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.

Proposition 2.1 (class formula)**.** Let S be a finite set, and G act on S, then

$$|S| = |Z| + \sum_{a \in A} [G : \mathsf{Stab}(a)] = |Z| + \sum_{a \in A} |O_a|$$

where $Z = \{a \in S : g \cdot a = a \text{ for all } g\}$, i.e., the fixed elements, and $A \subset S$ contains exactly one element from each nontrivial orbit of the action.

In other words, $|S|$ is the sum of the number of trivial orbits and each nontrivial orbit.

Proposition 2.2. Let G be a p-group that acts on a finite set S, then let Z be fixed elements of this acion, then

$$|S| \equiv |Z| \mod p$$

Proposition 2.3. Let G be finite, and if $G/Z(G)$ is cyclic, then G is abelian.

Definition 2.1 (centralizer, conjugacy class)**.** The centralizer $Z_G(g)$ where $g \in G$ is its stabilizer under conjugation:

$$Z_G(g) = \left\{h \in G : hgh^{-1} = g\right\}$$

The conjugacy class of $g \in G$ is the orbit $[g]$ of the conjugation action.

Proposition 2.4 (Class formula)**.** Let G be finite, then

$$|G| = |Z(G)| + \sum_{a \in A} [a]$$

where A contains one representative for each nontrivial conjugacy class.

Corollary 2.1. Let G be a nontrivial p-group, then G has a nontrivial center.

Proposition 2.5. The only possibility for the class formula of a nonabelian group of order 6 is

$$6 = 1 + 2 + 3$$

The center must be trivial if G is nonabelian.

Definition 2.2 (normalizer). Let $A \subset G$ be a subset. The normalizer $N_G(A)$ of A is

$$\text{Stab}_G(A) = \{g : gAg^{-1} = A\}$$

The centralizer of A is the subgroup $Z_G(A) \subset N_G(A)$ fixing each $a \in A$:

$$Z_G(A) = \{g : gag^{-1} = a \text{ for all } a \in A\}$$

If H is subgroup of G, every conjugate gHg^{-1} is also a subgroup of G, and all conjugate groups have the same order.

Proposition 2.6. H is a normal subgroup of G if and only if $N_G(H) = G$. More generally, the normalizer $N_G(H)$ for any subgroup H is the largest subgroup of G in which H is normal.

Proposition 2.7. Let $H \subset G$ be a subgroup, then the number of subgroups conjugate to H is equal to $[G : N_G(H)]$.

Corollary 2.2. If $[G : H]$ is finite, then the number of subgroups conjugate to H is finite, and

$$[G : H] = [G : N_G(H)] \cdot [N_G(H) : H]$$

In other words, the number of subgroups conjugate to H divides the index $[G : H]$.

Theorem 2.1 (Cauchy's Theorem). Let G be a finite group, and let p be a prime divisor of $|G|$, then G contains an element of order p.

Moreover, let N be the number of cyclic subgroups of order p, then

$$N \equiv 1 \mod p$$

Definition 2.3 (simple). A group is simple if it is nontrivial and its only normal subgroups are $\{e\}$ and G (has no nontrivial proper subgroup).

Definition 2.4 (p-Sylow subgroups). Let p be prime, a p-Sylow subgroup of a finite group G is a subgroup of order p^r, where $|G| = p^r m$, $\gcd(p, m) = 1$.

Theorem 2.2 (Sylow I). Every finite group contains a p-Sylow subgroup for all prime p. If p^k divides $|G|$, then G has a subgroup of order p^k.

Theorem 2.3 (Sylow II). Let G be finite, and P is a p-Sylow subgroup, let $H \subset G$ be a p-group, then H is contained in a conjugate of P. If P_1, P_2 are both p-Sylow subgroups, then they are conjugates to each other.

Theorem 2.4 (Sylow III). Let $|G| = p^r m$, and $\gcd(p, m) = 1$, then the number of p-Sylow subgroups is

$$n_p \mid m$$

and

$$n_p \equiv 1 \mod p$$

Proposition 2.8. Let G be a group of order mp^r, where p is prime and $1 < m < p$, then G is not simple.

Proposition 2.9. Let $p < q$ be primes, let G has order pq, if $p \nmid (q-1)$, then G is cyclic.

Proposition 2.10. Let q be an odd prime, and G be a noncommutative group of order $2q$, then

$$G \cong D_{2q}$$

Definition 2.5 (commutator subgroup). Let G be a group, the commutator subgroup of G is the subgroup **generated** by all elements

$$ghg^{-1}h^{-1}$$

Proposition 2.11. Let $[G, G]$ be the commutator subgroup of G, then $[G, G]$ is normal in G, and the quotient, also called the abelianization of G,

$$G^{\text{ab}} = \frac{G}{[G, G]}$$

is commutative.

