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.

The proofs for Theorems, Propositions and Lemmas will be added when I have completed the entire skeleton.

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 $\bigcup\limits_{i \in I} A_i = \{x|x \in A_i \text{ for some } i \in I\}$.

The intersection is defined as $\bigcap\limits_{i \in I} A_i = \{x|x \in A_i \text{ for every } i \in I\}$.

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 $\operatorname{dom} f$, 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 $\operatorname{Im} f$.

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

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 $\bigcap\limits_{\alpha \in \Sigma} R_\alpha$ 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 $R[x]overaringR$) 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.

Remark 4.2.5. *Let R be a ring and $S = M_n(R)$ the matrix ring with entries in R. Then*

(i) $0_S = (a_{ij})$ where $a_{ij} = 0$ (the zero matrix)

(ii) If R has $1 = 1_R$, then S also has $1 = 1_S$ with $1_S = Diag[1_R, \ldots, 1_R]$

(iii) The set $S_{c_n}(R) = \{Diag[a, \ldots, a] | a_i \in R\}$ of all scalar matrices in $M_n(R)$ is a subring of $M_n(R)$. There is a natural ring isomorphism $R \cong S_{c_n}(R)$.

(iv) The set $D_n(R) = \{Diag[]a_1, \ldots, a_n | a_i \in R\}$ of all diagonal matrices in $M_n(R)$ is a subring of $M_n(R)$. There is a natural ring isomorphism $D_n(R) \cong R^n := R \times \cdots \times R$ (n times).

(v) The set $UT_n(R) := \{(a_{ij} | (a_{ij} \in R, (a_{ij} = 0(\forall\ i > j))\}$ of all upper triangular matrices in $M_n(R)$ is a subring of $M_n(R)$. Similarly, the set $LT_n(R)$ of all lower triangular matrices in $M_n(R)$ is a subring of $M_n(R)$.

(vi) If R is a subring of R, then $M_n(T)$ is a subring of $M_n(R)$

(vii) Even if R is commutative, $M_n(R)$ may not be commutative when $n \geq 2$.

(viii) If $n \geq 2$, then $M_n(R)$ is not an integral domain (even when R is a field).

Definition 4.2.6. *Let R be a ring with 1. Set $GL_n(R) := U(M_n(R))$ the set of all units in $M_n(R)$. Then $GL_n(R)$ is a multiplicative group called the general linear group of degree n over R.*

Definition 4.2.7. *Let R be a commutative ring with 1. Define determinant $det(A) = |A|$, Let $SL_n(R) := \{A \in M_n(R) | det(A) = 1\}$ be the set of all matrices in $M_n(R)$ with determinants equal to 1. Then $SL_n(R)$ is a multiplicative subgroup of $GL_n(R)$ called the special linear group of degree n over R.*

Definition 4.2.8. *(Group Rings $R[G]$)*
Let R be a commutative ring with $1 \neq 0$. Let $G = \{g_1, \ldots, g_n\}$ be a finite multiplicative group of order n.
Then $R[G]$ is a group ring, where $R[G] = Rg_1 + \cdots + Rg_n = \{a_1g_1 + \cdots + a_ng_n | a_i \in R\}$.
Natural addition is defined as $(\sum_{i=1}^{n} a_ig_i) + (\sum_{i=1}^{n} b_ig_i) = (\sum_{i=1}^{n}(a_i + b_i)g_i)$.
Multiplication is defined as $(\sum_{i=1}^{n} a_ig_i) \times (\sum_{j=1}^{n} b_jg_j) := (\sum_{k=1}^{n} c_kg_k)$ where $c_k = \sum_{g_ig_j = g_k} a_ib_j$ with the sum running $\forall (i, j)$ with $g_ig_j = g_k$.

Remark 4.2.9. *Let R be a commutative ring with $1 \neq 0$, G a multiplicative group, and $R[G]$ the group ring. Then*

(i) $R[G]$ is a commutative ring if and only if G is commutative (=abelian) group

(ii) $R[G]$ has the multiplicative identity $1 = 1_Re_G$

Remark 4.2.10. *Let $R[G]$ be a group ring.*

(i) There is a natural injective ring homomorphism $R \to R[G]$; $r \mapsto re_G$. Identify R with the image Re_G of this injective homomorphism.

