

Algebra Definition Theorem List

Hui Sun

August 7, 2025

Contents

1	Category Theory	3
2	Group Theory I	4
3	Group Theory II	8
3.1	Conjugation Action	8
3.2	Sylow	10
3.3	Series and Solvability	11
3.4	S_n and A_n	12
3.5	Product of Groups	13
3.6	Classification of Finite Abelian Groups	14
4	Ring Theory	15
4.1	Modules	18
4.2	Free Modules	19
5	Ring Theory II	22
6	Linear Algebra I	26
7	Field Theory	27
7.1	Finite fields	29
7.2	Cyclotomic	29
8	Linear Algebra II	32
9	Field Theory	33
10	Representation Theory of Finite Groups	34
11	Semisimple Algebra	35

Chapter 1

Category Theory

Definition 1.1 (*initial, final*). Let \mathcal{C} be a category, then object I is initial if for every object A , there exists a unique morphism $I \rightarrow A$. We say F is final if for every A , there exists a unique morphism $A \rightarrow F$.

Chapter 2

Group Theory I

This corresponds to Aluffi Chapter II.

Proposition 2.1. Let G be a group, for all $a, g, h \in G$, if

$$ga = ha$$

then $g = h$.

Proposition 2.2. Let $g \in G$ have order n , then

$$n \mid |G|$$

Corollary 2.1. 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 2.3. 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 2.4. If $gh = hg$, then $|gh|$ divides $\text{lcm}(|g|, |h|)$.

Definition 2.1 (Dihedral Group). Let D_{2n} denote the group of symmetries of a n -sided polygon, consisting of n rotations and n reflections about lines through the origin and a vertex or a midpoint of a side.

Proposition 2.5. Let $m \in \mathbb{Z}/n\mathbb{Z}$, then

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

Corollary 2.2. The element $m \in \mathbb{Z}/n\mathbb{Z}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.

Definition 2.2 (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 2.6. Let $\varphi : G \rightarrow H$ 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 2.7. There is an isomorphism between D_6 and S_3 .

Proposition 2.8. Let $\varphi : G \rightarrow H$ be an isomorphism, for all $g \in G$, $|\varphi(g)| = |g|$, and G is commutative if and only if H is commutative.

Proposition 2.9. If H is commutative, then $\text{Hom}(G, H)$ is a group.

Definition 2.3. Let $A = \{1, \dots, n\}$, then the free abelian group on A is

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

Proposition 2.10. Let $\{H_\alpha\}$ be any family of subgroups of G , then

$$\bigcap_{\alpha} H_{\alpha}$$

is a subgroup of G .

Proposition 2.11. If $\varphi : G_1 \rightarrow G_2$ 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 2.12. Let $H \subset \mathbb{Z}/n\mathbb{Z}$ be a subgroup, then H is generated by some m where m divides n .

Proposition 2.13. If $\varphi : G_1 \rightarrow G_2$ is a homomorphism, then $\ker(\varphi)$ is a normal subgroup.

Theorem 2.1. Let $\varphi : G_1 \rightarrow G_2$ be a surjective homomorphism, then

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

Proposition 2.14. 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

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

For example,

$$\frac{\mathbb{Z}/6\mathbb{Z}}{\mathbb{Z}/3\mathbb{Z}} = \mathbb{Z}/2\mathbb{Z}$$

Proposition 2.15. Let H be a normal subgroup of G , then every subgroup K containing H , K/H can be identified with a subgroup of G/H .

Proposition 2.16. 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 2.17. 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 2.18. Let H be a subgroup of G , then for all $g \in G$, the function $H \rightarrow gH$ such that

$$h \mapsto gh$$

is a bijection.

Theorem 2.2 (Lagrange). If G is a finite group, and $H \subset G$ is a subgroup, then

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

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

Theorem 2.3 (Fermat's Little Theorem). Let p be a prime integer, and a be any integer, then

$$a^p \equiv a \pmod{p}$$

Proposition 2.19. Any group G acts on itself by left/right multiplications, and acts on the cosets G/H :

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

Definition 2.4 (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 2.20. The orbits of an action form a partition on the set A , and G acts transitively on each orbit.

Definition 2.5 (transitive action, faithful action). An action of G on A is transitive if for all $a, b \in A$, 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 2.21. 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 2.22. 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 3

Group Theory II

This corresponds to Aluffi Chapter IV.

Proposition 3.1. Every **transitive** action of a group G on a set S is isomorphic to the left multiplication on the cosets G/H . Here, H can be taken to be the stabilizer of any element $a \in S$.

Moreover, suppose G is finite, then

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

for any $a \in S$. (The size of the orbit must divide $|G|$.)

Proposition 3.2 (class formula). Let S be a finite set, and G act on S , then

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

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

$$|S| \equiv |Z| \pmod{p}$$



Warning 3.1. The important takeaway is that each summand on the right, $|O_a|$ divides $|G|$.

