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: $B - A = \{x|x \in B \text{ and } x \notin A\}$.*
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 $\mathrm{dom} f$, 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 $\{b \in B | b = f(a) \text{ for some } a \in S\}$.*

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

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 $g = g1_B = g(fh) = (gf)h = 1_Ah = h$, and $g = h$ is the two-sided inverse.

2 Group Theory

3 Group Structures

3.1 Free Abelian Groups

3.2 Finitely Generated Abelian Groups

3.3 Krull-Schmidt Theorem

3.4 Group Action

3.5 The Sylow Theorems

3.6 Semidirect Products

3.7 Normal and Subnormal Series

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

Remark 4.1.7. *The trivial ring is* $\{0\}$*.*

The integer ring is $(\mathbb{Z}, +, \times)$ *with* 1*, but is neither a division ring or field.*

$n\mathbb{Z} = \{ns | s \in \mathbb{Z}\}$ *is a subring of* $\mathbb{Z}$*.*

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *is a commutative ring with* 1 *for* $n \geq 2$*.*

Remark 4.1.8. *The* 2*-dimensional vector space* $\mathbb{Q}[\sqrt{D}] = \mathbb{Q} + \mathbb{Q}\sqrt{D} = \{a + b\sqrt{D} | a, b \in \mathbb{Q}\}$ *with* $\mathbb{Q}$*-basis* $\{1, \sqrt{D}\}$ *is a Quadratic Field.*

Define $\mathbb{Q}(\sqrt{D}) = \{\frac{a+b\sqrt{D}}{c+d\sqrt{D}} | a, b, c, d \in \mathbb{Q}, c + d\sqrt{D} \neq 0\}$*. Then* $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}[\sqrt{D}]$*.*

More generally, for a field F*,* $\mathbb{Q}(F) = \{\frac{\alpha}{\beta} = \alpha\beta^{-1} | \alpha\beta, \in F, \beta \neq 0\} = F$*.*

Remark 4.1.9. *Let* $H = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$ *be the* 4*-dimensional vector space over* $\mathbb{R}$ *with* $\mathbb{R}$*-basis* $(1, i, j, k)$*.*

The multiplication is extended linearly by distributive law: $i^2 = j^2 = k^2 = -1$*,* $ij = k = -ji, jk = i = -kj$*,* $ki = j = -ik$*. Then* H *is a Real Quaternion Ring.*

$H_{\mathbb{Q}} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k = \{a + bi + cj + dk | a, b, c, d \in \mathbb{Q}\}$ *is the Rational Hamilton Quaternion Ring.*

Remark 4.1.10. *Let* $\mathbb{R}V[x] = \{f : \mathbb{R} \to \mathbb{R}\}$ *be the set of all real-valued functions. Let* $x \mapsto c(x) = c$ *be a constant function.*

For $f, g \in \mathbb{R}V[x]$*, the natural addition is* $x \mapsto (f + g)(x) = f(x) + g(x)$*.*

The multiplication (not composition) is $x \mapsto (fg)(x) = f(x)g(x)$*.*

The $(\mathbb{R}V[x], +, \times)$ *is a commutative (real valued-function) ring with multiplicative identity* 1 *being the constant function* 1*.*

Definition 4.1.11. *Let* R *be a ring with* $1 \neq 0$*. An element* $u \in R$ *is a unit if it has a multiplicative identity inverse* u' *such that* $uu' = 1 = u'u$*.*

The set of all units of R *are* $U(R) = \{u \in R | u \text{ is a unit}\}$*.*

The multiplicative group of units of the ring R *is* $(U(R), \times)$*.*

Remark 4.1.12. *More generally, let* X *be a set and* R *be a ring. Let* $X_{to}R := \{f : X \to R\}$ *be the set of all maps between* X *and* R*. Then for* $f, g \in X_{to}R$*, there are natural addition* $f + g$ *and multiplication* fg *(*$x \mapsto f(x)g(x)$*) as in previous remark.*

Then $(X_{to}R, +, \times)$ *is a ring, called the R-Valued Function Ring.*

If R *has* 1 *then so does* $X_{to}R$*. If* R *is commutative then so does* $X_{to}R$*.*

Every $c \in R$ *defines a constant function (an element in* $X_{to}R$*,* $c : X \to R$*;* $x \mapsto c(x) = c$*.*

Identify R *with the subset of* $X_{to}R$ *of constant function. Then* R *is a subring of* $X_{to}R$*.*

Remark 4.1.13. *Let* $n \geq 2$*. Then* $U(\mathbb{Z}/n\mathbb{Z})$ *is a commutative multiplicative group of order* $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$*. Hence* $\varphi(n)$ *is the Euler's* φ*-function,* $\varphi(n) = |\{1 \leq s \leq n | gcd(s, n) = 1\}|$*.*

Definition 4.1.14. *An Integral Domain is a commutative ring with* $1 \neq 0$ *such that* $\forall a, b, \in R,\ ab = 0 \Rightarrow a = 0$ *or* $b = 0$*, or equivalently,* $\forall a, b \in R,\ a \neq 0,\ b \neq 0 \Rightarrow ab \neq 0$*.*

$\mathbb{Z}$ *is an integral domain.*

Every field is an integral domain.

Definition 4.1.15. *Let R be a ring. A nonzero element $a \in R$ is a zero divisor if there is a nonzero $b \in R$ such that either $ab = 0$ or $ba = 0$.*

A commutative ring R with 1 is an integral domain if and only if R as no zero divisors.

