} \in \mathbb{R}^n$:

- Solve the homogeneous system $T\boldsymbol{x}_h = \boldsymbol{0}$ for all homogeneous solutions $\boldsymbol{x}_h \in \mathbb{R}^n$;
- Find one particular solution $\boldsymbol{x}_p \in \mathbb{R}^n$ that satisfies $T\boldsymbol{x}_p = \boldsymbol{b}$;
- All solutions to the linear system $T\boldsymbol{x} = \boldsymbol{0}$ are of the form $\boldsymbol{x} = \boldsymbol{x}_p + \boldsymbol{x}_h$.

In group-theoretic language, $\boldsymbol{x}_h \in \ker(T)$, and all solutions to the system $T\boldsymbol{x} = \boldsymbol{b}$ forms the coset $\boldsymbol{x}_p + \ker(T)$.

Example 7.32 provides us with the intuition that given a group homomorphism $\varphi\colon G \to H$, cosets of $\ker(\varphi)$ corresponds to sets of solutions $\{x \in G \mid \varphi(x) = b\}$ for $b \in H$, and therefore with elements in the image $\varphi(G)$. The first isomorphism theorem makes this intuition precise.

7.33 Theorem (*The first isomorphism theorem of groups*)
Let G and H be groups, and let $\varphi\colon G \to H$ be a homomorphism. Then

$$G/\ker(\varphi) \cong \varphi(G).$$

Proof
Let $K = \ker(\varphi)$. Define a class function $f\colon G/K \to \varphi(G)$ by

$$f(gK) = \varphi(g) \text{ for all } gK \in G/K.$$

Then

- f is well-defined: Suppose that $aK = bK$. Then $a^{-1}b \in K$. Thus
$$e = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b).$$
This implies that $\varphi(a) = \varphi(b)$. Hence, $f(aK) = \varphi(a) = \varphi(b) = f(bK)$.
- f is injective: Suppose that $f(aK) = f(bK)$. Then $\varphi(a) = \varphi(b)$, and
$$\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) = e.$$
Thus $a^{-1}b \in \ker(\varphi) = K$. Hence, $aK = bK$.
- f is surjective: Let $h \in \varphi(G)$. Then $h = \varphi(g) = f(gK)$ for some $g \in G$.
- f is a homomorphism: for all $aK, bK \in G/K$,
$$f[(aK)(bK)] = f[(ab)K] = \varphi(ab) = \varphi(a)\varphi(b) = f(aK)f(bK).$$

We conclude that f is an isomorphism between $G/\ker(\varphi)$ and $\varphi(G)$. □

7.34 Remark
The isomorphism $f\colon gK \mapsto \varphi(g)$ defined in the proof of Theorem 7.33 is often referred to as a *canonical isomorphism*, as it is defined in a natural way.

7.35 Example
An immediate consequence of the first isomorphism theorem is that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, considering the homomorphism $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(x) = x \pmod n$. The kernel of this homomorphism is precisely $n\mathbb{Z}$, all the integer multiples of n, and this homomorphism is surjective.

7.36 Example
We may also prove $\mathbb{R}/\mathbb{Z} \cong [0, 1)$ with the first isomorphism theorem with a function $\varphi\colon \mathbb{R} \to [0, 1)$ defined by $\varphi(x) = x - \lfloor x \rfloor$, taking the non-integer part of x. The kernel of φ is $\mathbb{Z}$, and φ is surjective, hence $\mathbb{R}/\mathbb{Z} \cong [0, 1)$.

7.37 Example

If $T\colon \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation, regarded as a homomorphism between additive groups. Then $K = \ker(T) \leq \mathbb{R}^n$ is a subspace of dimension k, and $T(\mathbb{R}^n) \leq \mathbb{R}^m$ is a subspace of dimension ℓ. We can further show that the cosets in $\mathbb{R}^n/K$ form a vector space of dimension $n-k$. This fact, combined with the first isomorphism theorem of groups, gives the *rank-nullity theorem*:

$$\dim(\ker(T)) + \dim(\operatorname{im}(T)) = n.$$

7.38 Example

Consider the quotient $\mathbb{Z}_6/\langle 3\rangle$, we can construct a homomorphism $\varphi\colon \mathbb{Z}_6 \to \mathbb{Z}_6$ by defining $\varphi(k) = 2k$ for all $k \in \mathbb{Z}_6$. Then $\ker(\varphi) = \{0,3\} = \langle 3\rangle$, and the image $\varphi(\mathbb{Z}_6) = \{0,2,4\} = \langle 2\rangle \leq \mathbb{Z}_6$. Further, $2 \in \mathbb{Z}_6$ is of order 3, thus $\mathbb{Z}_6/\langle 3\rangle \cong \mathbb{Z}_3$.

7.39 Corollary

A quotient of a cyclic group is cyclic.

Proof

Let $G = \langle a\rangle$ be a cyclic group, and let $N \trianglelefteq G$ be a normal subgroup. Because all powers of a gives all elements in G, all powers of the coset aN would also give all cosets in G/N. Thus the coset aN generates the quotient G/N. □

8 Direct Product

Class 19
2020/10/28

The goal for this section is to state (and partially prove) the classification theorem of finitely generated abelian groups. The direct products of groups is an essential tools for this theorem, together with some minimal amount of number theory.

8.1 Direct product of groups

8.1 Definition *(Direct product)*
Let $G_1, G_2, \ldots, G_n$ be groups. The **direct product** of them is the group

$$\prod_{k=1}^{n} G_k = G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_k \in G_k \text{ for all } 1 \leq k \leq n\},$$

with group operation defined entry-wise

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n)$$

for all $(g_1, g_2, \ldots, g_n)$ and $(h_1, h_2, \ldots, h_n)$ in $G_1 \times G_2 \times \cdots \times G_n$.

8.2 Remark
It is a fairly straightforward exercise to check that $(e_1, e_2, \ldots, e_n)$ is the identity element of the direct product, where $e_k \in G_k$ is the identity in each group, and that the inverse of $(g_1, g_2, \ldots, g_n)$ in the direct product is $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$.

8.3 Example
The direct product $\mathbb{Z}_3 \times \mathbb{Z}_2$ contains six elements:

$$\mathbb{Z}_3 \times \mathbb{Z}_2 = \{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\}$$

Further, we notice that $\mathbb{Z}_3 \times \mathbb{Z}_2$ is cyclic, since it is generated by $(1,1)$. The "powers" (multiples in the additive context) of $(1,1)$ are

$$(0,0), (1,1), (2,0), (0,1), (1,0), (2,1)$$

in order. Thus $\mathbb{Z}_3 \times \mathbb{Z}_2 = \langle (1,1) \rangle$. Because $\mathbb{Z}_3 \times \mathbb{Z}_2$ is a group of order 6, by Theorem 5.8, we have $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$.