3.1 Conjugation Action

Definition 3.1 (fixed points, centralizer, conjugacy class). The fixed points under the conjugation action is the center of G . The centralizer $Z_G(g)$ where $g \in G$ is its stabilizer under conjugation:

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

The conjugacy class of $g \in G$ is the orbit $[g]$. (In other words, centralizer is the set of elements that commute with g .)

For arbitrary $a \in G$, we have

$$Z(G) \subset Z_G(a)$$

Moreover, a is the only element in $[a]$ iff $a \in Z(G)$.

Proposition 3.4. The center is the set of fixed points of G under the conjugation action, the conjugacy classes are the orbits.

Theorem 3.2. Let G be finite, and if $G/Z(G)$ is cyclic, then G is abelian.

Proof. One can show that every element $a \in G$ can be written as

$$a = g^r z$$

for some $z \in Z(G)$, then compute $ab = ba$. □

Proposition 3.5 (Class formula). Let G be finite, then

$$\begin{aligned} |G| &= |Z(G)| + \sum_{[a] \in A} |[a]| \\ &= |Z(G)| + \sum_a [G : Z_G(a)] \end{aligned}$$

where A contains one representative for each nontrivial conjugacy class.



Warning 3.3. There are many consequences of the class formula, showing center is nontrivial, etc. Mainly using the summand divides $|G|$!

Theorem 3.4. Let G be a nontrivial p -group, then G has a nontrivial center.

Proposition 3.6. Let G be a group of p^2 elements, where p is prime, then G is commutative.

Proposition 3.7. 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.

Proposition 3.8. Normal subgroups are unions of conjugacy classes. Thus, a noncommutative group of order 6 cannot have a normal subgroup of order 2.

It contains the identity, and there is no other conjugacy class of size 1.

Definition 3.2 (normalizer). Let $A \subset G$ be a subset. The normalizer $N_G(A)$ of A is

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

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

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

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

Proposition 3.9 (*). H is a normal in G if and only if $N_G(H) = G$. More generally, the normalizer $N_G(H)$ for any subgroup H is the largest subgroup such that H is normal in $N_G(H)$.

Proposition 3.10 (*). Let $H \subset G$ be a subgroup, then the number of subgroups conjugate to H is the size of the orbit=index of the stabilizer, which is $[G : N_G(H)]$.

Corollary 3.1. 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 $[G : H]$.

3.2 Sylow

Theorem 3.5 (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

$$N \equiv 1 \pmod{p}$$

Definition 3.3 (simple). A group is simple if it is nontrivial and its only normal subgroups are $\{e\}$ and G (has no nontrivial proper subgroup).

Definition 3.4 (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 3.6 (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 3.7 (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 3.8 (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

$$n_p \equiv 1 \pmod{p}$$

Proposition 3.11. Let G be a finite group, let P be a p -Sylow subgroup, the number of p -Sylow subgroup n_p is

$$n_p = [G : N_G(P)]$$

by definition.

Proposition 3.12. Let G be a group of order mp^r , where p is prime and $1 < m < p$, then G is not simple.

Proposition 3.13 (*). Let $p < q$ be primes, let G has order pq , if $p \nmid (q - 1)$, then G is cyclic.

Proof. If G is abelian, use elements of orders p, q . If G not necessarily abelian, then use the conjugation action. \square

Proposition 3.14 (*). Let q be an odd prime, and G be a noncommutative group of order $2q$, then

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

3.3 Series and Solvability

Definition 3.5 (composition series). A comp series for G is a normal series

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

such that G_{i+1}/G_i is simple.

Definition 3.6 (commutator subgroup). Let G be a group, the commutator subgroup of G is the subgroup **generated** by all elements

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

Proposition 3.15. 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 $\varphi : G \rightarrow H$, where H is commutative, then

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

Definition 3.7. A group G is solvable, if there 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 3.16. All p -groups are solvable!

Proposition 3.17. Let N be normal in G , then G is solvable if and only if $N, G/N$ are solvable.

3.4 S_n and A_n

Proposition 3.18. Disjoint cycles commute. For every $\sigma \in S_n$, σ can be written as disjoint nontrivial cycles, unique up to rearranging.

Proposition 3.19. 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 3.20. Let $\sigma \in S_n$, and $(a_1 \dots a_n)$ is a cycle in S_n , then

$$\sigma(a_1 \dots a_n)\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_n))$$

Proof: try $\varphi(a_1)$ on the left hand side.



Warning 3.9. Very useful!

Example 3.1. In S_4 , we have

$$(1234)(12)(1234)^{-1} = (23)$$

Definition 3.8 (Even permutation). Let $\sigma \in S_n$, then σ is even if

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

Proposition 3.21. A_n is always normal in S_n , because it is the kernel of the $\varepsilon : S_n \rightarrow \{\pm 1\}$ (determining parity).

