Groups and Rings

PMATH 347

William Slofstra

LaTeXed by *Sibelius Peng*

Preface

Disclaimer Much of the information on this set of notes is transcribed directly/indirectly from the lectures of PMATH 347 during Spring 2020 as well as other related resources. I do not make any warranties about the completeness, reliability and accuracy of this set of notes. Use at your own risk.

Spring 2020 classes online only. So the grading scheme:

- Participation: 4%
- Quizzes: 32%
- Written homework: 32%
- Final takehome exam: 32%

For any questions, send me an email via `https://notes.sibeliusp.com/contact/`.

You can find my notes for other courses on `https://notes.sibeliusp.com/`.

Sibelius Peng

Contents

1

Groups

1.1 Binary Operations

If we randomly ask someone on the street: *What's math about?* The answer we might get is **numbers**. It always comes with **operations**.

Objects	Operations
Natural numbers $\mathbb{N}$	addition $+$ subtraction $-$ multiplication $\cdot$ division with remainders
Integers $\mathbb{Z}$	negation $x \mapsto -x$
Rational number $\mathbb{Q}$	multiplicative inversion $x \mapsto 1/x$
Real numbers $\mathbb{R}$	kth roots, etc
$\mathbb{Z}/n\mathbb{Z}$	modular arithmetic and operations

Then we realizd that math is not just about numbers. We later have **elementary algebra**:

Objects	Operations
Expressions with variables	operations with variables
Functions	Pointwise operations $+, -, \cdot$ and Composition $\circ$

Then ..., and (leaving lots of stuff out), we have **linear algebra**:

Objects	Operations
Vectors	Vector addition $+$, scalar multiplication $\cdot$
Matrices	$+, -,$ scalar and matrix multiplication $\cdot$

Then *what's algebra about?*

Pre-university answer:

- manipulating expr involving indeterminates (variables):

If $a, b \in \mathbb{R}$, $ax = b$ and $a \neq 0$, then $x = \frac{b}{a}$.

- solving eqs by applying ops to both sides:
  If A, B are matrices, $AX = B$ and A is invertible, then $X = A^{-1}B$.

Key idea: algebra is about operations

Then *what operations should we study?* Polynomials in several vars; functions, pointwise ops and function composition... *Are there other operations we should study?* Then we introduce **abstract algebra**: try to answer this question by studying operations abstractly, and seeing what the possibilities are.

binary operation

A binary operation on a set X is a function $b : X \times X \to X$.

Notation:

- Any letter (b, m) or symbol $(+, \cdot)$
- function notation
  $$b : X \times X \to X : (x, y) \mapsto b(x, y)$$
  or inline notation
  $$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (x, y) \mapsto x + y$$
  Typically use inline notation with symbols and function notation with letters.
- There are lots of symbols to choose from: $a + b, a \times b, a \cdot b, a \circ b, a \oplus b, a \otimes b, a \odot b, a \diamond b, a \Diamond b, a \blacklozenge b, a * b, a \bullet b, a \boxplus b, a \boxtimes b, a \uplus b$
- If there's no chance of confusion, can even drop symbol completely:
  $$X \times X \to X : (a, b) \mapsto ab$$

Example:

- Addition $+$ is a binary op on $\mathbb{B}$, but subtraction $-$ is not, since $a - b$ is not necessarily a natural number.
- Subtraction $=$ is a binary op on $\mathbb{Z}$.
- If $(V, +, \cdot)$ is a vector space over a field $\mathbb{K}$, then $+$ is a binary op on V, but $\cdot$ is not, since $\cdot$ is a function $\mathbb{K} \times V \to V$.[a]

[a]We'll define fields later, now think of $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$.

k-ary operation

A k-ary operation on a set X is a function

$$\underbrace{X \times X \times \cdots X}_{k \text{ times}} \to X$$

A 1-ary operation is called a unary operation.

Example:
Negation $\mathbb{Z} \to \mathbb{Z} : x \mapsto -x$ is a unary operation.