If $\varphi : G \to H$, where H is commutative, then

$$[G, G] \subset \ker(\varphi)$$

Definition 2.6. A group G is solvable, if ther exists a sequence such that

$$\{e\} = G_0 \subset \cdots \subset G_k = G$$

where G_i is normal in G_{i+1}, and G_{i+1}/G_i is abelian, or equivalently, cyclic.

Proposition 2.12. All p-groups are solvable!

Proposition 2.13. Let N be normal in G, then G is solvable if and only if $N, G/N$ are solvable.

Proposition 2.14. Disjoint cycles commute. For every $\sigma \in S_n$, σ can be written as disjoint nontrivial cycles, unique up to rearranging.

Proposition 2.15. Two elements in S_n are conjugate in S_n if and only if they have the same type. Hence the number of conjugacy classes is the number of partitions of n as a sum.

Proposition 2.16. Normal subgroups are unions of conjugacy classes.

One can use this fact to show that there is no normal subgroup of order 30 in S_5.

Definition 2.7 (Even permutation)**.** Let $\sigma \in S_n$, then σ is even if

$$\prod_{i<j}(x_{\sigma(i)} - \sigma(j)) = \prod_{i<j}(x_i - x_j)$$

Definition 2.8. The alternating group A_n consists of even permutations of $\sigma \in S_n$, and

$$[S_n : A_n] = 2$$

Proposition 2.17. Let $\sigma \in A_n$, where $n \geq 2$, then the conjugacy class of σ in S_n splits into two conjugacy classes in A_n precisely if the type of σ consists of distinct odd numbers.

For example, the 5-cycle of S_5 splits into 2 conjugacy classes in A_5.

Proposition 2.18. The group A_5 is a simple noncommutative group of order 60

Proof. Any nontrivial normal subgroup consists of nontrivial conjugacy classes and $\{e\}$, the conjugacy classes of A_5 has the following size:

$$1, 15, 20, 12, 12$$

Thus any subgroup of G, i.e., order that divides 60 cannot be written as a sum of the numbers above. $\square$

Proposition 2.19. The alternating group is generated by 3-cycles.

Proposition 2.20. Let $n \geq 5$, if a normal subgroup of A_n contains a 3-cycle, then it contaisn all 3-cycles.

Proof. It suffices to note that the 3 cycles form a conjugacy class that doesn't split from S_n to A_n. $\square$

Theorem 2.5. The alternating group is simple for $n \geq 5$.

As a corollary, S_n is not solvable for $n \geq 5$.

Proposition 2.21. Let N, H be normal subgroups of G, then

$$[N, H] \subset N \cap H$$

where $[N, H]$ is the commutator of N, H.

Proposition 2.22. Let N, H be normal subgroups, and $N \cap H = \{e\}$, then N, H commute with each other.

Theorem 2.6. Let N, H be normal subgroups of G, such that $N \cap H = \{e\}$, then

$$NH \cong N \times H$$

Definition 2.9 (Short exact sequence). A short exact sequence of groups is a sequence:

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$$

where ψ surjective and φ is injective, and N is normal in φ which induces an isomorphism $G/N \cong H$.

A SES splits if H is identified with a subgroup of G such that

$$N \cap H = \{e\}$$

Definition 2.10 (semidirect product). Let N be a normal subgroup, and let $\theta : H \to \mathrm{Aut}(N)$, then define an operator $\cdot_\theta$ as

$$(n_1, h_1) \cdot_\theta (n_2, h_2) = (n_1\theta(h_1)(n_2), h_1h_2)$$

The semidirect product of $N \rtimes_\theta$ is the group $N \times H$ with operator $\cdot_\theta$.

Theorem 2.7. Let N, H be groups, and $\theta : H \to \mathrm{Aut}(N)$, let $G = N \rtimes_\theta H$, then

1. G contains isomorphic copies of N, H.
2. The natural projection $G \to H$ is surjective, with kernel N, thus N is normal in G and the sequence
$$1 \longrightarrow N \longrightarrow N \rtimes_\theta H \longrightarrow H \longrightarrow 1$$
is split exact.
3. $N \cap H = \{e\}$.
4. $G = NH$.
5. The homomorphism is conjugation:
$$\theta(h)(n) = hnh^{-1}$$

Proposition 2.23. Let N, H be subgroups, and N is normal, suppose that $N \cap H = \{e\}$, and $G = NH$, then let $\theta : H \to \mathrm{Aut}(N)$ be

$$\theta(h)n = nhn^{-1}$$

Then

$$G \cong N \rtimes_\theta H$$

Proposition 2.24. Let G be abelian, let H, K be subgroups such that $|H|, |N|$ are relatively prime, then

$$H + K \cong H \oplus K$$

Proof. Lagrange. □

Proposition 2.25. Every finite abelian group is a direct sum of its nontrivial Sylow subgroups.