Proposition 3.22. 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; or equivalently, the centralizer of σ is contained A_n . Otherwise, the conjugacy class stays the same.

Example 3.2. S_5 has even permutations 5, 3, 2+2, 1, and only 5-cycle of S_5 splits into 2 conjugacy classes in A_5 .

Proposition 3.23. The group A_5 is a simple noncommutative group of order 60.

Proposition 3.24. Every simple group of order < 60 is commutative, A_5 is the smallest simple group that is not commutative.

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 3.25. The alternating group is generated by 3-cycles.

Proposition 3.26. Let $n \geq 5$, if a normal subgroup of A_n contains a 3-cycle, then it contains 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

Proposition 3.27. The alternating group A_n is simple for $n \geq 5$. As a result, S_n is not solvable for $n \geq 5$.

3.5 Product of Groups

Proposition 3.28. Let N, H be normal subgroups of G , let $[N, H]$ be the commutator of N, H , then

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

Thus if $N \cap H = \{e\}$, then N, H commute with each other.

A stronger statement is the following:

Theorem 3.10. Let N, H be normal subgroups of G , such that $N \cap H = \{e\}$, then

$$NH \cong N \times H$$

Definition 3.9 (Split Short exact sequence). A short exact sequence of groups is a sequence:

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

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

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

Definition 3.10 (semidirect product). Let N be a normal subgroup, and let $\theta : H \rightarrow \text{Aut}(N)$, then define an operator \cdot_θ on $N \times H$ as

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

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

Proposition 3.29. Let N, H be subgroups, and N is normal, suppose that $N \cap H = \{e\}$, and $G = NH$, then let $\theta : H \rightarrow \text{Aut}(N)$ be $\theta \mapsto \theta_h$, and

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

Then

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

(Recall that the operation defined on $N \rtimes_{\theta} H$ is $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \theta_{h_1}(n_2), h_1 h_2)$).

Proposition 3.30. Let G be a noncommutative group of order pq , then there is exactly one group up to isomorphism.

3.6 Classification of Finite Abelian Groups

Proposition 3.31. Let G be abelian, let H, K be subgroups such that $|H|, |K|$ are relatively prime, then

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

Proof. Lagrange: $N \cap H = \{e\}$. □

Proposition 3.32. Every finite abelian group is a direct sum of its nontrivial Sylow subgroups.

Theorem 3.11. If G is finite and abelian, then G is a direct sum of cyclic p -groups.

Theorem 3.12. Let G be finite nontrivial abelian group, then there exists prime integers p_1, \dots, 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 $1 < d_1 \mid \dots \mid d_s$ such that $|G| = d_1 \dots d_s$, and

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

Example 3.3. Finite abelian group of order 360 has 6 isomorphism classes.

Theorem 3.13. Let F be a field, and G be a finite subgroup of the multiplicative group (F^{\times}, \cdot) , then G is cyclic.

Proof. Hard proof. Don't torture yourself. □

Chapter 4

Ring Theory

This corresponds to Aluffi Chapter III.

Definition 4.1 (free action). An action by G is free if there exists $x \in X$ such that $gx = x$ then $g = e$.

Definition 4.2 (faithful action). An action by G is faithful if $gx = x$ for all $x \in X$ implies that $g = e$.

Definition 4.3 (zero-divisor). An element $a \in R$ is a (left) zero-divisor if there exists $b \neq 0$ such that

$$ab = 0$$

Proposition 4.1. 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 4.4 (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. Equivalently, if $a, b \neq 0$, then $ab \neq 0$.

Proposition 4.2. 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.

Notice that in a commutative ring, this means u is a unit iff multiplication by u is bijective.

Definition 4.5 (division ring, field). 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 4.3. The group of units in $\mathbb{Z}/n\mathbb{Z}$ is exactly the group $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. m is a unit iff multiplication by m is surjective, iff m generates $\mathbb{Z}/n\mathbb{Z}$, iff $m \in (\mathbb{Z}/n\mathbb{Z})^*$. □

Definition 4.6 (Power Series Ring). The power series ring

$$\sum_{i=0}^{\infty} a_i x^i$$

is denoted by $R[[x]]$.

Definition 4.7 (Monoid Ring). Given a monoid M and a ring R , the elements

$$\sum_{m \in M} a_m \cdot m$$

where $a_m \in R$ and $a_m \neq 0$ for finitely many terms, forms a ring denoted as $R[M]$.

Proposition 4.4. Assume R is a finite commutative ring, then R is an integral domain if and only if R is a field.

Proposition 4.5. $\text{End}_{\text{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$, where $\text{End}_{\text{Ab}}(G) = \text{Hom}_{\text{Ab}}(G, G)$ where G is abelian.