Taking the multiplicative inverse $x \mapsto 1/x$ is not a unary operation on $\mathbb{Q}$, since $1/0$ is not defined, but it is a unary operation on

$$\mathbb{Q}^{\times} := \{a \in \mathbb{Q} : a \neq 0\}$$

Now let's discuss some properties that binary ops might satisfy.

1.2 Associativity and commutativity

associative

A binary operation $\boxtimes : X \times X \to X$ is associative if

$$a \boxtimes (b \boxtimes c) = (a \boxtimes b) \boxtimes c$$

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

Many operations we've mentioned so far are associative:

- Addition and multiplication for $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, polynomials, and functions
- Vector addition, matrix addition and multiplication
- Modular addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$
- Function composition

Note that Subtraction and division are not associative. Subtraction is adding negative numbers, same for division. So we aren't that interested in subtraction and division, and focus on associative operations.

Here we introduce an informal definition: A **bracketing** of a sequence $a_1, \ldots, a_n \in X$ is a way of inserting brackets into $a_1 \boxtimes \ldots \boxtimes a_n$ so that the expression can be evaluated.

Example:
The bracketings of $a_1, \ldots, a_4$ are

$$a_1 \boxtimes (a_2 \boxtimes (a_3 \boxtimes a_4))$$
$$a_1 \boxtimes ((a_2 \boxtimes a_3) \boxtimes a_4)$$

$$(a_1 \boxtimes a_2) \boxtimes (a_3 \boxtimes a_4)$$
$$(a_1 \boxtimes (a_2 \boxtimes a_3) \boxtimes a_4)$$
$$((a_1 \boxtimes a_2) \boxtimes a_3) \boxtimes a_4$$

Proposition 1.1

A binary operation $\boxtimes : X \times X \to X$ is associative if and only if for all finite sequences $a_1, \ldots, a_n \in X, n \geq 1$, every bracketing of $a_1, \ldots, a_n$ evaluated to the same element of X.

Note
If $\boxtimes$ is associative, can use notation $a_1 \boxtimes a_2 \boxtimes \ldots \boxtimes a_n$ without choosing a bracketing.

Proof:

$\Leftarrow$ The two bracketings $a \boxtimes (b \boxtimes c)$ and $(a \boxtimes b) \boxtimes c$ of a, b, c evaluate to the same element of X for all sequences of length 3.

$\Rightarrow$ Proof is by induction. Base cases are $n = 1, 2, 3$.

For $n = 1, 2$, there's only one bracketing. For $n = 3$ follows from defn of associativity.

Suppose prop is true for all sequences of length k, $1 \leq k < n$.

Let w be a bracketing of $a_1, \ldots, a_n$.

$w = w_1 \boxtimes w_2$ where w_1 is a bracketing of $a_1, \ldots, a_k$, w_2 is a bracketing of $a_{k+1}, \ldots, a_n$, for some $k < n$.

By induction,

$$w_1 = (\cdots((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \quad \text{and} \quad w_2 = (a_{k+1} \boxtimes \cdots (a_{n-1} \boxtimes a_n) \cdots)$$

Therefore

$$\begin{aligned} w &= (\cdots((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \boxtimes w_2 = (a_{k+1} \boxtimes \cdots (a_{n-1} \boxtimes a_n) \cdots) \\ &= (\cdots(a_1 \boxtimes a_2) \cdots \boxtimes a_{k-1}) \boxtimes (a_k \boxtimes (a_{k+1} \boxtimes \cdots a_n) \cdots) \\ &= \cdots \\ &= (a_1 \boxtimes (a_2 \boxtimes \cdots (a_n \boxtimes a_n) \cdots)) \end{aligned}$$

$\square$

commutative

A binary operation $\boxtimes : X \times X \to X$ is commutative (also known as abelian) if $a \boxtimes b = b \boxtimes a$ for all $a, b \in X$.

Fact The word "abelian" comes from the surname of Niels Henrik Abel (1802-1829).

Many familiar operations are commutative: addition and multiplication on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; vector and matrix addition; modular addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$. The following operation are **not** commutative: subtraction and division; function composition; matrix multiplication.