8.4 Example
The direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$ contains four elements:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$$

But $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic, because $(a,b) + (a,b) = (2a, 2b) = (0,0)$ for every $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$. In fact, $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong K_4$.

8.5 Example

It is worth pointing out that direct product is not the "inverse operation" of quotient on groups. For example, A_3 is a normal subgroup of S_3 with index 2. Thus $S_3/A_3 \cong \mathbb{Z}_2$. However, because $A_3 \cong \mathbb{Z}_3$, the direct product

$$A_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \ncong S_3.$$

There are a few properties of direct products of groups that are relatively straightforward to prove.

8.6 Proposition

Let G_1 and G_2 be groups. Then

(1) $G_1 \times G_2 \cong G_2 \times G_1$.

(2) If $G_3 \cong G_1$, then $G_1 \times G_2 \cong G_3 \times G_2$.

(3) If $H_1 \leq G_1$ and $H_2 \leq G_2$ are subgroups, then $H_1 \times H_2 \leq G_1 \times G_2$.

8.7 Example

Consider the direct product $\mathbb{Z}_6 \times \mathbb{Z}_6$, and consider subgroups $\langle 2 \rangle = \{0, 2, 4\} \leq \mathbb{Z}_6$ and $\langle 3 \rangle = \{0, 3\} \leq \mathbb{Z}_6$. Then

$$\langle 2 \rangle \times \langle 3 \rangle = \{(0,0), (2,0), (4,0), (0,3), (2,3), (4,3)\} \leq \mathbb{Z}_6 \times \mathbb{Z}_6.$$

However, not all subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_6$ are of the form $H_1 \times H_2$ for $H_1, H_2 \leq \mathbb{Z}_6$. For example,

$$\langle (2,2) \rangle = \{(0,0), (2,2), (4,4)\} \leq \mathbb{Z}_6 \times \mathbb{Z}_6.$$

But $\{(0,0), (2,2), (4,4)\} \neq H_1 \times H_2$ for any subsets $H_1, H_2 \leq \mathbb{Z}_6$.

8.8 Theorem (*The product of normal subgroups is normal*)

Let $G_1, G_2, \ldots, G_n$ be groups, and let $N_k \trianglelefteq G_k$ for each $1 \leq k \leq n$. Then

$$N_1 \times N_2 \times \cdots N_n \trianglelefteq G_1 \times G_2 \times \cdots G_n.$$

PROOF

We know from (inductively applying) Proposition 8.6 that

$$N_1 \times N_2 \times \cdots N_n \leq G_1 \times G_2 \times \cdots G_n.$$

Let $g_k \in G_k$ for each $1 \leq k \leq n$. Then

$$\begin{aligned}(g_1, g_2, \ldots, g_n) N_1 \times N_2 \times \cdots N_n &= g_1 N_1 \times g_2 N_2 \times \cdots \times g_n N_n \\ &= N_1 g_1 \times N_2 g_2 \times \cdots \times N_n g_n \\ &= N_1 \times N_2 \times \cdots N_n (g_1, g_2, \ldots, g_n).\end{aligned}$$

Thus $N_1 \times N_2 \times \cdots N_n$ is normal in $G_1 \times G_2 \times \cdots G_n$. □

8.9 Theorem (*The quotient by a product is a product of the quotients*)

Let $G_1, G_2, \ldots, G_n$ be groups, and let $N_k \trianglelefteq G_k$ for each $1 \leq k \leq n$. Then

Class 20
2020/10/30

$$\frac{G_1 \times G_2 \times \cdots \times G_n}{N_1 \times N_2 \times \cdots \times N_n} \cong (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_n/N_n).$$

Proof

We know from Theorem 8.8 that $N_1 \times N_2 \times \cdots \times N_n \trianglelefteq G_1 \times G_2 \times \cdots \times G_n$. Define $f\colon G_1 \times G_2 \times \cdots \times G_n \to (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_n/N_n)$ by

$$f(g_1, g_2, \ldots, g_n) = (g_1N_1, g_2N_2, \ldots, g_nN_n).$$

Evidently, f is a surjective homomorphism. Moreover, given an arbitrary $a = (a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$, we know that

$$\begin{aligned} a \in \ker(f) &\Leftrightarrow f(a) = (N_1, N_2, \ldots, N_n) \\ &\Leftrightarrow (a_1N_1, a_2N_2, \ldots, a_nN_n) = (N_1, N_2, \ldots, N_n) \\ &\Leftrightarrow a_k \in N_k \text{ for all } 1 \leq k \leq n \\ &\Leftrightarrow a \in N_1 \times N_2 \times \cdots N_n. \end{aligned}$$

This shows that $\ker(f) = N_1 \times N_2 \times \cdots N_n$. By the first isomorphism theorem (Theorem 7.33), we have achieved the desired result that

$$\frac{G_1 \times G_2 \times \cdots \times G_n}{N_1 \times N_2 \times \cdots \times N_n} \cong (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_n/N_n). \qquad \square$$

If we let $N_i = \{e_i\}$ for a single index i, and let all the other $N_k = G_k$, we obtain the following relation between direct products and quotient groups.

8.10 Corollary

Let $G_1, G_2, \ldots, G_n$ be groups, then

$$\frac{G_1 \times G_2 \times \cdots \times G_n}{G_1 \times \cdots \times G_{i-1} \times \{e_i\} \times G_{i+1} \times \cdots \times G_n} \cong G_i.$$

When $n = 2$, we have

$$G_1 \times G_2/G_1 \times \{e\} \cong G_2, \text{ and } G_1 \times G_2/\{e\} \times G_2 \cong G_1.$$

8.11 Example

By Theorem 8.9 and Example 7.35, we know that

$$\mathbb{Z}^n/(m_1\mathbb{Z} \times m_2\mathbb{Z} \times \cdots \times m_n\mathbb{Z}) \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$$

if all $m_1, m_2, \ldots, m_n \geq 1$. If some $m_i = 0$, then replace $\mathbb{Z}_{m_i}$ in the direct product with $\mathbb{Z}$. This is because $\mathbb{Z}/\{0\} \cong \mathbb{Z}$.

8.2 Finitely generated abelian groups

The classification theorem of finitely generated abelian groups is stated in terms of direct products of cyclic groups. We will state this theorem at the very beginning of this section, and prove some special cases that provides intuition. We will not provide a detailed proof of the classification of finitely generated abelian groups.

8.12 Theorem (*Classification of finitely generated abelian groups*)
Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}^k \times \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}},$$

where $k, n \geq 0$ are integers, and the $p_i^{r_i}$ are powers of primes. Moreover, the direct product is unique up to reordering the factors.