Proof. $\varphi \mapsto \varphi(1)$. □

Theorem 4.1. Let I be a two-sided ideal of a ring R . Then for every ring homomorphism $\varphi : R \rightarrow S$ such that $I \subset \ker \varphi$ there exists a unique ring homomorphism $\tilde{\varphi} : R/I \rightarrow S$ so that the diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \pi \downarrow & \nearrow \tilde{\varphi} & \\ R/I & & \end{array}$$

Theorem 4.2. Let $\varphi : R \rightarrow S$ be a surjective ring homomorphism, then

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

Proposition 4.6. 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 4.8 (Noetherian). A commutative ring R is Noetherian if every ideal of R is finitely generated. An ideal I is finitely generated if $I = (a_1, \dots, a_n)$, i.e., every element in I can be written as

$$r_1 a_1 + \dots + r_n a_n$$

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

Proposition 4.7. Let \bar{b} be the class of b in $R/(a)$, then

$$\frac{R/(a)}{(\bar{b})} \cong \frac{R}{(a, b)}$$

Proposition 4.8. \mathbb{Z} is a PID by taking the smallest positive element d in each ideal, obtaining (d) .

Definition 4.9. I is a prime ideal if R/I is an integral domain, and is a maximal ideal if R/I is a field.

Definition 4.10. Let I, J be ideals of R , then IJ is the ideal **generated** by elements $ij, i \in I, j \in J$.
Note that $IJ \subset I \cap J$.

Example 4.1. In \mathbb{Z} :

$$(4) \cap (3) = (12)$$

and

$$(4) \cap (6) = (12)$$

Definition 4.11 (Long division). Let $f(x) \in R[x]$ be monic, if $g(x) \in R[x]$ be another polynomial, then there exists unique $q, r \in R[x]$, where $\deg(r) < \deg(f)$, such that

$$g(x) = f(x)q(x) + r(x)$$

Moreover,

$$g(x) + (f(x)) = r(x) + (f(x))$$

as cosets of $(f(x))$.

Proposition 4.9. Let I be an ideal of commutative R , if R/I is finite, then I is prime if and only if maximal.

Proposition 4.10. Let R be a PID, a nonzero ideal I is prime if and only if it is maximal.

Proof. Is simple proof, you just do it. □

Theorem 4.3. Let R be commutative, let $f(x) \in R[x]$ be a monic polynomial of degree d , then

$$\varphi : R[x] \rightarrow R^{\oplus d}$$

where

$$\varphi : g(x) \mapsto r(x)$$

where $r(x)$ is the remainder $g(x) = f(x)q(x) + r(x)$ induces an isomorphism of **groups**:

$$\frac{R[x]}{(f(x))} \cong R^{\oplus d}$$

Ring Structure: can be induced by the map φ .

Example 4.2. Let $f(x) = x - a$ for some $a \in R$, then

$$\frac{R[x]}{(x - a)} \cong R$$

Example 4.3. Let $f(x) = x^2 + 1$, then there is isomorphism of groups:

$$R \oplus R \cong \frac{R[x]}{(x^2 + 1)}$$

note that elements on the right are of the form $a_0 + a_1x$. One can give a ring structure on $R \oplus R$ by φ .

Example 4.4. The ideal $(2, x)$ is maximal in $\mathbb{Z}[x]$.

Example 4.5. The maximal ideals in $\mathbb{C}[x]$ are precisely

$$(x - a)$$

where $a \in \mathbb{C}$.

Definition 4.12 (Krull dimension). Let R be commutative, the Krull dimension is the length of the longest chain of prime ideals in R . For example, PIDs but not fields have Krull dimension 1.

$$(0) \subset (d)$$

has length 1.

Moreover, $k[x_1, \dots, x_n]$ have Krull dimension n :

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \dots (x_1, \dots, x_n)$$

4.1 Modules

Definition 4.13 (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. $1m = m$.

A **submodule** N of M is an abelian group such that for all $r \in R, n \in N$,

$$rn \in N$$

A **homomorphism** of R -modules $\varphi : M \rightarrow M'$ is such that

$$\begin{cases} \varphi(m + n) = \varphi(m) + \varphi(n) \\ \varphi(rm) = r\varphi(m) \end{cases}$$

Let $R = k$ be a field, then R -modules are called vector spaces over k .

Definition 4.14. Let $r \in M$ be in the center of M , then

$$rM = \{rm : m \in M\}$$

is a submodule of M . If I is an ideal of R , then

$$IM = \left\{ \sum_i r_i m_i : r_i \in I, m_i \in M \right\}$$

i.e., generated by $rm, r \in I$ is a submodule.

