Abstract Algebra Summary

Mathematical Notes

October 19, 2025

Contents

1 Groups

1.1 Definition and Basic Properties

Definition 1.1. A **group** is a set G together with a binary operation $*$ such that:

1. **Closure**: For all $a, b \in G$, $a * b \in G$
2. **Associativity**: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$
3. **Identity**: There exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
4. **Inverses**: For each $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

1.2 Abelian Groups

Definition 1.2. A group G is **abelian** (or **commutative**) if $a * b = b * a$ for all $a, b \in G$.

1.3 Order of Elements and Groups

Definition 1.3. The **order** of an element $g \in G$ is the smallest positive integer n such that $g^n = e$. If no such n exists, g has infinite order.

Definition 1.4. The **order** of a group G, denoted $|G|$, is the number of elements in G.

1.4 Subgroups

Definition 1.5. A subset H of a group G is a **subgroup** if H is itself a group under the operation of G.

Theorem 1.1 (Subgroup Test)**.** A nonempty subset H of a group G is a subgroup if and only if:

1. For all $a, b \in H$, $ab \in H$
2. For all $a \in H$, $a^{-1} \in H$

1.5 Cyclic Groups

Definition 1.6. A group G is **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

Theorem 1.2. Every cyclic group is abelian.

Theorem 1.3. If G is a cyclic group of order n, then $G \cong \mathbb{Z}_n$.

1.6 Cosets and Lagrange's Theorem

Definition 1.7. Let H be a subgroup of G and $a \in G$. The **left coset** of H containing a is $aH = \{ah : h \in H\}$. The **right coset** is $Ha = \{ha : h \in H\}$.

Theorem 1.4 (Lagrange's Theorem)**.** If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

1.7 Normal Subgroups

Definition 1.8. A subgroup N of G is **normal** if $gN = Ng$ for all $g \in G$. We write $N \triangleleft G$.

Theorem 1.5. A subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.

1.8 Quotient Groups

Definition 1.9. If N is a normal subgroup of G, then the **quotient group** G/N is the set of cosets of N in G with operation $(aN)(bN) = (ab)N$.

1.9 Homomorphisms

Definition 1.10. A **homomorphism** from group G to group H is a function $\phi : G \to H$ such that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Definition 1.11. A homomorphism $\phi : G \to H$ is:

- An **isomorphism** if it is bijective
- A **monomorphism** if it is injective
- An **epimorphism** if it is surjective

1.10 First Isomorphism Theorem

Theorem 1.6. If $\phi : G \to H$ is a homomorphism, then $\ker(\phi) \triangleleft G$ and $G/\ker(\phi) \cong \mathrm{im}(\phi)$.

2 Rings

2.1 Definition and Basic Properties

Definition 2.1. A **ring** is a set R with two binary operations $+$ and $\cdot$ such that:

1. $(R, +)$ is an abelian group
2. Multiplication is associative: $(ab)c = a(bc)$
3. Distributive laws: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$

2.2 Types of Rings

Definition 2.2. A ring R is:

- **Commutative** if $ab = ba$ for all $a, b \in R$
- A **ring with unity** if there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$
- An **integral domain** if it is commutative, has unity, and has no zero divisors
- A **field** if it is commutative, has unity, and every nonzero element has a multiplicative inverse

2.3 Subrings and Ideals

Definition 2.3. A subset S of a ring R is a **subring** if S is itself a ring under the operations of R.

Definition 2.4. A subset I of a ring R is an **ideal** if:

1. I is a subgroup of $(R, +)$
2. For all $r \in R$ and $a \in I$, both $ra \in I$ and $ar \in I$

2.4 Quotient Rings

Definition 2.5. If I is an ideal of R, then the **quotient ring** R/I is the set of cosets of I in R with operations $(a+I)+(b+I) = (a+b)+I$ and $(a+I)(b+I) = (ab)+I$.