PROOF
Omitted here. □

By Theorem 8.12, every finite cyclic group $\mathbb{Z}_n$ is isomorphic to a direct product of cyclic groups, if n itself is not a prime power. The next theorem and a corollary of it tell us how to write every $\mathbb{Z}_n$ as a direct product.

8.13 Theorem
$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

PROOF
Suppose that $\gcd(m, n) = 1$. We will show that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic by showing that $(1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is a generator. The order of $(1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is the smallest positive number k of $(1, 1)$ that sums to the identity $(0, 0) \in \mathbb{Z}_m \times \mathbb{Z}_n$. In the first coordinate, $1 \in \mathbb{Z}_m$ yields $0 \in \mathbb{Z}_m$ after m summands, $2m$ summands, and so on; in the second coordinate, $1 \in \mathbb{Z}_n$ yields $0 \in \mathbb{Z}_n$ after n summands, $2n$ summands, and so on. For both coordinates to simultaneously yield 0, the number k of summands must be a multiple of both m and n. Because $\gcd(m, n) = 1$, the smallest positive integer multiple of both m and n is $k = mn$. Thus the order of $(1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is mn, and $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (1, 1) \rangle \cong \mathbb{Z}_{mn}$.

For the converse, suppose that $d = \gcd(m, n) \neq 1$. Then mn/d is a multiple of both m and n that is strictly less than mn. Thus for any $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, we have $mn/d(a, b) = (0, 0) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Hence, the order of every element in $\mathbb{Z}_m \times \mathbb{Z}_n$ is at most mn/d, and no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ generates the entire group. Therefore, $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic, thus not isomorphic to $\mathbb{Z}_{mn}$. □

8.14 Corollary
The direct product $\prod_{k=1}^{n} \mathbb{Z}_{m_k}$ is cyclic of order $\prod_{k=1}^{n} m_k$ if and only if the integers $m_1, m_2, \ldots, m_n$ are pairwise relatively prime.

Class 21
2020/11/02

PROOF
This statement can be proved by induction on n. □

8.15 Example
Every positive integer n can be written as a product of powers of distinct prime numbers. Corollary 8.14 shows that if $n = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times p_n^{r_n}.$$

As a concrete example, $\mathbb{Z}_{40} \cong \mathbb{Z}_8 \times \mathbb{Z}_5$ because $40 = 2^3 \cdot 5$.

8.16 Example

There are more than one way to find direct products of cyclic groups that are isomorphic to a given cyclic group. For example,

$$\mathbb{Z}_{60} \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_{20} \cong \mathbb{Z}_5 \times \mathbb{Z}_{12}.$$

8.17 Example

Theorem 8.13 also provides information upon whether a given direct product of two cyclic groups is cyclic. For example, $\mathbb{Z}_4 \times \mathbb{Z}_{10}$ is not cyclic, because $\gcd(4, 10) = 2 \neq 1$. But $\mathbb{Z}_4 \times \mathbb{Z}_{10}$ is also of order 40. We now have two non-isomorphic abelian groups of order 40:

$$\begin{aligned} \mathbb{Z}_{40} &\cong \mathbb{Z}_8 \times \mathbb{Z}_5, \\ \mathbb{Z}_4 \times \mathbb{Z}_{10} &\cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5. \end{aligned}$$

To find all isomorphism classes of abelian groups of order 40 (or any arbitrary finite order), we need to make use of Theorem 8.12.

First, we write $40 = 2^3 \cdot 5$. There are three different ways to break the product up into powers of prime numbers, so there are three abelian groups of order 40 *up to isomorphism*:

$$\begin{array}{rcl|l} 40 & = & 2^3 \cdot 5 & \mathbb{Z}_8 \times \mathbb{Z}_5 \\ 40 & = & 2 \cdot 2^2 \cdot 5 & \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \\ 40 & = & 2 \cdot 2 \cdot 2 \cdot 5 & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \end{array}$$

8.18 Theorem

Let G_1 and G_2 be groups. The order of $(g_1, g_2) \in G_1 \times G_2$ is the least common multiple of the order of $g_1 \in G_1$ and the order of $g_2 \in G_2$.

Proof

The proof follows a similar argument used in the proof of Theorem 8.13. □

8.19 Example

Theorem 8.18 allows us to distinguish groups of the same order by looking at the order of elements within each group. For example, consider the three abelian groups of order 40 up to isomorphism. $\mathbb{Z}_8 \times \mathbb{Z}_5$ is cyclic, thus there exists an element of order 40, which the other two do not. Further, every element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ is of order at most 10, but $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ contains an element of order 20.

8.20 Example

Consider the multiplicative abelian group $\mathbb{Z}_{15}^*$. The group is of order 8:

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Up to isomorphism, there are three abelian groups of order 8:

$$\mathbb{Z}_8, \ \mathbb{Z}_4 \times \mathbb{Z}_2, \ \text{and } \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

so $\mathbb{Z}_{15}^*$ must be isomorphic to one of them. Note that the order of each element in $\mathbb{Z}_{15}^*$ is

Element	1	2	4	7	8	11	13	14
Order	1	4	2	4	4	2	4	2

Because $\mathbb{Z}_8$ contains an element of order 8, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ contains no element of order 4, it follows that $\mathbb{Z}_{15}^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

9 Group Actions

Class 22
2020/11/04

Groups are models of symmetries of objects. We have already seen example of how groups may *act on objects* as symmetries. For example, the symmetric group S_n permutes the symbols $\{1, 2, \ldots, n\}$; the dihedral group D_{2n} rotates or reflects a regular n-gon; the general linear group $\mathsf{GL}_n(\mathbb{R})$ performs linear transformations on $\mathbb{R}^n$. In this section, we will study how groups interact with their underlying objects of symmetry through *group actions*.

9.1 Definitions and examples

9.1 Definition
Let G be a group, and let X be a set. A **left action** of G on X is a function $\alpha\colon G \times X \to X$, written as $\alpha(g, x) = gx$, such that

(1) $ex = x$ for all $x \in X$;

(2) $(g_1 g_2)x = g_1(g_2 x)$ for all $g_1, g_2 \in G$ and $x \in X$.

Under these conditions, we say that G **acts on** X, and we sometimes use the notation $G \curvearrowright X$ to denote an action of G on X. We also say X is a G**-set**.

LaTeX TIPS
↷
\curvearrowright

Likewise, the **right action** of G on X is a function $\beta\colon X \times G \to X$ defined analogously. When we say "action", we will always mean "left action".