Example 4.6. If R is not commutative, then R/I is not a ring, where I is a left ideal, but is defined as a left-module. The multiplication given by $r(a + I) = ra + I$.

Definition 4.15. An R -algebra is a ring with a ring R action.

Theorem 4.4. Suppose $\varphi : M \rightarrow M'$ be a surjective R -module homomorphism, then

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

Proposition 4.11. 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 4.12. Let N, P be submodules, then $N + P$ is a submodule of M , and $N \cap P$ is a submodule of P , and

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

4.2 Free Modules

Definition 4.16. Let A be a set, then

$$F^R(A) \cong R^{\oplus A}$$

where $F^R(A)$ denotes the free modules over A . Every element is written as

$$\sum_{a \in A} r_a a$$

(always a finite sum). We say a module $M = \langle A \rangle$ is finitely generated if A is finite.

Example 4.7. Let $R = \mathbb{Z}[x_1, \dots, x_n]$, when R viewed as a R -module over itself, it is finitely generated (by 1), by the ideal

$$(x_1, x_2, \dots)$$

as an R -module, is not finitely generated.

Definition 4.17 (Noetherian Modules). An R -module is Noetherian if every submodule of M is finitely generated as an R -module.

Proposition 4.13. Let M be an R -module, N be a submodule, then M is Noetherian iff $N, M/N$ are both Noetherian.

Definition 4.18 (finite, finite-type R -algebra). Let S be an R -algebra, it is called **finite** if it is finitely generated as an R -module; equivalently,

$$S \cong \frac{R^{\oplus n}}{M}$$

for some submodule M .

An R -algebra S is called **finite-type** if it is finitely generated as an R -algebra, i.e.,

$$S \cong \frac{R[x_1, \dots, x_n]}{I}$$

for some ideal I .

Elements in finite R -algebra is of the form:

$$\sum_{i=1}^n r_i s_i$$

where $S = \langle s_1, \dots, s_n \rangle$. Elements in finite-type R -algebra is of the form:

$$r_{11}s_1 + r_{12}s_1^2 + \dots + r_{21}s_2 + r_{22}s_2^2 + \dots + r_{nk}s_n^k$$

Proposition 4.14. The polynomial ring $R[x]$ is finite-type, not finite.

Proposition 4.15. Let R be a PID, and F be a finitely generated free module over R , and let $M \subset F$ be a submodule, then M is free.

Definition 4.19 (???). Let R be an integral domain, the rank of M is the maximal number of linearly independent elements of M .

Definition 4.20 (SES, split). A sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is short exact iff f is injective, g is surjective, and

$$\ker(g) = \operatorname{im}(f)$$

A SES is said to **split** if it is isomorphic in a sense that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \uparrow \cong & & \uparrow \cong & & \uparrow \cong & & \\ 0 & \longrightarrow & A' & \longrightarrow & A \oplus C & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

Chapter 5

Ring Theory II

This corresponds to Aluffi Chapter V.

Proposition 5.1. Let R be commutative, and M be an R -module, then the following are equivalent:

1. M is Noetherian: every submodule of M is finitely generated.
2. Every ascending chain of submodules of M stabilizes: no infinite strict inclusions of submodules.
3. Every nonempty family of submodules has a maximal element with respect to inclusion.

Proposition 5.2 (*). Let R be a Noetherian ring, then $R[x_1, \dots, x_n]$ is Noetherian. Let J be an ideal of the polynomial ring $R[x_1, \dots, x_n]$, then the ring

$$\frac{R[x_1, \dots, x_n]}{J}$$

is Noetherian, so is $R[x_1, \dots, x_n]$.

Proposition 5.3 (Hilbert's basis theorem). If R is Noetherian, then $R[x]$ is also Noetherian.

Definition 5.1 (prime, irreducible elements). Let R be an integral domain, an element $a \in R$ is prime if the ideal (a) is prime, i.e., a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$. ($a \mid b$ if $b \in (a)$.)

An element $a \in R$ is irreducible if a is not a unit and

$$a = bc$$

implies b is a unit or c is a unit. Equivalently, a is irreducible if $(a) \subset (b)$ implies $(b) = (a)$ or $(b) = (1) = R$, i.e., (a) is maximal in principal ideals.

Proposition 5.4. Let R be an integral domain, and let $a \in R$ be a nonzero prime element, then a is irreducible.

Proposition 5.5. Let R be an integral domain, and let r be a nonzero, nonunit element of R . Assume that every ascending chain of principal ideals,

$$(r) \subset (r_1) \subset \dots$$

stabilizes. Then r has a factorization into irreducibles.

Corollary 5.1. Let R be a Noetherian ring, then factorizations exist in R .
A non-Noetherian ring but factorization still exists:

$$\mathbb{Z}[x_1, \dots, x_n]$$

Proposition 5.6. Let R be a UFD, and $a, b, c \in R$ be nonzero, then

$$(a) \subset (b)$$

iff the multiset of irreducible factors of b is contained in that of a . Moreover, the irreducible factors of bc are the collection of irreducible factors of b and c .