(ii) For every $g \in G$, the element $1_R g$ is a unit in $R[G]$

(iii) There is a natural injective group homomorphism $G \to U(G[R])$; $g \mapsto 1_R g$. Identify G with the image $1_R G$ of this injective homomorphism.

(iv) If S is a subring of R, then $S[G]$ is a subring of $R[G]$. If H is a subgroup of G, then $R[H]$ is a subring of $R[G]$.

(v) $T = \{\sum_{i=1}^{n} a_i g_i \in R[G] | \sum_{i=1}^{n} a_i = 0\}$ is a subring of $R[G]$ (an ideal of $R[G]$)

Remark 4.2.11. *When R is a division ring or field, then $R[G]$ (as an additive group) is a vector space over R of dimension equal to $|G|$ with basis $\{g_1, \ldots, g_n\} = G$. Hence $R[G] = Rg_1 + \cdots + Rg_n = Rg_1 \oplus \cdots \oplus Rg_n$, the direct sum of 1-dimensional vector subspaces Rg_i over R.*

4.3 Ring Homomorphisms

Definition 4.3.1. *Let R, S be rings. A map $\varphi : R \to S$ is a ring homomorphism if it respects the additive and multiplicative structures.*
$\varphi(a + b) = \varphi(a) + \varphi(b)$ $\forall a, b \in R$
$\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in R$

Definition 4.3.2. *Let R, S be rings. A map $\varphi : R \to S$ is a ring isomorphism if it is a ring homomorphism and bijective. This is denoted $\varphi : R \xrightarrow{\sim} S$. Rings R and S is isomorphic, denoted $R \cong S$ or $R \simeq S$.*

Definition 4.3.3. *The kernel of a ring homomorphism φ is defined as ker $\varphi = \varphi^{-1}(0_S) = \{a \in R | \varphi(a) = 0_S\}$.*

Remark 4.3.4. *(Examples of homomorphism)*

(i) Let R, S be rings. The map $R \to S$, $a \mapsto 0$ is a zero or trivial map / homomorphism.

(ii) Suppose R_1 is a subring of a ring R. The map $\iota : R_1 \to R$, $a \mapsto a$ is a inclusion homomorphism.

(iii) Let $n \in \mathbb{Z}$. The quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $s \mapsto \bar{s} = [s]_n$ is a quotient homomorphism between additive groups $(\mathbb{Z}, +)$ and $((Z)/n(Z), +)$.

(iv) Let X be a set, R a ring, and $X_{to}R = \{f : X \to R\}$ the ring of all maps from X to R. Fix an element $c \in R$. Then $E_c : X_{to}R \to R$; $f \mapsto E_c(f) := f(c)$ is a function evaluation map, called the Evaluation at c.

Proposition 4.3.5. *Let R, S be rings and $\varphi : R \to S$ be a ring homomorphism. Let $R_1 \subseteq R$ be a subring. Then*

(i) The φ-image $\varphi(R_1) = b \in S | b = \varphi(a)$ $for\ some$ $a \in R_1$ is a subring of S.

(ii) ker φ is a subring of R such that $\forall a \in R$, $\forall k \in$ ker $\varphi \Rightarrow ak \in$ ker φ. In other words, ker φ is a subring of R, $R($ker $\varphi) \subseteq$ ker φ and $($ker $\varphi)R \subseteq$ ker φ.

Definition 4.3.6. *Let R be a ring, $I \subseteq R$ a subset and $r \in R$. The subset $I \subseteq R$ is a left-ideal of R if:*

(i) I is a subring of R; and

(ii) *I is closed under left multiplication by elements from R:* $rI \subseteq I$ $(\forall r \in R)$*, i.e.,* $RI \subseteq I$.