Proposition 2.26. Let p be prime, and $r \geq 1$, let G be a noncyclic abelian group of order p^{r+1}, then let $g \in G$ be an element of order p^r, then there exists an element $h \in G$ such that $h \notin \langle g \rangle$, such that $|h| = p$.

If G is finite and abelian, then G is a direct sum of cyclic groups, which may be assumed to be cyclic p-groups.

Theorem 2.8. Let G be finite nontrivial abelian group, then there exists prime integers $p_1, \ldots, p_r$, and positive integers $n_{i(j)}$ such that

$$G = \bigoplus_{i,j} \frac{\mathbb{Z}}{p_i^{n_{i(j)}}\mathbb{Z}}$$

There exists positive integers $1 < d_1 \mid \cdots \mid d_s$ such that $|G| = d_1 \ldots d_s$, and

$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_s\mathbb{Z}}$$

Theorem 2.9. Let F be a field, and G be a finite subgroup of the multiplicative group $(F^\times, \cdot)$, then G is cyclic.

Chapter 3

Ring Theory

This corresponds to Aluffi Chapter III.

Definition 3.1 (zero-divisor)**.** An element $a \in R$ is a (left) zero-divisor if there exists $b \neq 0$ such that

$$ab = 0$$

Proposition 3.1. In a ring R, $a \in R$ is not a left zero-divisor if and only if the left multiplication by a is injective.

Definition 3.2 (integral domain)**.** An ID is a nonzero commutative ring such that for all $a, b \in R$,

$$ab = 0$$

implies $a = 0$ or $b = 0$. In other words, IDs are commutative rings without zero divisors.

Proposition 3.2. In a ring R:

1. u is left unit iff the left multiplication by u is surjective.
2. If u is a left unit, then the right multiplication by u is injective, i.e., u is not a right zero-divisor.

Definition 3.3 (division ring)**.** A division ring is a ring in which every nonzero element is a unit.
A field is a nonzero commutative ring in which every nonzero element is a unit.

Proposition 3.3. Assume R is a finite commutative ring, then R is an integral domain if and only if R is a field.

Proposition 3.4. $\mathrm{End}_{\mathrm{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$

Theorem 3.1. Let I be a two-sided ideal of a ring R. Then for every ring homomorphism $\varphi : R \to S$ such that $I \subset \ker \varphi$ there exists a unique ring homomorphism $\tilde{\varphi} : R/I \to S$ so that the diagram commutes:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

Theorem 3.2. Let $\varphi : R \to S$ be a surjective ring homomorphism, then

$$S \cong \frac{R}{\ker(\varphi)}$$

Proposition 3.5. Let I be an ideal of a ring R, and let J be an ideal of R containing I, then J/I is an ideal of R/I, and

$$\frac{R/I}{J/I} = \frac{R}{J}$$

Definition 3.4 (Noetherian). A commutative ring R is Noetherian if every ideal of R is finitely generated. An ideal I is finitely generated if $I = (a_1, \ldots, a_n)$, i.e., every element in I can be written as

$$r_1 a_1 + \cdots + r_n a_n$$

for some $r_1, \ldots, r_n \in R$.

Definition 3.5. I is a prime ideal if R/I is an integral domain, and is a maximal ideal if R/I is a field.

Proposition 3.6. Let I be an ideal of commutative R, if R/I is finite, then I is prime if and only if maximal.

Proposition 3.7. Let R be a PID, a nonzero ideal I is prime if and only if it is maximal.

Definition 3.6 (module). A R-module M is an abelian group with a ring action, satisfying:

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

Definition 3.7. An R-algebra is a ring with a ring R action.

Theorem 3.3. Suppose $\varphi : M \to M'$ be a surjective R-module homomorphism, then

$$M' \cong \frac{M}{\ker \varphi}$$

Proposition 3.8. Let N be a submodule of an R-module M, and let P be a submodule of M containing N. Then P/N is a submodule of M/N, and

$$\frac{M/N}{P/N} \cong \frac{M}{P}$$

Proposition 3.9. Let N, P be submodules, then $N+P$ is a submodule of M, and $N \cap P$ is a submodule of P, and

$$\frac{N+P}{N} \cong \frac{P}{N \cap P}$$

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