MATH100A: Abstract Algebra

Course Webpage

September 27, 2021

Abstract

Warning: This is only a piece of lecture notes written by a careless scribe. So just be careful with and tolerant of any possible typos or misunderstandings when you read [0.1]. The scribe does not intend to make anyone to be driven by his stupidity! Also, the professor's explanation is extremely helpful as he discusses a lot about the interpretable ideas behind the dull scripts. So watch the lecture before reading this. If you have any suggestions (e.g. typos, typography, logistics), please do not hesitate contacting the scribe!

Without specifications, the notation use is as the following

- $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \ldots$: real, complex, quadratic, and so on
- $\mathcal{R}$: integrability
- $\mathbb{1}$: characteristic function
- $\boldsymbol{s}$: simple function
- $\mathcal{F}$: family
- $\mathcal{A}$: algebra

[0.1] Especially '$\cap$' and '$\cup$' are often mistaken because of typos.

Contents

MATH100A **Fall 2021**

Lecture 1: Law of Composition

Lecturer: Brandon Alberts *Scribes: Rabbittac*

Definition 1.1 (*Law of Composition*)

A ***law of composition*** *on set S is a rule for combining two elements $a, b \in S$ to create another element $p \in S$*

$$S \times S \to S$$

e.g.1.

- Addition on $\mathbb{Z}, \mathbb{R}$, etc
- Multiplication on $\mathbb{Z}, \mathbb{R}$, etc
- Cross product: $v_1, v_2 \in \mathbb{R}^3 \to v_1 \times v_2 \in \mathbb{R}^3$
- Dot product is **NOT**: $v_1, v_2 \in \mathbb{R}^3 \to v_1 \cdot v_2 \in \mathbb{R}$
- Division is **NOT**: division by 0 fails
- Composition of functions $f \circ g : t \to f(g(t))$

Definition 1.2 (*Commutative*)

A law of composition is ***commutative*** *if $ab = ba$* [1.1]*.*

Definition 1.3 (*Associative*)

A law of composition is ***associative*** *if $(ab)c = a(bc)$.*

Proposition 1.1

For an associate law of composition on S, there is a unique way to define a product of n elements $a_1, a_2, \dots, a_n$ temporarily denoted as $[a_1, a_2, \dots, a_n]$:

1. $[a_1] = a_1$
2. $[a_1, a_2] = a_1 a_2$
3. $\forall 1 \le i \le n : [a_1, a_2, \dots, a_n] = [a_1, \dots, a_i][a_{i+1}, a_n]$

Proof: By induction, $n = 1, 2$ are defined. Now suppose the proposition holds at $r = n - 1$, then $[a_1, a_2, \dots, a_n] = [a_1, \dots, a_{n-1}][a_n] = ([a_1, \dots, a_i][a_{i+1}, a_{n-1}][a_n]) = [a_1, \dots, a_i]([a_{i+1}, \dots a_{n-1}][a_n]) = [a_1, \dots, a_i][a_{i+1}, \dots, a_n]$. ■

[1.1] We commonly use ab to denote laws of composition. $a + b$ is only used for commutative laws in this course.

Definition 1.4 (*Identity*)

*An **identity** of a law of composition is an element $e \in S$ satisfying $\forall a \in S : ea = a = ae$* [1.2].

A law of composition can have at most one identity.

Definition 1.5 (*Invertible*)

*Suppose a law of composition on S has an identity 1. An element $a \in S$ is **invertible** if $\exists b \in S : ab = 1 = ba$* [1.3].

Proposition 1.2

1. *If a has both left inverse $la = 1$ and a right inverse $ar = 1$, then $l = r = a^{-1}$.*
2. *Inverses are unique.*
3. $(ab)^{-1} = b^{-1}a^{-1}$

Exercise: Let $T = \{a, b\}, S = \{f : T \to T\}$. Fill the i-τ-α-β table where $i(a) = a, i(b) = b$ (identity map); $\tau(a) = b, \tau(b) = a$ (transposition map); $\alpha(a) = \alpha(b) = a$ (constant function); $\beta(a) = \beta(b) = b$ (constant function).

[1.2] Identities are denoted 1 if compositions are written multiplicatively; 0 if compositions are written additively.

[1.3] If so, we call b the inverse of a and write $b = a^{-1}$, or $-a$ for addition notation.

MATH100A **Fall 2021**

Lecture 2: Group

Lecturer: Brandon Alberts *Scribes: Rabbittac*

	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

Proposition 2.1

If S has an associative law of composition, then any $a \in S$ has at most one inverse.

Proof: Suppose $b, c \in S$ are both inverses of a. Then $ac = 1 \implies b(ac) = b1 \implies (ba)c = b \implies c = b$. ■

Definition 2.1 (*Group*)

*A **group** is a set G with a law of composition that is*

- *Associative;*
- *Has identity;*
- *Every element has an inverse.*

*A group which is commutative is called an **Abelian group**.*

e.g.1. $(\mathbb{Z}, +)$ is a group.

Definition 2.2 (*Order*)

*The **order** of a group is the number of elements in the set G, $|G|$.*

Proposition 2.2

Let $a, b, c \in G$. If $ab = ac$ or $ba = ca$, then $b = c$.

Proof: $ab = ac \implies a^{-1}ab = a^{-1}ac \implies b = c$. ■

Q&A. $ab = ca \implies b = c$ implies a group is Abelian? Yes.

e.g.2.

1. The $n \times n$ **general linear group**

$$\mathrm{GL}_n = \{n \times n \text{ invertible matrices }\}$$

When $n > 1$, $\mathrm{GL}_n(\mathbb{C}) = \mathbb{C} \setminus \{0\}$; when $n > 1$, then $\mathrm{GL}_n(\mathbb{C})$ is not Abelian.

2. Let T be a set. A bijective map $T \to T$ is called a **permutation** of T. The **symmetric group**

$$\mathrm{Sym}(T) = \{ \text{ bijections } T \to T\}$$

If $T = \{1, 2, \ldots, n\}$, then we denoted

$$S_n := \mathrm{Sym}(T)$$

And $|S_n| = n!$.

e.g.3.

- $|G| = 1 : G = \{1\}$ is a trivial group.
- $|G| = 2 : G = \{1, g\}$. Then $g^2 = 1$ or $g^2 = g$

Exercise: How many groups of size 3 are there?

e.g.4. S_3 is the smallest non-Abelian group (size 6). Take the cyclic permutation x and the transposition y. Then $x^3 = 1, y^2 = 1, yx = x^2y$. With the cancellation law, elements of $\{1, x, x^2, y, xy, x^2y\}$ are distinct.

Definition 2.3 (*Subgroup*)

*A subset $H \subseteq G$ of a group is a **subgroup** if*

- *Closure: $\forall a, b \in H : ab \in H$*
- *Identity: $i \in H$*
- *Inverses: $a \in H \implies a^{-1} \in H$*

e.g.5. The circle group $\{z \in \mathbb{C} : |z| = 1\}$ is a subgroup of the multiplicative group $(\mathbb{C}, \times)$.