PMATH347S18 - Groups & Rings

Johnson Ng

May 6, 2018

Table of Contents

List of Definitions

List of Theorems

1 Lecture 1 May 02nd 2018

1.1 Introduction

1.1.1 Numbers

The following are some of the number sets that we are already familiar with:

$$\mathbb{N} = \{1, 2, 3, ...\} \qquad \mathbb{Z} = \{.., -2, -1, 0, 1, 2, ...\}$$
$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \right\} \qquad \mathbb{R} = \text{ set of real numbers}$$
$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i = \sqrt{-1}\} = \text{ set of complex numbers}$$

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

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

where the $[r]$, $0 \leq r \leq n-1$, are the congruence classes, i.e.

$$[r] = \{z \in \mathbb{Z} : z \equiv r \mod n\}$$

These sets share some common properties, e.g. $+$ and $\times$. Let's try to break that down to make further observation.

Note that for $R = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_n$, R has 2 operations, i.e. addition and multiplication.

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

- (**closure**) $r_1 + r_2 \in R$
- (**associativity**) $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$

Also, if $R \neq \mathbb{N}$, then $\exists 0 \in R$ (the **additive identity**) such that

$$\forall r \in R \quad r + 0 = r = 0 + r.$$

Also, $\forall r \in R$, $\exists (-r) \in R$ such that

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

Multiplication For $r_1, r_2, r_3 \in R$, we have

- (**closure**) $r_1 r_2 \in R$
- (**associativity**) $r_1(r_2 r_3) = (r_1 r_2) r_3$

Also, $\exists 1 \in R$ (a.k.a the **mutiplicative identity**), such that

$$\forall r \in R \quad r \cdot 1 = r = 1 \cdot r.$$

Finally, for $R = \mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, $\forall r \in R$, $\exists r^{-1} \in R$ such that

$$r \cdot r^{-1} = 1 = r^{-1} \cdot r.$$

Note that for $R = \mathbb{Z}_n$, where $n \in \mathbb{Z}$, 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 $[2][x] = [1]$.[1]

[1] This is best proven using techniques introduced in MATH135/145.

1.1.2 *Matrices*

For $n \in \mathbb{N} \setminus \{1\}$, an $n \times n$ matrix over $\mathbb{R}$ [2] is an $n \times n$ array that can be expressed as follows:

[2] $\mathbb{R}$ can be replaced by $\mathbb{Q}$ or $\mathbb{C}$.

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

where for $1 \leq i, j \leq n$, $a_{ij} \in \mathbb{R}$. We denote $M_n(\mathbb{R})$ as the set of all $n \times n$ matrices over $\mathbb{R}$.

As in Section 1.1.1, we can perform **addition and multiplication** on $M_n(\mathbb{R})$.

Matrix Addition Given $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}] \in M_n(\mathbb{R})$, we define matrix addition as

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

which immediately gives the **closure property**, since $a_{ij} + b_{ij} \in \mathbb{R}$ and hence $A + B \in M_n(\mathbb{R})$. Also, by this definition, we also immediately obtain the **associativity property**, i.e.

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

We define the zero matrix as

$$0 = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

Then we have that 0 is the **additive identity**, i.e.

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

Finally, $\forall A \in M_n(\mathbb{R}), \exists(-A) \in M_n(\mathbb{R})$ (the **additive inverse**) such that

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

Note that in this case, we also have that that the operation is **commutative**, i.e.

$$A + B = B + A.$$

Matrix Multiplication Given $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}] \in M_n(\mathbb{R})$, we define the matrix multiplication as

$$AB = [d_{ij}] \text{ where } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \in \mathbb{R}.$$

Clearly, $AB \in M_n(\mathbb{R})$, i.e. it is **closed under matrix multiplication**. Also, we have that, under such a defintion, matrix multiplication is **associative**, i.e.

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

JOHNSON NG

Define the identity matrix, $I \in M_n(\mathbb{R})$, as follows:

$$I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Then we have that I is the **multiplicative identity**, since

$$AI = A = IA.$$

However, contrary to matrix addition, $\forall A \in M_n(\mathbb{R})$, it is not always true that $\exists A^{-1} \in M_n(\mathbb{R})$ such that

This is especially true if the **determinant** of A is 0.