9.2 Remark
It may be very tempting to interpret gx as the product of g and x in G. This could be a potentially dangerous intuition. As we will see in the coming examples, elements of X does not need to come from G, so the "product" is not defined by the operation of the group G, but rather from the function α that is the group action itself. Formally, the conditions in Definition 9.1 are on the function $\alpha\colon G \times X \to X$ such that

(1) $\alpha(e, x) = x$ for all $x \in X$;

(2) $\alpha(g_1 g_2, x) = \alpha(g_1, \alpha(g_2, x))$ for all $g_1, g_2 \in G$ and $x \in X$.

9.3 Example
Let X be any set, and let $H \leq \mathrm{Sym}(X)$ be a permutation group. Then X is an H-set, where the group action is defined such that $\sigma x = \sigma(x)$ for all $\sigma \in H$ and $x \in X$. This is a group action, as

(1) $ex = e(x) = x$ for all $x \in X$;

(2) $(\sigma\tau)x = (\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(\tau x)$ for all $\sigma, \tau \in H$ and $x \in X$.

9.4 Example
Let $G = D_8$, and X be the set of vertices on a square. Then X is a G-set, where the group action is defined as in Example 5.30. For example,

$$\alpha(r, 1) = 2, \text{ and } \alpha(r^2 s, 3) = 4.$$

9.5 Example

Let $G = \mathsf{GL}_n(\mathbb{R})$. Then $\mathbb{R}^n$ is a G-set with the action defined by matrix-vector multiplication. This is a group action, as

(1) $I_n \boldsymbol{x} = \boldsymbol{x}$ for all $\boldsymbol{x} \in \mathbb{R}^n$;

(2) $(AB)\boldsymbol{x} = A(B\boldsymbol{x})$ for all $A, B \in G$ and $\boldsymbol{x} \in \mathbb{R}^n$.

9.6 Example

A group G can act on itself in a couple of meaningful ways. The **left-regular action** is defined by left multiplication, such that the action $\alpha\colon G \times G \to G$ coincides with the binary operation $*\colon G \times G \to G$ of the group G. In fact, the restriction function $\alpha\colon H \times G \to G$, where $H \leq G$ is a subgroup of G, realizes G as an H-set for any subgroup H of G.

Another important action of G on itself is the **conjugation action**, defined by the action

$$\alpha(g, x) = gxg^{-1}.$$

for all $g, x \in G$. To see that this is indeed an action, note that

(1) $\alpha(e, x) = exe^{-1} = x$ for all $x \in G$;

(2) $\alpha(g_1g_2, x) = (g_1g_2)x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = \alpha(g_1, \alpha(g_2, x))$ for all $g_1, g_2, x \in G$.

9.7 Theorem

Class 23
2020/11/06

Let G be a group, and let X be a G-set. The actions of G on X correspond with homomorphisms $G \to \mathrm{Sym}(X)$. That is, the functions $\sigma_g\colon X \to X$ defined by $\sigma_g(x) = gx$ are permutations of X, and $\varphi\colon G \to \mathrm{Sym}(X)$ defined by $\varphi(g) = \sigma_g$ for all $g \in G$ is a group homomorphism.

Proof

Let $G \curvearrowright X$ be a group action. Let $g \in G$, and consider the function $\sigma_g\colon X \to X$ defined by $\sigma_g(x) = gx$ for all $x \in X$. Then

$$\sigma_{g^{-1}}(\sigma_g(x)) = \sigma_{g^{-1}}(gx) = g^{-1}(gx) = (g^{-1}g)x = ex = x.$$

for all $x \in X$. Likewise $\sigma_g(\sigma_{g^{-1}}(x)) = x$ for all $x \in X$. Thus $\sigma_{g^{-1}}$ is the inverse function of σ_g, and that makes σ_g bijective. Hence, $\sigma_g \in \mathrm{Sym}(X)$.

To show that $\varphi\colon G \to \mathrm{Sym}(X)$ defined by $\varphi(g) = \sigma_g$ for all $g \in G$ is a group homomorphism, let $g_1, g_2 \in G$. Then for all $x \in X$,

$$\begin{aligned}\varphi(g_1g_2)(x) &= \sigma_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = g_1(\sigma_{g_2}(x)) = \sigma_{g_1}(\sigma_{g_2}(x)) \\ &= (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1}\sigma_{g_2})(x) = [\varphi(g_1)\varphi(g_2)](x).\end{aligned}$$

Thus φ is a group homomorphism. □

There are a few properties that a group action may satisfy, and we give them some fancy names.

9.8 Definition (*Transitive actions*)
A group action $G \curvearrowright X$ is **transitive** if for all $x_1, x_2 \in X$, there exists $g \in G$ such that $gx_1 = x_2$.

9.9 Definition (*Faithful actions*)
A group action $G \curvearrowright X$ is **faithful** if for all $g_1 \neq g_2 \in G$, there exists $x \in X$ such that $g_1 x \neq g_2 x$.

9.10 Example
The action of S_n on $X = \{1, 2, \ldots, n\}$ is both transitive and faithful.

- (Transitivity) Given $k, \ell \in X$, if $k \neq \ell$, the transposition $(k\ \ell)$ sends k to ℓ; if $k = \ell$, the identity $e \in S_n$ would do the trick.
- (Faithfulness) If $\sigma, \tau \in S_n$ are different permutations, then they are different as bijective functions $X \to X$, and by definition, there exists $x \in X$ such that $\sigma x \neq \tau x$.

9.11 Example
The action of S_m on $X = \{1, 2, \ldots, n\}$, where $m < n$, is faithful, but not transitive. Indeed, there is no permutation $\sigma \in S_m$ that can send n to 1, because every permutation $\sigma \in S_m$ fixes $m + 1, \ldots, n$.

9.12 Example
The conjugation action of a group G on itself does not need to be transitive or faithful.

- (Not transitive) The identity element $e \in G$ cannot be mapped to any other element by a conjugation action.
- (Not faithful) As an example, in the dihegral group D_8, conjugation by r^2 results in the same action as conjugation by the identity element, because we know that r^2 commutes with every element of D_8.

9.13 Remark
Example 9.12 tells us that the conjugation action is not transitive regardless of the group G. However, the conjugation action could be faithful for some choices of the group G. For example, the conjugation action of A_3 on itself is faithful. The details will be left for you to check.

9.14 Theorem (*Alternative definition for faithfulness*)
A group action $G \curvearrowright X$ is faithful if and only if $g = e \in G$ is the only element that satisfies $gx = x$ for all $x \in X$.

Proof
The proof of this theorem is mostly juggling the definitions, which will be left as an exercise in Homework #7. □

9.15 Definition (*Free actions*)
A group action $G \curvearrowright X$ is **free** if for all $g_1 \neq g_2 \in G$, and for all $x \in X$, $g_1 x \neq g_2 x$.

