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 $\text{lcm}(|g|, |h|)$.

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.

Proposition 1.13. Let $H \subset \mathbb{Z}/n\mathbb{Z}$ be a subgroup, then H is generated by some m where m divides n.

Proposition 1.14. If $\varphi : G_1 \to G_2$ is a homomorphism, then $\ker(\varphi)$ is a normal subgroup.

Theorem 1.1. Let $\varphi : G_1 \to G_2$ be a surjective homomorphism, then

$$G_2 = \frac{G_1}{\ker \varphi}$$

Proposition 1.15. Let H_1, H_2 be normal subgroups of G_1, G_2, then $H_1 \times H_2$ are normal subgroups of $G_1 \times G_2$, then

$$\frac{G_1 \times G_2}{H_1 \times H_1} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}$$

For example,

$$\frac{S_3}{\mathbb{Z}/3\mathbb{Z}} = \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Proposition 1.16. Let H be a normal subgroup of G, then every subgroup containing H can be identified with a subgroup K/H of G/H.

Proposition 1.17. Let H be a normal subgroup of G, and N be a subgroup of G containing H, then N/H is normal in G/H if and only if N is normal in G, in this case

$$\frac{G/H}{N/H} = \frac{G}{N}$$

Proposition 1.18. Let H, K be subgroups of G, and if H is normal, then HK is a subgroup of G and H is normal in HK. Moreover, $H \cap K$ is normal in K, and

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

Proposition 1.19. Let H be a subgroup of G, then for all $g \in G$, the function

$$H \to gH, h \mapsto gh$$

is a bijection.

Theorem 1.2 (Lagrange). If G is a fintie group, and $H \subset G$ is a subgroup, then

$$|G| = [G : H] \cdot |H|$$

In particular, $|H|$ divides $|G|$.

Theorem 1.3 (Fermat's Little Theorem). Let p be a prime integer, and a be any integer, then

$$a^p \equiv a \mod p$$

Proposition 1.20. Any group G acts on itself by left/right multiplications, and acts on the costs G/H:

$$\varphi : g \mapsto (aH \mapsto gaH)$$

Definition 1.4 (orbit). The orbit of $a \in A$ of a group action by G is

$$O(a) = \{g \cdot a : g \in G\}$$

The stabilizer of a is the following

$$\text{Stab}_G(a) = \{g \in G : g \cdot a = a\}$$

Proposition 1.21. The orbits of an action form a partition on the set A, and G acts transitively on each orbit.

Definition 1.5 (transitive action, faithful action). An action of G on A is transitive if for all $a, b \in G$, there exists $g \in G$ such that

$$g \cdot a = b$$

In other words, the orbit of any element $a \in A$ is the entire set.

An action is faithful if for any $g \in G$,

$$g \cdot a = a \text{ for all } a$$

implies that $g = e$.

Proposition 1.22. Every transitive action of G on a set A is isomorphic to multiplication of G on G/H, where $H = \text{Stab}(a)$ for any $a \in A$.

Proposition 1.23. If $O(a)$ is an orbit of the action of a finite group G, then $O(a)$ is a finite and $|O|$ divides $|G|$. Moreover,

$$|G| = |O(a)| \cdot |\text{Stab}_G(a)|$$

For example,there is no transitive action of S_3 on the set of 5 elements.

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