ARTHUR LI

ABSTRACT ALGEBRA

Introduction

This collection of notes serve as a guide to mastering abstract algebra with content from undergraduate to graduate level course. The notes combine knowledge from different sources, including course notes and textbooks used in the courses.

Prerequisites

These notes will assume no familiarity with any aspects of abstract algebra, and builds upon the foundation from Group Theory to more abstract topics such as Categories and Commutative Algebra. A good starting point will be the series on Visual Group Theory by Professor Matthew Macauley.

Familiarity with basic styles of proof is assumed (contradiction, contrapositive, etc.).

Organization and Sources

This section will be edited as the notes progress towards completion.

Contents

1 Preliminaries

1.1 Introductory Ideas and Definitions

Definition 1.1.1. *Class* is a collection A of objects (elements) such that given any object x it is possible to determine if x is a member of A.

Definition 1.1.2. *Axiom of extensionality* asserts that two classes with the same elements are equal.
(Formally, $[x \in A \iff x \in B] \Rightarrow A = B$).

Definition 1.1.3. A class is defined to be a *set* if and only if there exists a class B such that $A \in B$.
A class that is not a set is called a *proper set*.

Definition 1.1.4. *Axiom of class formation* asserts that for any statement $P(y)$ in the first predicate calculus involve a variable y, there exists a class A such that $x \in A$ if and only if x is a set and the statement $P(x)$ is true. The class is denoted $\{x|P(x)\}$.

Definition 1.1.5. A class A is a *subclass* of class B ($B \subset A$) provided $\forall x \in A, x \in A \iff x \in B$.
A subclass A of a class B that is itself a set is called a *subset* of B.
The *empty or null set* (denoted $\emptyset$) is the set with no elements.

Definition 1.1.6. *Power axiom* asserts that for every set A the class $P(A)$ of all subsets of A is itself a set. $P(A)$ is the *power set* of A, denoted 2^A.

Definition 1.1.7. A *family of sets* indexed by (nonempty) class I is a collection of sets A_i, one for each $i \in I$ (denoted $\{A_i|i \in I\}$).
The *union* is defined as $\bigcup\limits_{i \in I} A_i = \{x|x \in A_i \ for\ some\ i \in I\}$.
The *intersection* is defined as $\bigcap\limits_{i \in I} A_i = \{x|x \in A_i \ for\ every\ i \in I\}$.
If $A \cap B = \emptyset$, then A and B are disjoint.

Definition 1.1.8. The *relative complement* of A in B is the following subclass of B: $B - A = \{x|x \in B \ and\ x \notin A\}$.
If all classes under discussion are subsets of some fixed set U (the universe of discussion), then $U - A = A'$ is the *complement* of A.

Definition 1.1.9. Given classes A and B, a *function / map / mapping* f from A to B (written $f : A \to B$ assigns to each $a \in A$ exactly one element $b \in B$.

Then b is the value of function at a, or the *image* of a, written $f(a)$.

A is the *domain* of the function, written $dom f$, and B is the *range* or *codomain*.

Two functions are *equal* if they have the same domain and range, and have the same value for each element of their common domain.

Definition 1.1.10. If $f : A \to B$ is a function and $S \subset A$, the function from S to B given by $a \mapsto f(a)$, for $a \in S$, is *restriction* of f to S, denoted $f|S : S \to B$.

If $S \in A$, the function $1_A|S : S \to A$ is the *inclusion map* of S into A.

Definition 1.1.11. Let $f : A \to B$ and $g : B \to C$ be functions. The *composite* of f and g is the function $A \to C$ given by $a \mapsto g(f(a)), a \in A$. This is denoted $g \circ f$ or simply gf.

Definition 1.1.12. The *diagram of functions* is said to be commutative if $gf = h$, or if $kh = gf$.

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "h"'] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[d, "g"] \\ C \arrow[r, "k"] & D \end{tikzcd} \tag{1.1}$$

Definition 1.1.13. Let $f : A \to B$ be a function. If $S \in A$, *the image of S under f* (denoted $f(S)$)) is the class $\{b \in B | b = f(a) \ for \ some \ a \in S\}$.

The class $f(A)$ is the *image of f*, denoted $Im\ f$.

If $T \subset B$, the *inverse image of T* under f (denoted $f^{-1}(T)$), is the class $\{a \in A | f(a) \in T\}$.

Definition 1.1.14. A function $f : A \to B$ is said to be *injective* (or one-to-one) provided $\forall a,\ a' \in A,\ a \neq a' \Rightarrow f(a) \neq f(a')$, or $f(a) = f(a') \Rightarrow a = a'$.

A function f is *surjective* (or on-to) provided $f(A) \approx B$; in other words, for each $b \in B$, $b = f(a)$ for some $a \in A$.

A function f is *bijective* (or one-to-one correspondence) if it is both injective and surjective.

Definition 1.1.15. The map $g : B \to A$ is a *left inverse* of f if $gf = 1_A$.

The map $h : B \to A$ is a *right inverse* of f if $fb = 1_B$.

If a map $f : A \to B$ has both a left inverse g and a right inverse h, then $g = g1_B = g(fh) = (gf)h = 1_A h = h$, and $g = h$ is the *two-sided inverse*.

2 Group Theory

3 Group Structures

4 Ring Theory

4.1 Basic Axioms

Definition 4.1.1. A *ring* is a nonempty set R with two binary operations $+$ (addition) and $\times$ (multiplication), $(R, +, \times)$, such that:

(i) $(R, +)$ is an additive abelian group with 0 as the additive identity

(ii) the binary operation $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$, $\forall a, b, c \in R$

(iii) left and right distributive laws: $(a + b) \times c = (a \times c) + (b \times c)$, $a \times (b + c) = (a \times c) + (b \times c)$, $\forall a, b, c \in R$.

Definition 4.1.2. If in addition to definition of ring, $a \times b = b \times a \forall a, b \in R$, then R is a *commutative ring*.

Definition 4.1.3. The ring R has a *multiplicative identity* if there is an element $1_R \in R$ such that $1_R \times a = a \times 1_R = a$, $\forall a \in R$.

The ring R has a *additive identity* if there is an element $0_R \in R$ such that $a - b = a + (-b) = 0_R$, where $-b$ is the *additive inverse*.

Definition 4.1.4. A *division ring* R is a ring such that:

(i) R has a multiplicative identity 1_R;

(ii) $1_R \neq 0_R$; and

(iii) $\forall$ nonzero element $a \in R \backslash \{0\}$ has a unique multiplicative inverse a^{-1} such that $aa^{-1} = 1 = a^{-1}a$

Definition 4.1.5. A *field* is a division ring which is commutative.

If R is a division ring (field), then $(R, \times)$ is a (commutative) *multiplicative group*, $R^{\times} = R \backslash \{0\}$.

Definition 4.1.6. Let $F = (F, +, \times)$ be a field. A nonempty subset $E \subseteq F$ is a *subfield* if:

(i) $(E, +)$ is an additive subgroup of $(F, +)$;

(ii) E is closed under multiplication $\times$: $a, b \in E \Rightarrow a \times b \in E$;

(iii) $1_F \in E$; and

(iv) $a \in E \backslash \{0 \;\Rightarrow a^{-1} \in E$

4.2 *Ring Homomorphisms*

4.3 *Ring Isomorphisms*

4.4 *Ideals, Rings of Fractions, Local Rings*

4.5 *Euclidean Domains, PID, UFD*

5 Modules

5.1 Basic Axioms

6 Category Theory

6.1 Basic Axioms