PMATH 347
Groups and Rings
Spring 2018

James Yu

May 9, 2018

Contents

Chapter 1

Introduction

1.1 Numbers

In this course we denote

$$\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \ldots\} \\
\mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\
\mathbb{Q} &= \left\{\frac{a}{b} : a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\right\} \\
\mathbb{R} &= \text{set of real numbers} \\
\mathbb{C} &= \left\{a + bi : a, b \in \mathbb{R} \text{ and } i^2 = -1\right\} \\
&= \text{set of complex numbers}
\end{aligned}$$

For $n \in \mathbb{Z}$ let $\mathbb{Z}_n$ denote the set of integers modulo n, i.e.

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

with congruence classes

$$[r] = \{z \in \mathbb{Z} : z \equiv r \mod n\} \qquad\qquad (0 \leq r \leq n-1)$$

We note that for $R = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_n$ we have two operations: addition and multiplication.

1.1.1 Addition

If $r_1, r_2, r_3 \in R$ then

$$\begin{aligned}
&r_1 + r_2 \in R && (\underline{\text{closure}}) \\
&r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3 && (\underline{\text{associativity}})
\end{aligned}$$

Also, if $R \neq \mathbb{N}$, there exists $0 \in R$ (identity) such that, for all $r \in \mathbb{R}$

$$r + 0 = r = r + 0$$

and there exists $-r \in R$ (inverse) such that

$$r + (-r) = 0 = (-r) + r$$

1.1.2 Multiplication

If $r_1, r_2, r_3 \in R$ then

$$r_1 \cdot r_2 \in R$$

$$r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$$

Also, there exists $1 \in R$ such that, for all $r \in R$

$$r \cdot 1 = r = 1 \cdot r$$

Finally, for $R = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, if $r \in R$, there exists $\frac{1}{r} \in R$ such that

$$r \cdot \frac{1}{r} = 1 = \frac{1}{r} \cdot r$$

We note that for $R = \mathbb{Z}_n$, not all $[r] \in \mathbb{Z}_n$ have a "multiplicative inverse." For example, for $[2] \in \mathbb{Z}_4$ there is no $[x] \in \mathbb{Z}_4$ such that $[2] \cdot [x] = [1]$.

1.2 Matrices

For $n \in \mathbb{N}$, an $n \times n$ matrix over $\mathbb{R}$ (where $\mathbb{R}$ can be replaced by $\mathbb{Q}$ or $\mathbb{C}$) is an $n \times n$ array

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

where $a_{ij} \in \mathbb{R}(1 \leq i, j \leq n)$.

We denote by $M_n(\mathbb{R})$ the set of all $n \times n$ matrices over $\mathbb{R}$.

1.2.1 Matrix Addition

Given $A = [a_{ij}]$, $B = [b_{ij}] \in M_n(\mathbb{R})$, we define

$$A + B = [a_{ij} + b_{ij}]$$

Note that $A + B \in M_n(\mathbb{R})$ and for A, B, $C \in M_n(\mathbb{R})$ we have

$$A + (B + C) = (A + B) + C$$

Define $0 \in M_n(\mathbb{R})$ by

$$0 = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

Thus we have

$$A + 0 = A = 0 + A$$

Finally, for $A \in M_n(\mathbb{R})$, there exists $-A = [-a_{ij}] \in M_n(\mathbb{R})$ such that

$$A + (-A) = 0 = (-A) + A$$

We also note that in this case

$$A + B = B + A \qquad \text{(\underline{commutativity})}$$

1.2.2 Matrix Multiplication

Given $A = [a_{ij}]$, $B = [b_{ij}] \in M_n(\mathbb{R})$ we define

$$AB = [c_{ij}] \qquad c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Note that $AB \in M_n(\mathbb{R})$. Also, for A, B, $C \in M_n(\mathbb{R})$ we have

$$A(BC) = (AB)C$$

Define $I \in M_n(\mathbb{R})$ by

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Then we have

$$AI = A = IA$$

However, for $A \in M_n(\mathbb{R})$, it is not always ture that there exists some $A^{-1} \in M_n(\mathbb{R})$ such that

$$AA^{-1} = I = A^{-1}A$$

Also, we can find A, $B \in M_n(\mathbb{R})$ such that

$$AB \neq BA$$

1.3 Permutations

Definition 1.3.1. Let $f : X \to Y$ be a function, we say f is 1-1 if

$$f(x_1) = f(x_2) \implies x_1 = x_2$$

We say f is onto if for all $y \in Y$, there exists $x \in X$ such that

$$f(x) = y$$

If f is 1-1 and onto, then we say f is a bijection.

Definition 1.3.2. Given a non-empty set L, a permutation of L is a bijection from L to L. The set of permutations of L is denoted by S_L

Index