Proposition 5.7. Let R be a UFD, let a, b be nonzero elements, then a, b have a greatest common divisor, i.e., the smallest ideal (d) such that $(a, b) \subset (d)$.

Proposition 5.8 (*). In UFD, a is irreducible implies a is prime.

Theorem 5.1 (*). An integral domain R is a UFD if and only if

1. The acc holds for principal ideals in R .
2. Every irreducible element of R is prime.

Proposition 5.9. If R is a PID, then it is a UFD. (Hence irreducibles are primes).
($\mathbb{Z}[x]$ is not a PID).

Definition 5.2 (Euclidean domain). A Euclidean valuation on an integral domain R is an valuation: for all $a \in R$, and all nonzero $b \in R$, there exists q, r such that

$$a = qb + r$$

with either $r = 0$ or $v(r) < v(b)$. An integral domain is a ED if it admits a Euclidean valuation.

Proposition 5.10. ED is also PID.

Definition 5.3 (*Field of fractions). Let R be an integral domain, then the field of fractions is

$$K(R) = \left\{ \frac{a}{r} : a, r \in R, r \neq 0 \right\}$$

Definition 5.4. (Assuming R is an integral domain). The field of rational functions with coefficients in R is the field of fractions of the ring $R[x]$, denoted as $R(x)$.

Theorem 5.2. Let R be a UFD, then $R[x]$ is also a UFD.

Proposition 5.11. Let R be a UFD, and K be its field of fractions, let $f \in R[x]$ be a nonconstant, irreducible polynomial, then f is irreducible as an element in $K[x]$.

Definition 5.5. Let R be a commutative ring, let $f \in R[x]$, then f is primitive if for all principal prime ideals p ,

$$f \notin pR[x]$$

where $pR[x]$ is an ideal of $R[x]$ of polynomials with coefficients from p .

Proposition 5.12 (*). Let R be a UFD, f is primitive if and only if $\gcd(a_0, \dots, a_d) = 1$.

Definition 5.6. Let R be a UFD. The content of a nonzero polynomial $f \in R[x]$ denoted by

$$\text{cont}(f) = \gcd(a_0, \dots, a_n)$$

The principal ideal generated by $(\text{cont}(f))$ is uniquely determined by f .

Proposition 5.13 (Gauss's lemma). Let R be a UFD. Let $f, g \in R[x]$, then

$$(\text{cont}(fg)) = (\text{cont}(f))(\text{cont}(g))$$

Proposition 5.14. Let R be a UFD, and K be its field of fractions. Let $f \in R[x]$ be nonconstant, then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$ and $\gcd(a_0, \dots, a_n) = 1$

Proposition 5.15. Let k be field, $f \in k[x]$ of degree 2 or 3 is irreducible iff it has a root in k .

Proposition 5.16. Let R be a UFD, K its field of fractions. Let

$$f(x) = a_0 + \dots + a_n x^n \in R[x]$$

let $c = \frac{p}{q} \in K$ be a root of f , then $p \mid a_0$ and $q \mid a_n$. (Note p/q is written in the minimal form).

Proposition 5.17. Let k be a field, $f(t) \in k[t]$, be irreducible, then

$$F = \frac{k[t]}{(f(t))}$$

is a field.

Definition 5.7. A field is algebraically closed if all the irreducible polynomials in $k[x]$ have degree 1.

Proposition 5.18. Every polynomial $f \in R[x]$ of degree ≥ 3 is reducible.

Proposition 5.19. Let $f \in \mathbb{Z}[x]$ be a polynomial such $\gcd(a_0, \dots, a_n) = 1$ then let p be a prime integer. Assume $f \pmod p$ has the same degree as f and is irreducible over $\mathbb{Z}/p\mathbb{Z}$, then f is irreducible over \mathbb{Z} .

Proposition 5.20 (Generalized Eisenstein). Let R be a commutative ring, let p be a prime ideal in R , let $f \in R[x]$, assume that

1. $a_n \notin p$.
2. $a_i \in p$.
3. $a_0 \notin p^2$.

then f is not the product of polynomials with degree strictly less than $\deg(f)$.

Theorem 5.3 (CRT). Let I_1, \dots, I_k be ideals of R such that $I_i + I_j = (1)$ for all $i \neq j$. Then

$$\frac{R}{I_1 \cap \dots \cap I_k} \cong \frac{R}{I_1} \times \dots \times \frac{R}{I_k}$$

(It uses if $I_i + I_j = (1)$, then $I_1 \dots I_k = I_1 \cap \dots \cap I_k$).