Proposition 4.1.16. *Let R be w ring with $1 \neq 0$. Then R is an integral domain if and only if the cancellation law holds: $\forall a, b, c \in R,\ c \neq 0,\ ca = cb \Rightarrow a = b$.*

Corollary 4.1.17. *Let R be a finite integral domain, i.e., R is an integral domain with the cardinality $|R| < \infty$. Then R is a field.*

Proposition 4.1.18. *Let $n \geq 2$. Then the following are equivalent:*

- *(i)* $\mathbb{Z}/n\mathbb{Z}$ *is a field*
- *(ii)* $\mathbb{Z}/n\mathbb{Z}$ *is an integral domain*
- *(iii)* n *is a prime*

Definition 4.1.19. *Let R be a ring. A nonempty subset $S \subseteq R$ is a subring of R if:*

- *(i)* $(S, +)$ *is an additive subgroup of* $(R, +)$ *and*
- *(ii)* S *is closed under multiplication*

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Proposition 4.1.20. *(Subring Criterion) Let R be a ring and $S \subseteq R$ a nonempty subset. Then the following are equivalent:*

- *(i)* S *is a subring of* R
- *(ii)* S *is closed under subtracting and multiplication:* $a, b \in S \Rightarrow ab \in S;\ a - b = a + (-b) \in S$

Remark 4.1.21. *Being a subring is a transitive condition. If R is a subring of S and S is a subring of T, then R is a subring of T.*

If both S_i are subring of R and $S_1 \subseteq S_2$, then S_1 is a subring of S_2.

Remark 4.1.22. *(Subring without 1) If R is a ring with $1 = 1_R$ then a subring $S \subseteq R$ may not contain 1, i.e., $m\mathbb{Z} = ms|s \in \mathbb{Z}, |m| \geq 2$ is a subring of $\mathbb{Z}$ which does not contain 1.*

Remark 4.1.23. *(Intersection of subrings) Let R_α ($\alpha \in \Sigma$) be a (not necessarily finite or countable) collection of subrings of a ring R. Then the intersection $\bigcap_{\alpha \in \Sigma} R_\alpha$ is a subring of R.*

Generally, the union of subrings may not be a subring.

Remark 4.1.24. *(Union of ascending subrings) Let $R_1 \subseteq R_2 \subseteq \cdots$ be an ascending chain of subrings R_i of a ring R. Then the union $\bigcup_{i=1}^{\infty} R_\alpha$ is a subring of R.*

Remark 4.1.25. *(Addition of subrings) Let R be a ring and let R_i be subrings of R.*

Then the addition $R_1 + \cdots + R_n$ is closed under subtraction, but may not be closed under multiplication, hence may not be a subring of R.

Remark 4.1.26. *(Integral domain is a subring of a field)*

Let F be a field. Let $R \subseteq F$ be a subring such that $1 \in R$. Then R is an integral domain.

Every integral domain R is a subring of some field $\mathbb{Q}(R)$ (the fractional field of R).

Remark 4.1.27. *(Product of Rings) let $n \geq 1$ and let $R_i = (R_i, +, \times)$ $(i = 1, \ldots, n)$ be rings.*

Then the direct product is a ring, $R = R_1 \times \cdots \times R_n$. (The direct product is $(a_1, \ldots, a_n) \times (a'_1, \ldots, a'_n) = (a_1 a'_1, \ldots, a_n a'_n)$.

The unit subgroups has the relation $U(R) = U(R_1) \times \cdots \times U(R_n)$

4.2 Examples of Rings

Definition 4.2.1. *The (polynomial ring $R[x] overaring R$) is $(R[x], +, \times)$,*

where $R[x] = \{\sum_{j=0}^{d} b_j x_j | d \geq 0,\ b_j \in \mathbb{R}\}$.

There are natural addition and multiplication operations for polynomials.

Remark 4.2.2. *Let R be a commutative ring with 1. Let $S := R[x]$ be the polynomial ring over R.*

(i) R is a subring of S which consists of constant polynomial functions.

(ii) $0_S = 0_R$

(iii) S contains $1 = 1_S$, and $1_S = 1_R$.

Proposition 4.2.3. *(Polynomial ring over integral domain) Let R be an integral domain. Let $f(x), g(x) \in R[x]$. Then*

(i) $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$

(ii) $U(R[x]) = U(R)$. Namely, $g(x)$ is a unit of $R[x]$ if and only if $g = a_0 \in R$ (constant polynomial) with a_0 a unit in R.

(iii) $R[x]$ is an integral domain

Remark 4.2.4. *The matrix ring of $n \times n$ square matrices with entries in the ring R is defined as $(M_n(R), +, \times)$, where*

$$M_n(R) = \left\{ A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} | a_{ij} \in R \right\}$$

If $A = (a_{ij}), B = (b_{ij}) \in M_n(F)$*, then* $A + B = (a_{ij} + b_{ij}), AB = (c_{ij})$ *where* $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$.
$A = (a_{ij}) = Diag[a_{11}, \ldots, a_{nn}]$ *is a diagonal matrix if* $a_{ij} = 0$ *(*$i \neq j$*).*
$A = (a_{ij}) = Diag(a_1, \ldots, a_n)$ *is a scalar matrix if* $a_{ii} = a \in R\ \forall i$*, and* $a_{ij} = 0$ *(*$i \neq j$*).*
$A = (a_{ij})$ *is an upper triangular matrix if* $a_{ij} = 0$ *(*$i < j$*). The lower triangular matrix is defined similarly.*

4.3 Ring Homomorphisms

4.4 Ring Isomorphisms

4.5 Ideals, Rings of Fractions, Local Rings

4.6 Euclidean Domains, PID, UFD

5 Modules

5.1 Basic Axioms

6 Category Theory

6.1 Basic Axioms