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

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

$$AB \neq BA,$$

i.e. matrix multiplication is not always commutative.

THE COMMON PROPERTIES of the operations from above: **closure, associativity, and existence of an inverse**, are not unique to just addition and multiplication. We shall see in the next lecture that there are other operations where these properties will continue to hold, e.g. **permutations**.

2 Lecture 2 May 04th 2018

2.1 Introduction (Continued)

2.1.1 Permutations

Definition 2.1.1 (Injectivity)
Let $f : X \to Y$ be a function. We say that f is ***injective*** *(or* ***one-to-one****) if $f(x_1) = f(x_2)$ implies $x_1 = x_2$.*

Definition 2.1.2 (Surjectivity)
Let $f : X \to Y$ be a function. We say that f is ***surjective*** *(or* ***onto****) if $\forall y \in Y \;\; \exists x \in X \;\; f(x) = y$.*

Definition 2.1.3 (Bijectivity)
Let $f : X \to Y$ be a function. We say that f is ***bijective*** *if it is both* ***injective*** and ***surjective***.

Definition 2.1.4 (Permutations)
Given a non-empty set L, a permutation of L is a bijection from L to L. The set of all permutations of L is denoted by S_L.

Example 2.1.1
Consider the set $L = \{1, 2, 3\}$, which has the following 6 different permutations:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Note

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

indicates the bijection $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ with $\sigma(1) = 1$, $\sigma(2) = 3$ and $\sigma(3) = 2$.

For $n \in \mathbb{N}$, we denote $S_n := S_{\{1,2,\ldots,n\}}$, the set of all permutations of

$\{1, 2, ..., n\}$. Example 2.1.1 shows the elements of the set S_3.

Definition 2.1.5 (Order)
*The **order** of a set A, denoted by $|A|$, is the cardinality of the set.*

Example 2.1.2
We have seen that the order of S_3, $|S_3|$ is $6 = 3!$.

Proposition 2.1.1
$|S_n| = n!$

Proof
$\forall \sigma \in S_n$, there are n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$, ..., 2 choices for $\sigma(n-1)$, and finally 1 choice for $\sigma(n)$. □

Do elements of S_n share the same properties as what we've seen in the numbers? Given $\sigma, \tau \in S_n$, we can **compose** the 2 together to get a third element in S_n, namely $\sigma\tau$ (wlog), where $\sigma\tau : \{1, ..., n\} \to \{1, ..., n\}$ is given by $\forall x \in \{1, ..., n\}$, $x \mapsto \sigma(\tau(x))$.

It is important to note that $\because$ σ, τ are **both bijective**, $\sigma\tau$ is also bijective. Thus, together with the fact that $\sigma\tau : \{1, ..., n\} \to \{1, ..., n\}$, we have that $\sigma\tau \in S_n$ by definition of S_n.

$\therefore \forall \sigma, \tau \in S_n$, $\sigma\tau, \tau\sigma \in S_n$, but $\sigma\tau \neq \tau\sigma$ in general. The following is an example of the stated case:

Example 2.1.3
Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Compute $\sigma\tau$ and $\tau\sigma$ to show that they are not equal.

Solution

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

Perhaps what is interesting is the question of: **when does commutativity occur?** One such case is when σ and τ have support sets that are disjoint[1].

[1] This is proven in A1

On the other hand, the associative property holds[2], i.e.

[2]

Exercise 2.1.1
Prove this as an exercise.

PMATH347S18 - Groups & Rings

$$\forall \sigma, \tau, \mu \in S_n \;\; \sigma(\tau\mu) = (\sigma\tau)\mu$$

The set S_n also has an identity element[3], namely

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

[3]

Exercise 2.1.2
Verify that the given identity element is indeed the identity, i.e.

