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 $a, b, c \in X$.

Index