9.16 Corollary
A free action on a non-empty set is faithful.

9.17 Example
The left-regular action of a group G on itself is free. Indeed, if $g_1, g_2 \in G$ are distinct, then $g_1 x \neq g_2 x$ for all $x \in G$, by the cancellation property of group operation.

9.2 Orbits and stabilizers

Class 24
2020/11/09

We have discussed orbits of an element under a permutation in Section 6.2. In this section, we are going to discuss orbits in terms of group actions.

9.18 Definition (*Orbits*)
Let G be a group, and let X be a G-set. Let $x \in X$. The **orbit** of x under the action of G is the subset of X defined by

$$\mathrm{orb}_G(x) = \{gx \mid g \in G\}.$$

That is, the orbit of x is the set of elements of X that can be obtained from x by the actions of elements in G.

9.19 Example (cf. Example 6.15)
Let $G = \langle (1\ 2\ 4)(3\ 6) \rangle \leq S_6$. Then G acts on $X = \{1, 2, 3, 4, 5, 6\}$ by permutation; that is, $\sigma k = \sigma(k)$ for each $\sigma \in G$ and each $k \in X$. In this example,

- $\mathrm{orb}_G(1) = \{1, 2, 4\} = \mathrm{orb}_G(2) = \mathrm{orb}_G(4)$;
- $\mathrm{orb}_G(3) = \{3, 6\} = \mathrm{orb}_G(6)$;
- $\mathrm{orb}_G(5) = \{5\}$.

9.20 Example
Let $G = S_n$, and consider the conjugation action of G on itself. We have seen in a previous homework assignment that all 3-cycles are in the same conjugacy class, and thus in the same orbit with $(1\ 2\ 3)$ under the conjugation action. Furthermore, it is in fact true that

$$\sigma(a_1\ a_2\ \cdots\ a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)).$$

for any $\sigma \in S_n$. If $\tau = (a_1\ \cdots\ a_k)\cdots(z_1\ \cdots\ z_\ell)$, then we have

$$\begin{aligned}\sigma\tau\sigma^{-1} &= \sigma(a_1\ \cdots\ a_k)\cdots(z_1\ \cdots\ z_\ell)\sigma^{-1} \\ &= \sigma(a_1\ \cdots\ a_k)\sigma^{-1}\cdots\sigma(z_1\ \cdots\ z_\ell)\sigma^{-1} \\ &= (\sigma(a_1)\ \cdots\ \sigma(a_k))\cdots(\sigma(z_1)\ \cdots\ \sigma(z_\ell)).\end{aligned}$$

So $\mathrm{orb}_G(\tau)$ is the set of all permutations with the same cycle structure as τ.

9.21 Lemma (*The orbits of a group action partition the set,* cf. Theorem 6.22)
Let X be a G-set. Then the orbits under the action of G partition X.

Proof
We will show that "being in the same orbit under the action of G" is an equivalence relation on X. Define a relation $\sim$ on X such that $x \sim y$ if $y = gx$ for some $g \in X$. Then

- $\sim$ is reflexive: for all $x \in X$, we have $x = ex$.
- $\sim$ is symmetric: if $y = gx$ for some $g \in G$, then

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

- $\sim$ is transitive: if $y = gx$ for some $g \in G$ and $z = hy$ for some $h \in G$, then

$$z = h(gx) = (hg)x.$$

Thus $\sim$ is an equivalence relation. Moreover, for all $x \in X$, the $\sim$-equivalence class containing x is

$$[x] = \{y \in X \mid y \sim x\} = \{gx \mid g \in G\} = \mathrm{orb}_G(x).$$

It follows that the orbits under the action of G partition X. □

9.22 Remark

Lemma 9.21 implies that, if X is a finite set being acted on by a group G, then its size $|X|$ can be computed by adding up the sizes of all the distinct orbits.

9.23 Definition *(Stablizers and fixed point sets)*

Let G be a group, and let X be a G-set. The **stabilizer** of an element $x \in X$ is a subgroup of G defined by

$$\mathrm{stab}_G(x) = \{g \in G \mid gx = x\} \leq G;$$

that is, the stabilizer of x is the set of elements of G that fix x. Stabilizers are also known as **isotropy subgroups**.

The **fixed point set** of an element $g \in G$ is a subset of X defined by

$$\mathrm{fix}_X(g) = \{x \in X \mid gx = x\} \subseteq X;$$

that is, the fixed point set of g is the set of elements of X that are fixed by g.

9.24 Remark

The notions of stabilizer and fixed point set are closely related. For all $g \in G$ and all $x \in X$, we have $g \in \mathrm{stab}_G(x)$ if and only if $x \in \mathrm{fix}_X(g)$.

9.25 Lemma

Let G be a group, and let X be a G-set. Then $\mathrm{stab}_G(x)$ is a subgroup of G for all $x \in X$.

Proof

Let $x \in X$, and let $g, h \in \mathrm{stab}_G(x)$. Then $gx = hx = x$, and thus

$$(gh^{-1})x = (gh^{-1})(hx) = (gh^{-1}h)x = gx = x.$$

It follows that $gh^{-1} \in \mathrm{stab}_G(x)$. We further know that $e \in \mathrm{stab}_G(x)$ because $ex = x$. By the one-step subgroup test, $\mathrm{stab}_G(x) \leq G$. □

9.26 Example
Consider the action of $G = \langle (1\ 2\ 4)(3\ 6) \rangle \leq S_6$ on $X = \{1, 2, 3, 4, 5, 6\}$ by permutation. Note that

$$G = \{e, (1\ 2\ 4)(3\ 6), (1\ 4\ 2), (3\ 6), (1\ 2\ 4), (1\ 4\ 2)(3\ 6)\}.$$

Then the stabilizers are

- $\mathrm{stab}_G(1) = \{e, (3\ 6)\} = \mathrm{stab}_G(2) = \mathrm{stab}_G(4)$;
- $\mathrm{stab}_G(3) = \{e, (1\ 2\ 4), (1\ 4\ 2)\} = \mathrm{stab}_G(6)$;
- $\mathrm{stab}_G(5) = G$.

The fixed-point sets are

- $\mathrm{fix}_X(e) = X$;
- $\mathrm{fix}_X((1\ 2\ 4)(3\ 6)) = \{5\} = \mathrm{fix}_X((1\ 4\ 2)(3\ 6))$;
- $\mathrm{fix}_X((1\ 2\ 4)) = \{3, 5, 6\} = \mathrm{fix}_X((1\ 4\ 2))$;
- $\mathrm{fix}_X((3\ 6)) = \{1, 2, 4, 5\}$.