$$\forall \sigma \in S_n \;\; \sigma\varepsilon = \sigma = \varepsilon\sigma.$$

Finally, $\forall \sigma \in S_n$, since σ is a bijection, we have that its inverse function, σ^-1 is also a bijection, and thus satisfies the requirements to be in S_n. We call $\sigma^{-1} \in S_n$ to be the **inverse permutation** of σ, such that

$$\forall x, y \in \{1, ..., n\} \quad \sigma^{-1}(x) = y \iff \sigma(y) = x.$$

It follows, immediately, that

$$\sigma\left(\sigma^{-1}(x)\right) = x \wedge \sigma^{-1}\left(\sigma(y)\right) = y.$$

$\therefore$ We have that

$$\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma.$$

Example 2.1.4
Find the inverse of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 273 & \end{pmatrix}$$

Solution
By rearranging the image in ascending order, using them now as the object and their respective objects as their image, construct

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

It can easily (although perhaps not so prettily) be shown that

$$\sigma\tau = \varepsilon = \tau\sigma.$$

With all the above, we have for ourselves the following proposition:

Proposition 2.1.2 (Properties of S_n)
We have

1. $\forall \sigma, \tau \in S_n \;\; \sigma\tau, \tau\sigma \in S_n$.
2. $\forall \sigma, \tau, \mu \in S_n \;\; \sigma(\tau\mu) = (\sigma\tau)\mu$.

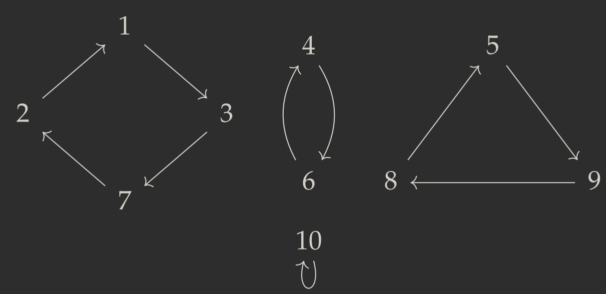
3. $\exists \varepsilon \in S_n \;\; \forall \sigma \in S_n \;\; \sigma\varepsilon = \sigma = \varepsilon\sigma.$

4. $\forall \sigma \in S_n \;\; \exists! \sigma^{-1} \in S_n \;\; \sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma.$

Consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 9 & 4 & 2 & 5 & 8 & 10 \end{pmatrix} \in S_{10}$$

If we represent the action of σ geometrically, we get



We observe that σ can be **decomposed** into one 4-cycle, $\begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix}$, one 2-cycle, $\begin{pmatrix} 4 & 6 \end{pmatrix}$, one 3-cycle, $\begin{pmatrix} 5 & 9 & 8 \end{pmatrix}$, and one 1-cycle, $\begin{pmatrix} 10 \end{pmatrix}$.

Note that these cycles are (pairwise) **disjoint**, and we can write[4]

$$\sigma = \begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 5 & 9 & 8 \end{pmatrix}$$

[4] We generally do not include the 1-cycle and assume that by excluding them, it is known that any number that is supposed to appear loops back to themselves.

Note that we may also write

$$\begin{aligned} \sigma &= \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 5 & 9 & 8 \end{pmatrix} \begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 6 & 4 \end{pmatrix} \begin{pmatrix} 9 & 8 & 5 \end{pmatrix} \begin{pmatrix} 7 & 2 & 1 & 3 \end{pmatrix} \end{aligned}$$

It is interesting to note that the cycles can rotate their "elements" in a **cyclic** manner, i.e.

$$\begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 7 & 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 7 & 3 \end{pmatrix}.$$

Although the decomposition of the cycle notation is not unique (i.e. you may rearrange them), each individual cycle is unique, and is proven below[5].

[5] See bonus question of A1. Proof will be included in the notes once the assignment is over.

Theorem 2.1.1 (Cycle Decomposition Theorem)
If $\sigma \in S_n$, $\sigma \neq \varepsilon$, then σ is a product of (one or more) disjoint cycles of length at least 2. This factorization is unique up to the order of the factors.

PMATH347S18 - Groups & Rings

Note (Convention)

Every permutation in S_n can be regarded as a permutation of S_{n+1} by fixing the permutation of $n+1$. Therefore, we have that

$$S_1 \subseteq S_2 \subseteq \ldots \subseteq S_n \subseteq S_{n+1} \subseteq \ldots$$

3 Index