Corollary 5.2. Let R be a PID, and let a_1, \dots, a_k be elements such that $\gcd(a_i, a_j) = 1$, let $a = a_1 \dots a_k$, then

$$\frac{R}{(a)} \cong \frac{R}{(a_1)} \times \dots \times \frac{R}{(a_k)}$$

Proposition 5.21. A positive integer prime $p \in \mathbb{Z}$ splits in $\mathbb{Z}[i]$ iff it is the sum of two squares in \mathbb{Z} .

Proof. Use norm. □

Theorem 5.4 (Fermat). A positive odd prime $p \in \mathbb{Z}$ is a sum of two squares iff $p \equiv 1 \pmod 4$.

Chapter 6

Linear Algebra I

This corresponds to Aluffi Chapter VI.

Chapter 7

Field Theory

Aluffi Chapter VII.

Proposition 7.1. Any ring homomorphism from a field to a nonzero ring is injective.

Definition 7.1 (finite field extension). A field extension $k \subset F$ is finite, of degree n , if F has finite dimension $\dim F = n$ as a vector space over k .

Definition 7.2 (simple extension). A field extension $k \subset F$ is simple if there exists an element $\alpha \in F$ such that $F = k(\alpha)$.

For example, the extension $\frac{K[t]}{(f(t))} = K(\alpha)$ for some $f(\alpha) = 0$.

Proposition 7.2. Let $k \subset k(\alpha)$ be a simple extension, then consider the evaluation map

$$\varepsilon : f(t) \mapsto f(\alpha)$$

Then ε is not injective iff $k(\alpha)$ is a finite extension, i.e., there exists a monic irreducible polynomial p such that

$$k(\alpha) = \frac{k[t]}{(p(t))}$$

Definition 7.3. Let $k \subset F$ be an extension, then the group of automorphisms of this extension, denoted $\text{Aut}_k(F)$ is the group of automorphisms $\varphi : F \rightarrow F$ that fixes k .

Corollary 7.1. Let $k \subset k(\alpha)$, and $p(x)$ be the minimal polynomial over k , then

$$|\text{Aut}_k(k(\alpha))| = \text{number of distinct roots of } p \text{ in } k(\alpha)$$

and

$$|\text{Aut}_k(k(\alpha))| \leq [k(\alpha) : k]$$

with equality if and only if $p(x)$ factors over $k(\alpha)$ as a product of distinct linear factors.

Proposition 7.3. Let $k \subset F$ be finite, then it is also an algebraic extension, where for any $\alpha \in F$,

$$[k(\alpha) : k] \leq [F : k]$$

Proposition 7.4. Let $k \subset E \subset F$ be field extensions, then $k \subset F$ is finite iff both E/k and F/E are finite, in this case

$$[F : k] = [F : E][E : k]$$

Corollary 7.2. Let $k \subset F$ be finite, and E be an intermediate field, then both $[E : k], [F : E]$ divide $[F : k]$.

Definition 7.4. A field ext $k \subset F$ is finitely generated if there exists $\{\alpha_i\} \subset F$ such that

$$F = k(\alpha_1) \dots (\alpha_n)$$

Proposition 7.5. Let $k \subset k(\alpha_1, \dots, \alpha_n)$ be finitely generated, then $k \subset F$ is algebraic implies that $k \subset F$ is finite.

Corollary 7.3. Let $k \subset F$ be a field extension, then

$$E = \{\alpha \in F : \alpha \text{ is algebraic over } k\}$$

is a field extension over k .

Corollary 7.4. Let $k \subset E \subset F$, then $k \subset F$ is algebraic iff both $k \subset E$ and $E \subset F$ are algebraic.

Definition 7.5. Let $f(x) \in k[x]$ be a polynomial of degree d , the splitting field of f over k

$$F = k(\alpha_1) \dots (\alpha_d)$$

generated by all roots of f , i.e., such that f splits into linear factors over F .

Proposition 7.6. Splitting field of f is unique up to isomorphisms, and

$$[F : k] \leq (\deg(f))!$$

Definition 7.6. A field extension $k \subset F$ is normal if every irred polynomial f has a root in F iff f splits into product of linear factors over F .

Proposition 7.7 (normal). A field extension $k \subset F$ is **finite and normal** iff F is the splitting feild of some polynomial $f \in k[x]$.

Definition 7.7. Let k be a field, $f \in k[x]$ is separable if it has no multiple factors over its splitting field.

Proposition 7.8. Let $f \in k[x]$, then f is separable iff f, f' are relatively prime. If it is inseparable, then $f' = 0$.

Definition 7.8. Let k be a field of characteristic p , the map from $k \rightarrow k$ such that $x \mapsto x^p$ is a homomorphism (Frobenius).

A field is perfect if $\text{char}(k) = 0$ or the Frobenius map is surjective.