Definition 4.3.7. *Let* R *be a ring,* $I \subseteq R$ *a subset and* $r \in R$*. The subset* $I \subseteq R$ *is a right-ideal of* R *if:*

(i) *I is a subring of R; and*

(ii) *I is closed under right multiplication by elements from R:* $Ir \subseteq I$ $(\forall r \in R)$*, i.e.,* $IR \subseteq I$.

Definition 4.3.8. *Let* R *be a ring,* $I \subseteq R$ *a subset and* $r \in R$*. The subset* $I \subseteq R$ *is a (two-sided) ideal of* R *if is both a left-ideal and right-ideal. In other words,* $RI \subseteq I$ *and* $IR \subseteq I$.

Proposition 4.3.9. *(Ideal Criterion) Let* R *be a ring and* I *a nonempty subset of* R*. The following are equivalent:*

(i) *I is a two-sided ideal of R;*

(ii) $\forall r \in R, \forall a, b \in R \Rightarrow ra, ar, a - b \in I$

(iii) *(If R is commutative)* $\forall r \in R, \forall a, b \in R \Rightarrow ra, a - b \in I$

(iv) *(If R is commutative with 1)* $\forall r \in R, \forall a, b \in R \Rightarrow a + rb \in I$

Proposition 4.3.10. *Let* R_α $(\alpha \in \sum)$ *be a family of subrings of a ring* R*. Let* J_α *be a left (resp. 2-sided) ideal of* R_α*. Then the intersection* $\bigcap_{\alpha \in \sum} J_\alpha$ *is a left (resp. 2-sided) ideal of the subring* $\bigcap_{\alpha \in \sum} R_\alpha$.

Corollary 4.3.11. *Let* J_α $(\alpha \in \sum)$ *be a family of left (resp. 2-sided) ideals of a ring* R*. Then the intersection* $\bigcap_{\alpha \in \sum} J_\alpha$ *is also a left (resp. 2-sided) ideal of* R.

Proposition 4.3.12. *Let* J_α $(\alpha \in \sum)$ *be a finite family of left (resp. 2-sided) ideals of a ring* R*. Then the addition* $\sum_{\alpha \in \sum} J_\alpha$ *is also a left (resp. 2-sided ideal) of* R.
More generally, if J_α $(\alpha \in \sum)$ *is an infinite (countable or uncountable) family of left (resp. 2-sided) ideals of a ring* R*, then the subset* $\{\sum x_\alpha | x_\alpha \in J_\alpha, x_\alpha \neq 0 \text{ for only finitely many } \alpha\}$ *is also a left (resp. 2-sided) ideal of* R.

Definition 4.3.13. *Let* X *be a subset of a ring* R*. Let* J_α $(\alpha \in \sum)$ *be all the ideals of* R *with* $J_\alpha \supseteq X$.
Then the intersection $\bigcap_{\alpha \in \sum} J_\alpha$ *is the ideal generated by X, denoted* (X).
This (X) *is the smallest among all ideals of* R *containing* X.
If $X = \{r_1, \ldots, r_n\}$*, then write* $(X) = (r_1, \ldots, r_n)$.

Definition 4.3.14. *For* $r \in R$*, the ideal* (r) *generated by a single element* r *is the principal ideal of ring R.*

Definition 4.3.15. *Let* R *be a ring. An ideal* I *is finitely generated if* $I = (r_1, \ldots, r_n)$ *for some* $r_i \in R$.

Proposition 4.3.16. *Let* R *be a ring;* X, Y, X_i *the subsets of* R*; and* $r_j \in R$.

(i) Let J be an ideal of R. Then $(X) \subseteq J$ if and only if $X \subseteq J$.

(ii) The equality of ideals holds: $(X_1 \cup \cdots \cup X_n) = (X_1) + \cdots + (X_n)$.

(iii) In particular, $(r_1, \ldots, r_n) = (r_1) + \cdots + (r_n)$.

Proposition 4.3.17. *Let R be a ring. Let $B \subseteq R$ and $a, a_1, \ldots, a_n \in R$.*

(i) $RB = \{\sum_{i=1}^{s} r_i b_i | r_i \in R, b_i \in B, s \geq 1\}$ is a left-ideal of R, but may not be a 2-sided ideal.