Therefore, subtraction and division are not commutative or associative. Function composition and matrix multiplication are not commutative, but are associative. We are not going to worry about the first type of operation, but we are interested in operations of the second type.

First half of the course: group theory – single associative operation, not necessarily commutative.

Second half of the course: ring theory – two associative operations (like addition and multiplication on $\mathbb{Z}$), focus on commutative case.

1.3 Identities and inverses

Let $\boxtimes$ be a binary operation on a set X.

identity

An element $e \in X$ is an identity for $\boxtimes$ if

$$e \boxtimes x = x \boxtimes e = x$$

for all $x \in X$.

Example:
The zero element 0 of $\mathbb{Z}$ is an identity for $+$. $1 \in \mathbb{Q}$ is identity for $\cdot$. $0 \in \mathbb{Q}$ is not identity for $\cdot$

Lemma 1.2

If $e, e' \in X$ are both identities for $\boxtimes$, then $e = e'$.

Proof:
$e = e \boxtimes e' = e'$ $\square$

inverse

Let $\boxtimes$ be a binary operation on X with identity element e. An element y is a left inverse for x (w.r.t. $\boxtimes$) if $y \boxtimes x = e$, a right inverse if $x \boxtimes y = e$, and an inverse if $x \boxtimes y = y \boxtimes x = e$.

Example:
$-n$ is an inverse for $n \in \mathbb{Z}$ w.r.t. $+$.

$n \in \mathbb{Z}$ does not have an inverse w.r.t. $\cdot$ unless $n = \pm 1$.

If $x \in \mathbb{Q}$ is non-zero, then $1/x$ is an inverse of x w.r.t. $\cdot$. The element 0 does not have an inverse.

Lemma 1.3

Let $\boxtimes$ be an **associative** binary op with an identity e. If y_L and y_R are left and right inverse of x respectively, then $y_L = y_R$.

Proof:
$y_L = y_L \boxtimes e = y_L \boxtimes (x \boxtimes y_R) = (y_L \boxtimes x) \boxtimes y_R = e \boxtimes y_R = y_R$ □

Corollary 1.4

- If x has both a left and right inverse, then x has an inverse.
- Inverses are unique.

invertible

An element a is invertible if it has an inverse, in which case the inverse is denoted by a^{-1}.

Exercise
It's possible to have a left (resp. right inverse), but not be invertible. Also, left and right inverses don't have to be unique (unless an element has both).

Lemma 1.5

1. If $\boxtimes$ has an identity e, then e is invertible, and $e^{-1} = e$.
2. If a is invertible, then so is a^{-1}, and $(a^{-1})^{-1} = a$.
3. If $\boxtimes$ is associative, and a and b are invertible, then so is $a \boxtimes b$, and $(a \boxtimes b)^{-1} = b^{-1} \boxtimes a^{-1}$.

Proof:

1. $e \boxtimes e = e$
2. $a \boxtimes a^{-1} = a^{-1} \boxtimes a = e$, so a is clearly an inverse to a^{-1}.
3. $(a \boxtimes b) \boxtimes (b^{-1} \boxtimes a^{-1}) = a \boxtimes (b \boxtimes b^{-1}) \boxtimes a^{-1} = a \boxtimes e \boxtimes a^{-1} = a \boxtimes a^{-1} = e$, and similarly $(b^{-1} \boxtimes a^{-1}) \boxtimes (a \boxtimes b) = e$.

□

Proposition 1.6

Let $\boxtimes$ be an associative binary operation on X with identity e, and let x and $y$be variables taking values in X.

An element $a \in X$ is invertible if and only if the equations

$$a \boxtimes x = b \text{ and } y \boxtimes a = b$$

have unique solutions for all $b \in X$.

Proof:

$\Leftarrow$ A solution to $ax = e$ is a right inverse of a, and a solution to $ya = b$ is a left inverse. If a both have a left and right inverse, then it has an inverse.

$\Rightarrow$ Suppose a is invertible. Then

$$a \boxtimes (a^{-1}b) = (a \boxtimes a^{-1}) \boxtimes b = e \boxtimes b = b$$

so $a^{-1} \boxtimes b$ is a solution to $a \boxtimes x = b$.