2.5 Ring Homomorphisms

Definition 2.6. A **ring homomorphism** from ring R to ring S is a function $\phi : R \to S$ such that:

1. $\phi(a+b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

2.6 First Isomorphism Theorem for Rings

Theorem 2.1. If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R and $R/\ker(\phi) \cong \mathrm{im}(\phi)$.

3 Fields

3.1 Definition and Examples

Definition 3.1. A **field** is a commutative ring with unity in which every nonzero element has a multiplicative inverse.

Example 3.1. Examples of fields:

- $\mathbb{Q}$ (rational numbers)
- $\mathbb{R}$ (real numbers)
- $\mathbb{C}$ (complex numbers)
- $\mathbb{Z}_p$ where p is prime

3.2 Field Extensions

Definition 3.2. If F is a subfield of field E, then E is a **field extension** of F, denoted E/F.

Definition 3.3. The **degree** of extension E/F, denoted $[E : F]$, is the dimension of E as a vector space over F.

3.3 Algebraic and Transcendental Elements

Definition 3.4. An element $\alpha \in E$ is **algebraic** over F if there exists a nonzero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise, α is **transcendental**.

3.4 Minimal Polynomial

Definition 3.5. The **minimal polynomial** of α over F is the monic polynomial of least degree in $F[x]$ that has α as a root.

3.5 Finite Fields

Theorem 3.1. For every prime p and positive integer n, there exists a unique field of order p^n, denoted $\mathbb{F}_{p^n}$.

4 Polynomial Rings

4.1 Definition

Definition 4.1. The **polynomial ring** $R[x]$ over ring R is the set of all polynomials with coefficients in R.

4.2 Division Algorithm

Theorem 4.1. Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ where $\deg(r) < \deg(g)$.

4.3 Irreducible Polynomials

Definition 4.2. A polynomial $f(x) \in F[x]$ is **irreducible** over F if it cannot be factored as a product of two non-constant polynomials in $F[x]$.

4.4 Eisenstein's Criterion

Theorem 4.2. Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. If there exists a prime p such that:

1. $p \nmid a_n$
2. $p \mid a_i$ for $i = 0, 1, \ldots, n-1$
3. $p^2 \nmid a_0$

then $f(x)$ is irreducible over $\mathbb{Q}$.

5 Galois Theory

5.1 Automorphisms

Definition 5.1. An **automorphism** of field E is an isomorphism from E to itself.

Definition 5.2. The **Galois group** of extension E/F, denoted $\mathrm{Gal}(E/F)$, is the group of all automorphisms of E that fix F pointwise.

5.2 Fixed Fields

Definition 5.3. If G is a group of automorphisms of field E, then the **fixed field** of G is $\text{Fix}(G) = \{a \in E : \sigma(a) = a \text{ for all } \sigma \in G\}$.

5.3 Galois Extensions

Definition 5.4. A finite extension E/F is **Galois** if $|\text{Gal}(E/F)| = [E : F]$.

5.4 Fundamental Theorem of Galois Theory

Theorem 5.1. Let E/F be a Galois extension with Galois group G. Then there is a one-to-one correspondence between:

- Subgroups of G and intermediate fields of E/F
- Normal subgroups of G and normal extensions of F contained in E

6 Modules

6.1 Definition

Definition 6.1. Let R be a ring. A **left R-module** is an abelian group M together with a scalar multiplication $R \times M \to M$ satisfying:

1. $(r + s)m = rm + sm$
2. $r(m + n) = rm + rn$
3. $(rs)m = r(sm)$
4. $1m = m$ (if R has unity)

6.2 Submodules and Quotient Modules

Definition 6.2. A **submodule** of R-module M is a subgroup N of M such that $rn \in N$ for all $r \in R$ and $n \in N$.

Definition 6.3. If N is a submodule of M, then the **quotient module** M/N is the quotient group with scalar multiplication $r(m + N) = rm + N$.

6.3 Module Homomorphisms

Definition 6.4. An **R-module homomorphism** from M to N is a group homomorphism $\phi : M \to N$ such that $\phi(rm) = r\phi(m)$ for all $r \in R$ and $m \in M$.