9.3 Counting with group actions

Class 25
2020/11/11

We have laid enough ground for us to apply group actions in counting problems. If you pick up a standard die you purchase from the store, chances are 1 and 6 are on opposite faces, 2 and 5 are on opposite faces, and 3 and 4 are on opposite faces. There are of course other ways to label the six faces of a cube with the numbers $1, \ldots, 6$ to form a die. The goal of this section is to count the number of distinguishable ways to do so, and to solve similar problems of this type. The following two theorems will be our main tools in these counting problems.

9.27 Theorem (*Orbit-stabilizer theorem*)
Let G be a group, and let X be a G-set. Then for all $x \in X$, we have

$$|\mathrm{orb}_G(x)| = [G : \mathrm{stab}_G(x)].$$

9.28 Corollary
If G is a finite group acting on X, then $|G| = |\mathrm{orb}_G(x)| \cdot |\mathrm{stab}_G(x)|$.

9.29 Theorem (*Burnside's counting lemma*)
Let G be a finite group, and let X be a finite G-set. If r is the number of orbits in X under the action of G, then

$$r = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}_X(g)|.$$

9.30 Example (*Number of rotations of a cube*)
Let G be the group of rotations (no reflections in $\mathbb{R}^3$ allowed) that preserve the

cube. We saw in Discussion #6 that $|G| \leq 24$. We will prove in this example that $|G| = 24$.

The rotation group G acts on the faces of the cube. Let X be the set of faces of a cube, and let x be the top face. Then

- By rotating the cube in $\mathbb{R}^3$, we can move any face to any other face. So the action $G \curvearrowright X$ is transitive, and $|\text{orb}_G(x)| = |X| = 6$.
- The rotations in G that fix the top face x are the rotations about the vertical axis through the centers of the top and bottom faces. There are 4 such rotations (including the identity), thus $|\text{stab}_G(x)| = 4$.

By the orbit-stabilizer theorem, $|G| = |\text{orb}_G(x)| \cdot |\text{stab}_G(x)| = 6 \cdot 4 = 24$.

9.31 Example (*Number of distinguishable cubic dice*)
There are a total of 720 different methods to label each face of a cube. Indeed, to start the labeling process, we have 6 options for the top face, then 5 options for the bottom, 4 for the front, 3 for the back, 2 for the left, and only 1 option remaining for the right face. So the total number of labeling methods is $6! = 720$.

Let $X = \{\text{methods to label each face of a cube with } 1, \ldots, 6\}$. Then the group G of rotations of the cube acts on X. Further, two labeling methods are indistinguishable if one can be obtained by a rotation of the other, *i.e.*, if they are in the same orbit under the action of G. To count the number of distinguishable cubic dice, it is equivalent to count the number of orbits in X under the action of G.

For every non-identity element $g \in G$, the fixed point set $\text{fix}_X(g)$ is empty, because every non-trivial rotation changes any one of the 720 methods of labeling. For the identity $e \in G$, the fixed point set $\text{fix}_X(e) = X$. Thus $|\text{fix}_X(e)| = 720$, and $|\text{fix}_X(g)| = 0$ for all $g \neq e \in G$. By Burnside's counting lemma,

$$\#\text{ of orbits} = \frac{1}{|G|} \sum_{g \in G} |\text{fix}_X(g)| = \frac{1}{24} \cdot (0 + \cdots + 0 + 720) = 30.$$

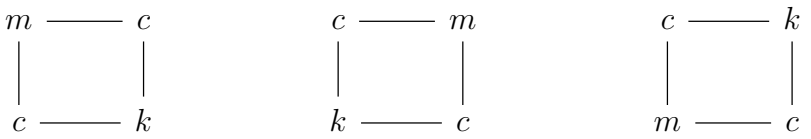
Therefore, there are 30 distinguishable cubic dice.

In the preceding example, each face is labeled by a unique number, and the numbers are not repeated when labeling the faces. A combinatorial problem becomes vastly different depending on whether *repetitions* are allowed. To reduce the computational complexity, we will present an example with squares.

9.32 Example
How many distinguishable ways can we color the vertices of a square with four colors, assuming only one color is used on each vertex, but the same color is allowed to be used on multiple vertex?

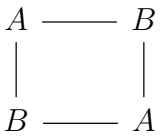
There are $4^4 = 256$ ways of coloring the vertices. Let X be the set of these 256 possible ways to color a square. Then the group D_8 acts on X. Two colorings are indistinguishable if they are in the same orbit under the action

of D_8. For example, using the colors $\{c, m, y, k\}$, the following three colorings are indistinguishable, as they can be obtained from each other by either a rotation or a reflection.

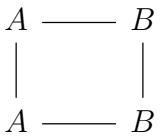


We need to find the number of disjoint orbits in X under the action of D_8. Burnside's counting lemma can help us do that, but we first need to compute the sizes of the fixed point sets.

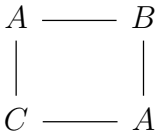
- $|\text{fix}_X(e)| = 256$: Every coloring is fixed by the identity $e \in D_8$.
- $|\text{fix}_X(r)| = 4$: To be fixed by the rotation of $\pi/2$, all vertices must be the same color, and there are 4 colors available.
- $|\text{fix}_X(r^2)| = 16$: To be fixed by the rotation of π, opposite vertices across a diagonal must be the same color, so the coloring is of the form

  where A and B are not necessarily different colors. So there are $4 \cdot 4 = 16$ different colorings.
- $|\text{fix}_X(r^3)| = 4$: Same reason as for $\text{fix}_X(r)$.
- $|\text{fix}_X(s)| = 16$: To be fixed by the reflection across the horizontal axis, the coloring must be of the form

  So there are $4 \cdot 4 = 16$ different colorings.
- $|\text{fix}_X(rs)| = 64$: To be fixed by the reflection across the diagonal (from top right to bottom left), the coloring must be of the form

  So there are $4 \cdot 4 \cdot 4 = 64$ different colorings.
- $|\text{fix}_X(r^2s)| = 16$: Similar reason as for $\text{fix}_X(s)$.

- $|\mathrm{fix}_X(r^3s)| = 64$: Similar reason as for $\mathrm{fix}_X(rs)$.

By Burnside's counting lemma,

$$\begin{aligned}\#\text{ of orbits} &= \frac{1}{|D_8|}\sum_{g\in D_8}|\mathrm{fix}_X(g)| \\ &= \frac{1}{8}\cdot(256+4+16+4+16+64+16+64) = 55.\end{aligned}$$

Class 26
2020/11/13

We shall prove the orbit-stabilizer theorem and Burnside's counting lemma here.