If x_0 is a solution to $a \boxtimes x = b$, then

$$a^{-1} \boxtimes b = a^{-1} \boxtimes (a \boxtimes x_0) = (a^{-1} \boxtimes a) \boxtimes x_0 = e \boxtimes x_0 = x_0$$

So $a^{-1} \boxtimes b$ is the unique solution to $a \boxtimes x = b$.

Similarly $b \boxtimes a^{-1}$ is the unique solution to $y \boxtimes a = b$.

$\square$

Proposition 1.7: Cancellation property

Let $\boxtimes$ be an associative binary operation, and $a \in X$. Then

1. If a has a left inverse and $a \boxtimes u = a \boxtimes v$, then $u = v$.
2. If b has a right inverse and $u \boxtimes a = v \boxtimes a$, then $u = v$.

Proof:

1. $u = a^{-1} \boxtimes a \boxtimes u = a^{-1} \boxtimes a \boxtimes v = v$
2. similar.

$\square$

1 and 2 also hold for $n \in \mathbb{Z}$ w.r.t. $\cdot$ if $n \geq 0$, even though n is not invertible for $n \neq \pm 1$.

1.4 Groups

group, finite, order

A **group** is a pair $(G, \boxtimes)$, where

1. G is a set, and
2. $\boxtimes$ is an associative binary operation on G such that
   (a) $\boxtimes$ has an identity e, and
   (b) every element $g \in G$ is invertible with respect to $\boxtimes$.

A group is **abelian** (or commutative) if $\boxtimes$ is abelian.

A group is **finite** if G is a finite set. The **order** of G the number of elements in G if G is finite, and $+\infty$ if G is infinite.

The order of G is denoted by $|G|$.

1.4.1 Terminology

Usually we refer to $(G, \boxtimes)$ simply as G, and just assume the operation is given. (Note: we still need to clearly specify the operation for each group we work with).

It's cumbersome to write $\boxtimes$ all the time, so usually we use one of the following options:

- Use $\cdot$ as the standard symbol, write $g \cdot h$ for the product of $g, h \in G$
- Drop the symbol entirely, write gh for the product of $g, h \in G$.

The identity of G is denoted by e (or e_G when we want to make the group clear). 1 and 1_G are also used.

Since every element of a group G is invertible, g^{-1} is defined for all $g \in G$. The function $G \to G : G \mapsto g^{-1}$ can be regarded as a unary operation on G.

Consider $\iota : G \to G : g \mapsto g^{-1}$. Since $(g^{-1})^{-1} = g$, $\iota \circ \iota = \mathrm{Id}_G$, the identity map $G \to G$. In particular, ι is a bijection, both injective and surjective.

If $g \in G$, then

$$g^n := \underbrace{g \cdot \dots \cdot g}_{n \text{ times}} \text{ and } g^{-n} := (g^{-1})^n = (g^n)^{-1}$$

Exercise
If $m, n \in \mathbb{Z}$, then $(g^n)^m = g^{mn}$.

If $g, h \in G$, then

$$(gh)^n = ghgh \cdots gh,$$

which is not necessarily the same as $g^n h^n$ if G is not abelian.

Example: Groups

$\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all groups under operation $+$. The identity is 0 and the inverse of n is $-n$. These groups have infinite order. They are infinite abelian groups.

$\mathbb{Z}/n\mathbb{Z}$ is also a group under $+$. The identity is $0 = [0]$, and the inverse of $[m]$ is $-[m] = [-m]$. This group is finite, with order $|\mathbb{Z}/n\mathbb{Z}| = n$. It is a finite abelian group.

If $(V, +, \cdot)$ is a vector space, then $(V, +)$ is group. The identity element is 0, and the inverse of v is $-v$.

Example: Not a group?! & Trivial group

$\mathbb{Z}$ is not a group with respect to $\cdot$, since most elements do not have an inverse.

$\mathbb{Q}$ is also not a group with respect to $\cdot$, since 0 does not have an inverse.

$\mathbb{Q}^{\times}$ is a group with respect to $\cdot$.

