MATH 323, Algebra I, Fall 2020

Course notes, Chapter 1, Introduction

Laurence Barker, Bilkent University. Version: 14 November 2020.

These notes, updated as the course progresses, are a record of the prepared text of the lectures, with a little more detail added, but they cannot cover much of the oral component of the lectures.

The course text is:

Thomas W. Judson, *Abstract Algebra*, 2020 edition.

To download a free copy of it, search for "Judson Abstract Algebra". The website is abstract.ups.edu, supported by University of Puget Sound.

These notes are independent of that text, but cover similar material.

Summary of contents

The material below is a review of some notions from set theory and introductory number theory. Thorough details on the material we shall be summarizing can be found in Judson, Chapters 1 and 2. (We mention that Judson Section 1.1 has some lucid comments about mathematical method. See, especially, the paragraph in Judson headed "Some cautions and suggestions".)

We shall be reviewing the notions of:

- a *set*,
- a *function*,
- an *equivalence relation*,
- a *partial ordering*.

Sets and direct products: For the purposes of the course, we understand a **set** to be a well-behaved collection of mathematical objects. And we understand any set to be, itself, a well-behaved mathematical object.

We shall assume familiarity with standard basic notation concerning sets. For instance, the **direct product** of sets A and B is defined to be

$$A \times B = \{(a, b) : a \in A, b \in B\} .$$

Correspondences: We define a **correspondence** to be a triple (A, G, B) where A and B are sets and $G \subseteq A \times B$. We call A the **codomain**, G the **graph**, B the **domain** of (A, G, B). We call (A, G, B) a correspondence $A \leftarrow B$.

Sometimes, not always, the following form is used as notation for correspondences. Consider a correspondence $\sim = (A, G, B)$. For $a \in A$ and $b \in B$, we write $a \sim b$ provided $(a, b) \in G$. Thus, for any $a \in A$ and $b \in B$, the expression $a \sim b$ denotes a statement. In other words, $a \sim b$ has a truth-value: true or false. When $a \sim b$ is false, we write $a \not\sim b$. Note that $\not\sim$ is another relation $A \leftarrow B$. We call $\not\sim$ the **negative** of the relation $\sim$. Of course, $\sim$ is the negative of $\not\sim$. Negations of a correspondence are often indicated with a slash through the symbol denoting the relation. As a possibly familiar example of the usage, we write $a \neq b$ when a is not equal to b.

Functions: The notion of a function is a special case of the notion of a correspondence. We define a **function** to be a correspondence $f = (A, G, B)$ such that, for all $b \in B$, there exists a unique $a \in Y$ satisfying afb.

But the notation afb is rarely used when discussing functions. Instead, a different notation is conventionally used, as follows. When afb, we write $a = f(b)$ and $f : a \leftarrow\!\shortmid b$. The element $a = f(b)$ is called the **image** of b under f.

The **identity function** on any set A is defined to be the function id_A such that $\mathrm{id}_A(a) = a$ for all $a \in A$.

Composites of functions: Given sets A, B, C and functions $f : A \leftarrow B$ and $g : B \leftarrow C$, we define the **composite** of f and g, denoted $f \circ g$, to be the function $A \leftarrow C$ such that

$$(f \circ g)(c) = f(g(c))$$

for all $c \in C$. The notion of a composite function is illustrated by the following diagram.

Injections, surjections, bijections: Let A and B be sets and $f : A \leftarrow B$ a function.

• We say that f is **injective** or **into** provided, for all $a \in A$, there exists at most one $b \in B$ such that $a = f(b)$.

• We say that f is **surjective** or **onto** provided, for all $a \in A$, there exists at least one $b \in B$ such that $a = f(b)$.

• We say that f is **bijective** provided f is injective and surjective. That is equivalent to the condition that there exists a function $g : A \to B$ satisfying $f \circ g = \mathrm{id}_A$ and $g \circ f = \mathrm{id}_B$. In that case, g is unique and we write $f^{-1} = g$. We call f^{-1} the **inverse** of g.

Relations: Given a set X, we define a **relation** on X to be a correspondence $X \leftarrow X$. Thus, given a relation $\sim$ on X then, for all $x, y \in X$, we have a statement $x \sim y$.

Recall, given integers a and b, we write $a < b$ and $b > a$ when a is less than b. We write $a \leq b$ and $b \geq a$ when a is less than or equal to b. Thus, $<$, $>$, $\leq$, $\geq$ are four relations on $\mathbb{Z}$.

Equivalence relations: We define an **equivalence relation** on a set X to be a relation $\equiv$ on X that satisfies the following three conditions:

Reflexivity: For all $x \in X$, we have $x \equiv x$.
Symmetry: For all $x, y \in X$ such that $x \equiv y$, we have $y \equiv x$.
Transitivity: For all $x, y, z \in X$ such that $x \equiv y$ and $y \equiv z$, we have $x \equiv z$.

For an equivalence relation $\equiv$ on a set X and an element $x \in X$, the set

$$[x] = \{y \in X : x \equiv y\} = \{y \in X : y \equiv x\}$$

is called the **equivalence class** of x under $\equiv$.

Remark: *Given a set X and an equivalence relation $\equiv$ on X, then the equivalence classes under X are mutually disjoint and their union is X. In other words, each element of x belongs to a unique equivalence class.*

Partial orderings: We define a **partial ordering** on a set X to be a relation $\leq$ on X that satisfies the following three conditions:

Reflexivity: For all $x \in X$, we have $x \equiv x$.
Antisymmetry: For all $x, y \in X$ such that $x \leq y$ and $y \leq x$, we have $x = y$.
Transitivity: For all $x, y, z \in X$ such that $x \equiv y$ and $y \equiv z$, we have $x \equiv z$.

Note that the reflexivity and antisymmetry can be unified as the condition: for all $x, y \in X$, we have $x = y$ if and only if $x \leq y$ and $y \leq x$.

When $x \leq y$, we may write $y \geq x$. When $x \leq y$ and $x \neq y$, we may write $x < y$ and $y < x$.

Some preliminary exercises

The following exercises are just by way of reviewing some prerequisite material. Please let me know if you have difficulty with any of them.

Question A: Let A and B be sets. Let $f : A \leftarrow B$ be a function. Let g_1 and g_2 be functions $A \to B$ such that $g_1 \circ f = \mathrm{id}_B$ and $f \circ g_2 = \mathrm{id}A$. Show that f is bijective and $f^{-1} = g_1 = g_2$.

Question B: Can every function be expressed as a composite $f \circ g$ where f is injective and g is surjective? (Give a proof or a counter-example.)

Question C: Can every function be expressed as a composite $f \circ g$ where f is surjective and g is injective? (Give a proof or a counter-example.)

Question D: Let A be a set with size 5.
(a) How many functions $f : A \leftarrow A$ are there such that there exists a function $g : A \leftarrow A$ satisfying $g \circ f = \mathrm{id}_A$?
(b) How many functions $f : A \leftarrow A$ are there such that there exists a function $g : A \leftarrow A$ satisfying $f \circ g = \mathrm{id}_A$?

Question E: Let A and B be sets and let f be a function $A \leftarrow B$. A function $g : A \to B$ satisfying $g \circ f = \mathrm{id}_B$ is called a **left inverse** of f. The term **right inverse** is defined similarly. Give a nice description of the functions that have left inverses, likewise for functions that have right inverses.

Question F: How many equivalence relations on the set $\{1, 2, 3\}$ are there?

Question F: How many partial orderings on the set $\{1, 2, 3\}$ are there?