Proof of the Orbit-Stabilizer Theorem (Theorem 9.27)
Let $x \in X$, and let $H = \mathrm{stab}_G(x)$. Let $\mathcal{C} = \{gH \mid g \in G\}$ be the collection of left cosets of H in G. We will construct a bijection between $\mathrm{orb}_G(x)$ and $\mathcal{C}$.

Let $F\colon \mathrm{orb}_G(x) \to \mathcal{C}$ be defined by $F(gx) = gH$. There may be multiple $g_i \in G$ such that their action results g_ix are all the same, so we first need to show well-defined-ness of F.

- (F is well-defined) Let $g_1, g_2 \in G$ such that $g_1x = g_2x$. Then
$$(g_1^{-1}g_2)x = g_1^{-1}(g_2x) = g_1^{-1}(g_1x) = (g_1^{-1}g_1)x = ex = x.$$
Thus $g_1^{-1}g_2 \in \mathrm{stab}_G(x) = H$. It follows that $g_1H = g_2H$, so that
$$F(g_1x) = g_1H = g_2H = F(g_2x).$$
- (F is injective) Let $g_1x, g_2x \in \mathrm{orb}_G(x)$, and suppose that $F(g_1x) = F(g_2x)$. Then $g_1H = g_2H$ as cosets. Thus $g_1^{-1}g_2 \in H = \mathrm{stab}_G(x)$, which means $(g_1^{-1}g_2)x = x$. It follows that
$$g_1x = g_1[(g_1^{-1}g_2)x] = (g_1g_1^{-1}g_2)x = g_2x.$$
- (F is surjective) Note that for all $gH \in \mathcal{C}$, we have $F(gx) = gH$.

Hence, $F\colon \mathrm{orb}_G(x) \to \mathcal{C}$ is bijective, and $|\mathrm{orb}_G(x)| = |\mathcal{C}| = [G : \mathrm{stab}_G(x)]$. □

Proof of Burnside's Counting Lemma (Theorem 9.29)
Let $P = \{(g, x) \in G \times X \mid gx = x\}$. Thus
$$P = \bigcup_{g\in G}\{g\}\times \mathrm{fix}_X(g), \text{ and } P = \bigcup_{x\in X}\mathrm{stab}_G(x)\times\{x\}.$$
Because both unions are taken over disjoint sets, we have
$$\sum_{g\in G}|\mathrm{fix}_X(g)| = \left|\bigcup_{g\in G}\{g\}\times\mathrm{fix}_X(g)\right| = \left|\bigcup_{x\in X}\mathrm{stab}_G(x)\times\{x\}\right| = \sum_{x\in X}|\mathrm{stab}_G(x)|.$$
By the orbit-stabilizer theorem, $|\mathrm{orb}_G(x)| = [G : \mathrm{stab}_G(x)]$ for all $x \in X$. Because G is finite, we can say that
$$|\mathrm{stab}_G(x)| = \frac{|G|}{|\mathrm{orb}_G(x)|}$$

for all $x \in X$. Thus

$$\sum_{g \in G} |\mathrm{fix}_X(g)| = \sum_{x \in X} \frac{|G|}{|\mathrm{orb}_G(x)|} = |G| \cdot \sum_{x \in X} \frac{1}{|\mathrm{orb}_G(x)|}.$$

Let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be the disjoint orbits in X under the action of G. Note that for an $x \in \mathcal{O}_k$, the function $|\mathrm{orb}_G(x)| = |\mathcal{O}_k|$. Because $\mathcal{O}_1, \ldots, \mathcal{O}_r$ partition X, we have

$$\sum_{x \in X} \frac{1}{|\mathrm{orb}_G(x)|} = \sum_{k=1}^{r} \sum_{x \in \mathcal{O}_k} \frac{1}{|\mathcal{O}_k|} = \sum_{k=1}^{r} 1 = r.$$

It follows further that

$$\sum_{g \in G} |\mathrm{fix}_X(g)| = |G| \cdot r.$$

Dividing both sides by $|G|$ gives the desired result. □

10 Conjugacy Classes and Simples Groups

Class 27
2020/11/16

Just like how we factorize integers into products of primes, one of the big problems in group theory is to find a way of decomposing groups into "simple" component parts. In this task, the role of simple groups plays a similar role as that of prime numbers.

10.1 The basics

10.1 Definition
A non-trivial group G is **simple** if its only normal subgroups are $\{e\}$ and G.

We can reformulate the fundamental theorem of arithmetic as saying that, for each $n \geq 1$, there is a chain

$$1 = d_0 < d_1 < \cdots < d_r = n$$

such that d_{i+1}/d_i is prime for each i; and that any two such chains have the same length, and the primes d_{i+1}/d_i are unique up to reordering. For example, when $n = 60$, two such chains are

$$1 < 2 < 4 < 12 < 60 \quad \text{and} \quad 1 < 5 < 10 < 20 < 60$$

Although these are not the same chain, they have the same length, and the quotients d_{i+1}/d_i are $2, 2, 3, 5$ in some order.

The *Jordan–Hölder theorem* gives us an analogous result for groups. It says that for every finite group G, there is a chain of normal subgroups

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G$$

with $N_{i+1} \neq N_i$ and N_{i+1}/N_i is simple for each i; and moreover this chain is essentially unique, in the sense that any two such chains have the same length r, and the quotients N_{i+1}/N_i are unique up to some reordering.

Thus if we can understand simple groups, we're well on our way towards understanding *all* groups—kind of in the same way that if we can understand prime numbers, we're well on our way towards understanding all integers.

Finding out when a finite group is simple is therefore an important task. The finite simple groups were classified only as recently as 2004, and the proof wasn't formally verified until 2012. The proof is spread across hundreds of journal papers by dozens of authors and is tens of thousands of pages long. So we won't prove it in Math 330-1. But we can give some examples.

10.2 Example
A cyclic group $\mathbb{Z}_n$ is simple if and only if n is a prime number.

It turns out that the cyclic groups of prime order $\mathbb{Z}_p$ are the only abelian simple groups. This follows relatively quickly from the classification theorem for finite(ly generated) abelian groups (Theorem 8.12), and the fact that every subgroup of an abelian group is normal.

10.3 Example
If G has an index-2 subgroup H, then $H \trianglelefteq G$, and G is not a simple group, unless $H = \{e\}$ is the trivial subgroup, in which case $G \cong \mathbb{Z}_2$ is simple.

The smallest non-abelian simple group is A_5. We will show its simplicity in this section. Yet we need to formally introduce the notion of *conjugacy classes*, which is already familiar to us through various examples in class and in homework problems.

