Algebra Definition Theorem List

Hui Sun

May 4, 2025

Contents

Chapter 1

Group Theory I

This corresponds to Aluffi Chapter II.

Proposition 1.1. Let G be a group, for all $a, g, h \in G$, if

$$ga = ha$$

then $g = h$.

Proposition 1.2. Let $g \in G$ have order n, then

$$n \mid |G|$$

Corollary 1.1. If g is an element of finite order, and let $N \in \mathbb{Z}$, then

$$g^N = e \iff N \text{ is a multiple of } |g|$$

Proposition 1.3. Let $g \in G$ be of finite order, then g^m also has finite order, for all $m \geq 0$, and

$$|g^m| = \frac{\text{lcm}(m, |g|)}{m} = \frac{|g|}{\gcd(m, |g|)}$$

Proposition 1.4. If $gh = hg$, then $|gh|$ divides lcm$(|g|, |h|)$.

Definition 1.1 (Dihedral Group)**.** Let D_{2n} denote the group of symmetries of a n-sided polynomial, consisting of n rotations and n reflections about lines trhough the origin and a vertex or a midpoint of a side.

Proposition 1.5. Let $m \in \mathbb{Z}/n\mathbb{Z}$, then

$$|m| = \frac{n}{\gcd(n, m)}$$

Corollary 1.2. The element $m \in \mathbb{Z}/n\mathbb{Z}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.

Definition 1.2 (Multiplicative $(\mathbb{Z}/n\mathbb{Z})^\times$)**.** The multiplicative group of $\mathbb{Z}/n\mathbb{Z}$ is

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{m \in \mathbb{Z}/n\mathbb{Z} : \gcd(m,n) = 1\}$$

Proposition 1.6. Let $\varphi : G \to H$ be a homomorphism, and let $g \in G$ be an element of finite order, then $|\varphi(g)|$ divides $|g|$.

For example, there is no nontrivial homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$.

Proposition 1.7. There is an isomorphism between D_6 and S_3.

Proposition 1.8. Let $\varphi : G \to H$ be an isomorphism, for all $g \in G$, $|\varphi(g)| = |g|$, and G is commutative if and only if H is commutative.

Proposition 1.9. If H is commutative, then $\mathrm{Hom}(G, H)$ is a group.

Definition 1.3. Let $A = \{1, \ldots, n\}$, then the free abeliean group on A is

$$\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} = \mathbb{Z}^{\oplus n}$$

Proposition 1.10. For every set A, the free abelian group A is

$$\mathbb{Z}^{\oplus A}$$

In other words, any element in the free abelian group of A can be written as

$$\sum_{a \in A} m_a j(a)$$

where $m_a \neq 0$ for only finitely many terms, and

$$j_a(m) = \begin{cases} 1, m = a \\ 0, m \neq a \end{cases}$$

Proposition 1.11. Let $\{H_\alpha\}$ be any family of subgroups of G, then

$$\bigcap_\alpha H_\alpha$$

is a subgroup of G.

Proposition 1.12. If $\varphi : G_1 \to G_2$ is a group homomorphism, then if $H_2 \subset G_2$ is a subgroup, then

$$\varphi^{-1}(H_2)$$

is a subgroup of G_1.

Chapter 2

Group Theory II

This corresponds to Aluffi Chapter IV.

Chapter 3

Ring Theory

This corresponds to Aluffi Chapter III.

Chapter 4

Irreducibility and Factorization

This corresponds to Aluffi Chapter V.

Chapter 5

Linear Algebra I

This corresponds to Aluffi Chapter VI.

Chapter 6

Linear Algebra II

This corresponds to Aluffi Chapter VIII.

Chapter 7

Field Theory

This corresponds to Aluffi Chapter VII.

Chapter 8

Representation Theory of Finite Groups

Chapter 9

Semisimple Algebra