(ii) More generally, $R\{a_1, \ldots, a_n\} = Ra_1 + \cdots + Ra_n = \{\sum_{i=1}^{n} r_i a_i | r_i \in R\}$ are left-ideals of R, but they may not be 2-sided ideals.

(iii) The ideal (a) generated by a is given by $(a) = \mathbb{Z}a + aR + Ra + RaR$. An arbitrary element of (a) is of the form $ma + ar + r'a + \sum_{i=1}^{n} r_i a r_i'$ where $m \in \mathbb{Z}; r, r', r_i, r_i' \in R; n \geq 1$.

(iv) If R contains 1, then $(a) = RaR$, and an arbitrary element of (a) is of the form $\sum_{i=1}^{n} r_i a r_i'$ where $r_i, r_i' \in R; n \geq 1$.

(v) If R is commutative and contains 1, then $(a) = aR = Ra = ra | r \in R$. An arbitrary element of (a) is of the form ra where $r \in R$.

Proposition 4.3.18. *Let R be a ring with $1 \neq 0$ and I an ideal of R. Then the following are equivalent:*

(i) $I = R$

(ii) $1 \in I$

(iii) I contains a unit.

Proposition 4.3.19. *Suppose R is a ring with 1. Let $X \subseteq R$ be a subset, and $b_1, \ldots, b_n \in R$. Then*

(i) the ideal generated by X is $(X) = RXR = \left\{\sum_{i=1}^{s} r_i a_i r_i' | a_i \in X; r_i, r_i' \in R; s \geq 1\right\}$, the smallest among all ideals of R containing X.

(ii) the ideal generated by $\{b_1, \ldots, b_n\}$ is given by $(b_1, \ldots, b_n) = (b_1) + \cdots + (b_n) = Rb_1R + \cdots + Rb_nR$, the smallest among all ideals of R containing $\{b_1, \ldots, b_n\}$.

Proposition 4.3.20. *Let J_α ($\alpha \in \sum$) be a family of left (resp. 2-sided) ideals of a ring R.*

Then the inclusion is $R(\bigcup\limits_{\alpha \in \sum} J_\alpha) \subseteq \left\{\sum_{\alpha \in \sum} a_\alpha | a_\alpha \in J_\alpha; a_\alpha \neq 0 \; for \; only \; finitely \; many \alpha\right\}$, where the RHS is a left (resp. 2-sided) ideal of R, and the smallest among those of R containing all J_α, where LHS = RHS when R contains 1.

If R contains 1 and $\sum$ is finite, then $R(\bigcup\limits_{\alpha \in \sum} J_\alpha) = \sum_{\alpha \in \sum} J_\alpha$.

Proposition 4.3.21. *Let $J, J_1, \ldots, J_n$ be ideals of a ring.*

Then $J_1 \cdots J_n = \left\{\sum_{l=1}^{k} a_1(l) \cdots a_n(l) | a_i(l) \in J_i, k \geq 1\right\}$ and it is an ideal of R.

in particular, $J^n = J \cdots J = \left\{\sum_{l=1}^{k} a_1(l) \cdots a_n(l) | a_i(l) \in J, k \geq 1\right\}$ and it is an ideal of R.

Proposition 4.3.22. *Let $R = R_1 \times \cdots \times R_n$ be a direct product of rings.*

Then $S_i = \{0_{R_1}\} \times \cdots \times \{0_{R_{i-1}}\} \times R_i \times \{0_{R_{i+1}}\} \times \cdots \times \{0_{R_n}\}$ is an ideal (2-sided) of R.

Furthermore, $R = \sum_{i=1}^{n} S_i$.

Proposition 4.3.23. *Let $\varphi : R \to S$ be a ring homomorphism.*
Then ker φ is an ideal of R.