10.4 Definition
Let G be a group. The **conjugacy class** of an element $x \in G$, denoted by $\mathrm{Cl}(x)$, is the orbit of x under the conjugation action of G on itself. That is,

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

10.5 Example
We have seen in Example 9.20 that the conjugacy classes in $G = S_n$ are the sets of permutations in S_n with the same cycle structures. For example, S_4 has 5 conjugacy classes:

$$\begin{aligned}
\mathrm{Cl}(e) &= \{e\},\\
\mathrm{Cl}((1\ 2)) &= \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\},\\
\mathrm{Cl}((1\ 2\ 3)) &= \{(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4),\\
&\qquad (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)\},\\
\mathrm{Cl}((1\ 2\ 3\ 4)) &= \{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\},\\
\mathrm{Cl}((1\ 2)(3\ 4)) &= \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.
\end{aligned}$$

10.6 Theorem
Let G be a group, and let $H \leq G$. Then H is a normal subgroup of G if and only if H is a union of conjugacy classes in G.

Proof
This was on Homework #7. □

10.7 Example (*A_5 is simple*)
Besides the identity element, there are three possible cycle structures for permutations in A_5:

$$(*\ *\ *), (*\ *\ *\ *\ *), \text{ and } (*\ *)(*\ *)$$

However, the 5-cycles splits into two conjugacy classes in A_5, as $(1\ 2\ 3\ 4\ 5)$ and $(1\ 2\ 3\ 5\ 4)$ cannot be obtained from each other by a conjugation by an even permutation. Thus there are five conjugacy classes in A_5:

- $\mathrm{Cl}(e)$, containing the single identity element.
- $\mathrm{Cl}((1\ 2\ 3))$, containing $\binom{5}{3} \cdot 2 = 20$ elements that are 3-cycles in A_5.
- $\mathrm{Cl}((1\ 2)(3\ 4))$, containing $\binom{5}{2}\binom{3}{2}/2 = 15$ double 2-cycles in A_5.
- $\mathrm{Cl}((1\ 2\ 3\ 4\ 5))$, containing $4!/2 = 12$ elements that are 5-cycles in A_5.
- $\mathrm{Cl}((1\ 2\ 3\ 5\ 4))$, containing the other 12 elements that are 5-cycles.

Now let's assume that $N \trianglelefteq A_5$ is a normal subgroup. Lagrange's theorem asserts that the only possible orders for N as a subgroup of A_5 are the divisors of 60:

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.$$

On the other hand, N is a disjoint union of conjugacy classes. This must include $\mathrm{Cl}(e)$ because $e \in N$. Thus $|N| = 1 + k$, where k is a sum of the sizes of some of the other four conjugacy classes in A_5. The possible values of k are

$$0, 12, 15, 20, 24, 27, 32, 35, 39, 44, 47, 59.$$

Among these values, the only possible k that make $1+k$ a divisor of 60 are $k = 0$ and $k = 59$. They corresponds to the trivial subgroups $\{e\}$ and A_5, respectively. So A_5 is simple.

10.8 Lemma

Let G be a group. The subgroup of G generated by the conjugacy class $\mathrm{Cl}(x)$ is normal for every $x \in G$.

Class 28
11/18/2020

This lemma is extremely useful in determining the simplicity of groups. We will present an outline of the proof, and leave the details as an exercise in Homework #8.

Idea of proof

Let $x \in G$. We want to show that $g\langle \mathrm{Cl}(x)\rangle g^{-1} = \langle \mathrm{Cl}(x)\rangle$ for all $g \in G$.

Let $h \in \langle \mathrm{Cl}(x)\rangle$. Then h is a finite product of elements of the form $g_k x g_k^{-1}$.

- If we can show ghg^{-1} is also a finite product of elements of the form $g_k x g_k^{-1}$, we are done with $g\langle \mathrm{Cl}(x)\rangle g^{-1} \subseteq \langle \mathrm{Cl}(x)\rangle$.
- If we can show $h = gh_0g^{-1}$, where h_0 is a finite product of elements of the form $g_k x g_k^{-1}$, we are done with $\langle \mathrm{Cl}(x)\rangle \subseteq g\langle \mathrm{Cl}(x)\rangle g^{-1}$. □

Topics after this line are non-examinable.

10.2 Solvability and simple groups

We have seen a family of simple groups in the previous section – every cyclic group of prime order is simple. These are the only abelian simple groups. There

are many non-abelian simple groups as well. For example, A_5 is the smallest non-abelian simple group with order 60. In fact, the alternating groups form another family of simple groups.

10.9 Theorem
The alternating group A_n is simple for $n \geq 5$.

Proof
The proof of this theorem is the content of the last discussion session of the course. □

This theorem tells us that the next alternating group A_6, a group of order 360, is simple. In fact, there is a non-abelian simple group in between A_5 and A_5 in terms of size. The *projective special linear group* of dimension 2 over $\mathbb{Z}_7$, denoted by $\mathsf{PSL}_2(7)$, is a simple group of order 168.

Besides cyclic groups of prime order and alternating groups, there are 16 additional infinite families of finite simple groups. In addition to these families of simple groups, there are 26 *sporadic groups*. The classification of all finite simple groups was only very recently completed. Two of the many milestones in the classification process relates to the superstar in the preceding chapter – William Burnside.

10.10 Theorem (*Burnside's theorem, 1904*)
If G is a finite group of order $p^m q^n$, where p and q are primes, and m and n are non-negative integers, then G is solvable.

10.11 Theorem (*Feit-Thompson theorem, 1963, first conjectured by Burnside*)
Every finite group of odd order is solvable.

Both theorems concerns the notion of *solvability*.

10.12 Definition (*Subnormal series and solvable groups*)
Let G be a group. A **subnormal series** of G is a finite sequence of subgroups H_k of G such that

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G.$$

A group is **solvable** if it has a subnormal series such that every quotient H_k/H_{k-1} is abelian.

The next corollary almost follows immediately from the definition.

10.13 Corollary
A solvable group of non-prime order is not simple.

Now we can appreciate how powerful Theorem 10.11 is: it tells us that a non-abelian simple group must have an odd order. The entire proof filled an entire issue of a journal, 255 pages in all. The methods introduced in Feit-Thompson proof were generalized and improved with great success by many mathematicians in the 1960s working towards a complete classification of finite simple groups.

Thompson received a Fields medal for his fundamental contributions to simple group theory in 1970.

In 1972, Daniel Gorenstein proposed a program (Gorenstein's program) for completing the classification of finite simple groups, consisting of 16 steps, which he delivered in a series of lectures at the University of Chicago. Soon after that, most mathematicians involved believed that enough techniques had been developed to complete the classification.

In 1982, Robert Griess constructed "the moster group M", which is the largest sporadic simple group. Its order is a whopping

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

approximately 8×10^{53}! It is a group is of rotations in $196,883$ dimensions. Thus, each element can be expressed as a $196,883 \times 196,883$ matrix.