Every group has to contain at least one element, the identity. So the simplest possible group is $\{1\}$ with operation $1 \cdot 1 = 1$. This is called the **trivial group**.

A non-abelian example

All the examples previously are abelian.

Let $\mathrm{GL}_n(\mathbb{K})$ denote the invertible $n \times n$ matrices with entries in a field $\mathbb{K}$.

Proposition 1.8

$\mathrm{GL}_n(\mathbb{K})$ is a group under matrix multiplication (called the **general linear group**). For $n \geq 2$, $\mathrm{GL}_n(\mathbb{K})$ is non-abelian.

Proof:

If A and B are invertible matrices, then AB is also invertible, so matrix multiplication is an associative binary operation $\mathrm{GL}_n(\mathbb{K})$. The identity matrix is an identity, and every element has an inverse by definition, so $\mathrm{GL}_n(\mathbb{K})$ is a group.

Exercise

Find matrices A, B such that $AB \neq BA$.

$\square$

1.4.2 Additive notation

Standard notation for operation in a group is gh. This is called **multiplicative notation**. For groups like $(\mathbb{Z}, +)$, it is confusion to write mn instead of $m + n$, since mn already has another meaning. For abelian groups G, there is another convention called **additive notation**. In additive notation, we write the group operation as $g + h$. The identity is denoted by 0 or 0_G. Inverse are denoted by $-g$. Writing g^n in additive notation gives

$$\underbrace{g + g + \ldots + g}_{n \text{ times}},$$

so rather than g^n we use ng. Similarly g^{-n} is $-ng$.

Multiplicative notation	Additive notation
$g \cdot h$ or gh	$g+h$
e_G or 1_G	0_G
g^{-1}	$-g$
g^n	ng

Table 1.1: Comparison between multiplicative and additive notation

For nonabelian groups we always use multiplicative notation. For abelian groups, we can choose either.

Note the potential for conflict between the two conventions. We must be clear about what convention we are using!.

For groups like $(\mathbb{Z}, +)$, we could denote the operation by mn, but it's clearer to write $m+n$. For groups like $(Q^\times, \cdot)$, we could denote the operation by $x+y$, but it is clearer to write $x \cdot y$ or xy.

1.4.3 Multiplicative table

multiplicative table

The multiplicative table of a group G is a table with rows and columns indexed by the elements of G. The cell for row g and column h contains the product gh.

The multiplication table contains the complete info of the group G. It is defined for finite and infinite groups, but makes the most sense for finite groups.

Example: $\mathbb{Z}/2\mathbb{Z}$

The multiplication table for $\mathbb{Z}/2\mathbb{Z}$ is

	0	1
0	0	1
1	1	0

1.4.4 Order of elements

order

If G is a group, then the order $g \in G$ is

$$|G| := \min\{k \geq 1 : g^k = e_G\} \cup \{+\infty\}$$

Some easy properties:

- $|g| = 1$ if and only if $g = e_G$.
- If $g^n = 1$, then $g^{n-1}g = gg^{n-1} = g^n = 1$, so $g^{n-1} = g^{-1}$. In particular, if $|g| = n < +\infty$, then $g^{-1} = g^{n-1}$.

Example: $\mathbb{Z}/n\mathbb{Z}$

We use additive notation for $\mathbb{Z}/n\mathbb{Z}$, so g^n is written as ng, $e = 0$. For this group, $k1 = 0$ if and only if n divides k, so $|1| = n$.

Lemma 1.9

$g^n = e$ if and only if $g^{-n} = e$, so in particular $|g| = |g^{-1}$.

Proof:

We have $g^{-n} = (g^n)^{-1}$. Since $g \mapsto g^{-1}$ is a bijection,

$$g^n = e \text{ if and only if } (g^n)^{-1} = e^{-1} = e.$$

But g^{-n} also equals $(g^{-1})^n$, so

$$\left\{k \geq 1 : g^k = e\right\} = \left\{k \geq 1 : \left(g^{-1}\right)^k = e\right\}$$

and this implies $|g| = |g^{-1}|$. $\square$

Index