Definition 4.3.24. *Let R e a ring and $I \subseteq R$ an ideal. Then $(I, +)$ is a normal subgroup of additive group $(R, +)$. The quotient additive group is $R/I = \{\bar{r} = r + I | r \in R\}$, with well-defined addition $\bar{r} + \bar{s} := r \bar{+} s$.*

Theorem 4.3.25. *Let R be a ring and $I \subseteq R$ an ideal. Then*

(i) for cosets $\bar{r}, \bar{s} \in R/I$, the multiplication $\bar{r} \times \bar{S} := \bar{rs}$ is a well-defined binary operation on R/I, i.e., this multiplication does not depend on the choice of representatives r, s of the cosets.

(ii) $(R/I, +, \times)$ is a ring with $0_{R/I} = \bar{0_R}$.

(iii) $\bar{r} = 0_{R/I}$ ($= \bar{0_R}$) if and only if $r \in I$.

Definition 4.3.26. *Let R be a ring and $I \subseteq R$ an ideal.*
Then the ring $(R/I, +, \times)$ is the quotient ring of R by I.

Remark 4.3.27. *Let R be a ring and $(I, +)$ a subgroup of the additive group $(R, +)$.*
Then I is an ideal of R is and only if the multiplication $\times$ on the additive quotient group $(R/I, +)$ is well-defined so that $(R/I, +, \times)$ is a ring.

Definition 4.3.28. *Let R be a ring, $I \subseteq R$ an ideal, and R/I the quotient ring.*
The surjective quotient map $\gamma : R \to R/I; r \mapsto \bar{r} = r + I$ from the additive group $(R, +)$ to the additive group $(R/I, +)$ is a ring homomorphism such that ker $\gamma = I$.
The quotient ring homomorphism refers to γ.

Remark 4.3.29. *(Equivalence concepts of kernel and ideal)*
The kernel of every ring homomorphism is an ideal.
Every ideal is equal to the kernel of some (surjective) homomorphism.

Definition 4.3.30. *Let R be a commutative ring and I an ideal.*
An element $a \in R$ is nilpotent if $a^n = 0$ for some $n \geq 1$ (depending on a).
The set of all nilpotent elements of R is the nilradical of R, $nil(R) := \{a \in R | a^n = 0,\ for\ some\ n \geq 1\}$.
In fact, $nil(R)$ is an ideal of R, and $nil(R/nil(R)) = 0$.

Definition 4.3.31. *Let R be a commutative ring and I an ideal.*
The set of radical of I is $rad(I) = \{r \in R | r^n \in I,\ for\ some\ n \geq 1\}$.
In fact, $rad(I)$ is an ideal of R containing I such that $rad(I)/I = nil(R/I)$.

Definition 4.3.32. *Let R be a commutative ring and J an ideal.*

J is a radical if $rad(J) = J$. Every prime idea of R is ideal.

Definition 4.3.33. *Let R be a commutative ring and I an ideal. When R contains 1 and $I \subset R$, define $Jac(I) = \bigcap_{M:max, M \supseteq I} M$, where M runs in the set of all maximal ideals of R containing I.*

In fact, $Jac(I)$ is an ideal of R containing the radical $rad(I)$ of I.

$Jac(0)$ is the Jacobson radical of R.

Thus $Jac(I)$ is the pre-image of $Jac(0_{R/I})$ via $R \to R/I$.

Remark 4.3.34. *Let R be a commutative ring and I an ideal. Then $nil(R/I^n) \supseteq I/I^n$, and $rad(I^n) \supseteq I$ (the inclusions might be strict).*

Remark 4.3.35. *For the polynomial ring $F[x]$ over field F, if $I = (x)$ is the principal ideal generated by x, then $I^n = (x^n)$. Hence $nil(F[x]/I^n) = I/I^n$ and $rad(I^n) = I$.*

Remark 4.3.36. *The Jacobson radical of $\mathbb{Z}/12\mathbb{Z}$ is $6\mathbb{Z}/12\mathbb{Z}$, included in the intersection (of two maximal ideals) $(2\mathbb{Z}/12\mathbb{Z}) \cap (3\mathbb{Z}/12\mathbb{Z})$.*

The Jacobson radical of the polynomial ring $F[x]$ over field F is 0, which is contained in the intersection (of two maximal ideals) $(x) \cap (x-1)$.

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