Proposition 7.9. k is perfect iff irred polynomial in $k[x]$ are separable.

Corollary 7.5. Finite fields are perfect, i.e., irred polynomials are separable.

7.1 Finite fields

Definition 7.9. Let F be a finite field of characteristic p , then F is an extension of \mathbb{F}_p , i.e.,

$$F = \mathbb{F}_{p^d}$$

for some $d \in \mathbb{Z}^+$.

Theorem 7.1. The polynomial

$$x^{p^d} - x$$

is separable over \mathbb{F}_p , and the splitting field of $x^{p^d} - x$ over \mathbb{F}_p is a field with p^d elements.

Conversely, let F be a field with p^d elements, then F is the splitting field of

$$x^{p^d} - x$$

over \mathbb{F}_p .

Corollary 7.6. For every p^d for some d , there exists only one finite field of order p^d up to isomorphisms. This is the Galois field of order p^d .

Corollary 7.7. $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$ iff $d \mid e$.

Corollary 7.8. Let $F = \mathbb{F}_{q^n}$, then

$$x^{q^n} - x$$

factors over \mathbb{F}_q as irreducible polynomials of degree d , where d ranges over all divisors of n . These polynomials factor completely over \mathbb{F}_{q^n} .

Theorem 7.2. $\text{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d})$ is cyclic, generated by the Frobenius isomorphism.

7.2 Cyclotomic

Definition 7.10. Polynomial

$$\Phi_n(x) = \prod_{i=0}^{n-1} (x - \xi_n^i)$$

is called the n th cyclotomic polynomial.

Proposition 7.10. If $n = p$ is prime, then

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

For all positive integers n , we have

$$x^n - 1 = \prod_{1 \leq d|n} \Phi_d(x)$$

Proposition 7.11. For all positive n , $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible over \mathbb{Q} .

Definition 7.11. The splitting field $\mathbb{Q}(\zeta_n)$ for $x^n - 1 \in \mathbb{Q}[x]$ is the n th cyclotomic field.

Proposition 7.12. $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ is isomorphic to the group $(\mathbb{Z}/n\mathbb{Z})^\times$

Proposition 7.13. An algebraic extension $k \subset F$ is simple iff the number of distinct intermediate fields $k \subset E \subset F$ is finite.

Theorem 7.3. Every finite separable is simple.

One should draw diagrams

$$k - E - F$$

and

$$\text{Aut}_k(F) = \text{Aut}_E(F) = \{e\}$$

each extension (reversely) corresponds to a subgroup that fixes that extension in the Galois group $\text{Gal}(F/k)$.

Theorem 7.4. Let $k \subset F$ be Galois, then $k \subset E \subset F$, $k \subset E$ is Galois iff $\text{Aut}_E(F)$ is normal in $\text{Gal}(F/k)$, in this case,

$$\text{Gal}(E/k) \cong \frac{\text{Gal}(F/k)}{\text{Gal}(F/E)}$$

Definition 7.12 (discriminant). The discriminant of f , separable, irreducible is

$$D(f) = \Delta^2 f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

Proposition 7.14. Let k be field of char not equal to 2, and f is separable, with discriminant D . Then the Galois group of f is contained in A_n iff D is a square in k .
(We note that Δ is fixed by the Galois group G iff $G \subset A_n$)

Proposition 7.15. Let $f \in \mathbb{Q}[x]$ be irred of degree p , assume that f has $p - 2$ real roots and 2 complex roots, then the Galois group is S_p .

Theorem 7.5. Every finite abelian group is the Galois group of some extension F over \mathbb{Q} .

More specifically, every finite abelian group G is the group of some intermediate field of the extension $\mathbb{Q} \subset \mathbb{Q}(\xi_n)$ in a cyclotomic field.

Proof. Classification:

$$G \cong \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_r\mathbb{Z}}$$

Choose distinct p_i such that $p_i \equiv 1 \pmod{n_i}$. Let $n = p_1 \cdots p_r$, by CRT

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^\times$$

Then $(\mathbb{Z}/n\mathbb{Z})^\times$ has a subgroup H such that

$$G \cong \frac{(\mathbb{Z}/n\mathbb{Z})^\times}{H}$$

Since $(\mathbb{Z}/n\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}(\zeta_n))$, H corresponds to an intermediate field F , where

$$\mathbb{Q} \subset F \subset \mathbb{Q}(\zeta_n)$$

H is automatically normal, hence $\mathbb{Q} \subset F$ is Galois and

$$\text{Gal}(F/\mathbb{Q}) = G$$

□

Chapter 8

Linear Algebra II

This corresponds to Aluffi Chapter VIII.

Chapter 9

Field Theory

This corresponds to Aluffi Chapter VII.

Chapter 10

Representation Theory of Finite Groups

Chapter 11

Semisimple Algebra