7 Vector Spaces

7.1 Definition

Definition 7.1. A **vector space** over field F is an abelian group V with scalar multiplication $F \times V \to V$ satisfying the module axioms.

7.2 Basis and Dimension

Definition 7.2. A **basis** for vector space V is a linearly independent spanning set.

Theorem 7.1. Every vector space has a basis, and any two bases have the same cardinality.

Definition 7.3. The **dimension** of vector space V, denoted $\dim(V)$, is the cardinality of any basis.

7.3 Linear Transformations

Definition 7.4. A **linear transformation** from vector space V to vector space W is a function $T : V \to W$ such that:

1. $T(v + w) = T(v) + T(w)$
2. $T(cv) = cT(v)$

8 Group Actions

8.1 Definition

Definition 8.1. A **group action** of group G on set X is a function $G \times X \to X$ (denoted $(g, x) \mapsto g \cdot x$) such that:

1. $e \cdot x = x$ for all $x \in X$
2. $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$

8.2 Orbits and Stabilizers

Definition 8.2. The **orbit** of $x \in X$ under action of G is $\mathrm{Orb}(x) = \{g \cdot x : g \in G\}$.

Definition 8.3. The **stabilizer** of $x \in X$ is $\mathrm{Stab}(x) = \{g \in G : g \cdot x = x\}$.

8.3 Orbit-Stabilizer Theorem

Theorem 8.1. If G acts on X and $x \in X$, then $|\mathrm{Orb}(x)| = |G|/|\mathrm{Stab}(x)|$.

9 Sylow Theorems

9.1 Definition

Definition 9.1. Let G be a finite group and p a prime. A **Sylow p-subgroup** of G is a maximal p-subgroup of G.

9.2 First Sylow Theorem

Theorem 9.1. If G is a finite group and p divides $|G|$, then G has a Sylow p-subgroup.

9.3 Second Sylow Theorem

Theorem 9.2. All Sylow p-subgroups of G are conjugate to each other.

9.4 Third Sylow Theorem

Theorem 9.3. If G is a finite group and p divides $|G|$, then the number of Sylow p-subgroups is congruent to 1 mod p and divides $|G|$.

10 Free Groups and Presentations

10.1 Free Groups

Definition 10.1. A group F is **free** on set X if every function from X to a group G extends uniquely to a homomorphism from F to G.

10.2 Group Presentations

Definition 10.2. A **group presentation** is an expression of the form $\langle X|R\rangle$ where X is a set of generators and R is a set of relations.

11 Important Theorems

11.1 Cayley's Theorem

Theorem 11.1. Every group is isomorphic to a subgroup of a symmetric group.

11.2 Chinese Remainder Theorem

Theorem 11.2. If m and n are relatively prime integers, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

11.3 Classification of Finite Simple Groups

Theorem 11.3. Every finite simple group is one of:

- A cyclic group of prime order
- An alternating group A_n for $n \geq 5$
- A group of Lie type
- One of 26 sporadic groups

11.4 Wedderburn's Theorem

Theorem 11.4. Every finite division ring is a field.

11.5 Hilbert's Nullstellensatz

Theorem 11.5. Let k be an algebraically closed field and I an ideal in $k[x_1, \ldots, x_n]$. Then $I(V(I)) = \sqrt{I}$ where $V(I)$ is the variety of I and $\sqrt{I}$ is the radical of I.

12 Applications

12.1 Cryptography

Abstract algebra is fundamental to:

- RSA encryption (based on Euler's theorem)
- Elliptic curve cryptography
- Diffie-Hellman key exchange
- Digital signatures

12.2 Coding Theory

Applications include:

- Error-correcting codes
- Linear codes over finite fields
- Cyclic codes
- Reed-Solomon codes

12.3 Algebraic Geometry

Connections to:

- Varieties and schemes
- Commutative algebra
- Homological algebra
- Category theory

12.4 Number Theory

Applications in:

- Algebraic number theory
- Class field theory
- Modular forms
- Diophantine equations