Algebra Definition Theorem List

Hui Sun

August 23, 2025

Contents

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 $I \to A$. We say F is final if for every A, there exists a unique morphism $A \to F$.

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 $g = h$.

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 2.2. 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 2.3. If $gh = hg$, then $|gh|$ divides lcm$(|g|, |h|)$.

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

Proposition 2.4. 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 2.5. 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 2.6. There is an isomorphism between D_3 and S_3.

Proposition 2.7. 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 2.8. If H is commutative, then $\mathrm{Hom}(G, H)$ is a group.

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

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

Proposition 2.9. Let $\{H_\alpha\}$ be any family of subgroups of G, then

$$\bigcap_\alpha H_\alpha$$

is a subgroup of G.

Proposition 2.10. 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 2.11. Let $H \subset \mathbb{Z}/n\mathbb{Z}$ be a subgroup, then H is generated by some m where m divides n.

Proposition 2.12. If $\varphi : G_1 \to G_2$ is a homomorphism, then $\ker(\varphi)$ is a normal subgroup.

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

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

Proposition 2.13. 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,

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

Proposition 2.14. 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 2.15. 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 2.16. 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 2.17. Let H be a subgroup of G, then for all $g \in G$, the function $H \to gH$ such that

$$h \mapsto gh$$

is a bijection.

Theorem 2.2 (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 2.3 (Fermat's Little Theorem). Let p be a prime integer, and a be any integer, then

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

Proposition 2.18. Any group G acts on itself by left/right multiplications, and acts on the costs 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 2.19. 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 $a, b \in G$, 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 2.20. 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 2.21. 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

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

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

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

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 acion, then

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

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:

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

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

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

Moroever, 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

$$N \equiv 1 \mod p$$

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

$$n_p \equiv 1 \mod p$$

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. □

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

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

Definition 3.7. 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 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 $\varepsilon : S_n \to \{\pm 1\}$ (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. □

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 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. □

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 $\theta : H \to \mathrm{Aut}(N)$, then define an operator $\cdot_\theta$ on $N \times H$ 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 $N \rtimes_\theta H$ is the group $N \times H$ with operation $\cdot_\theta$.

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

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

Then

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

(Recall that the operation defined on $N \otimes_\theta H$ is $(n_1, h_1) \cdot (n_2, h_2) = (n_1\theta_{h_1}(n_2), h_1h_2)$).

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 $|H|, |N|$ 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 $p_1, \ldots, p_r$, 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

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

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. □

Warning 3.14. Next one is important.

Proposition 3.33. Let G be a finite group of order n, then G can be embedded into S_n.

Proof. G acts on itself by left multiplication. □

Proposition 3.34. The number of conjugacy classes of $D_n = \langle r, s : r^n = s^2 = e, rs = sr^{-1}$:

1. $n =$odd, then $\{e\}$ is its own conjugacy class, the pairs of rotations $\{r^k, r^{-k}\}$ are conjugacy classes, the reflections form ONE conjugacy class:
$$1 + \frac{n-1}{2} + 1 = \frac{n+3}{2}$$
conjugacy classes.

2. $n =$even, then $[e]$, $[r^{n/2}]$ forms their own conjugacy classes, the remaining rotations $[r^k, r^{-k}]$, and there are TWO conjugacy classes of reflection:
$$1 + 1 + \frac{n-2}{2} + 1 + 1 = \frac{n+6}{2}$$
conjugacy classes.

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. $\mathrm{End}_{\mathrm{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$, where $\mathrm{End}_{\mathrm{Ab}}(G) = \mathrm{Hom}_{\mathrm{Ab}}(G, G)$ 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 $\varphi : R \to S$ 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 4.2. Let $\varphi : R \to S$ 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 $I = (a_1, \ldots, a_n)$, i.e., every element in I can be written as

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

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

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

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

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 $a_0 + a_1 x$. 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, $k[x_1, \ldots, x_n]$ have Kruell dimension n:

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

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 $\varphi : M \to M'$ 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

$$IM = \{\sum_i r_i m_i : r \in I, m \in M\}$$

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 $\varphi : M \to M'$ 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:

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

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:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, leftrightarrow, "\cong"] & B \arrow[r, "g"] \arrow[d, leftrightarrow, "\cong"] & C \arrow[r] \arrow[d, leftrightarrow, "\cong"] & 0 \\
0 \arrow[r] & A' \arrow[r] & A \oplus C \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

Chapter 5

Ring Theory II

This corresponds to Aluffi Chapter V.

Proposition 5.1. Let N be a submodule of M, where M is finitely generated, let $\langle m_1, \ldots, m_k \rangle$ be the elements whose cosets generate M/N, then

$$M = N + \langle m_1, \ldots, m_k \rangle$$

Proof. This is the same proof that if $N, M/N$ are finitely generated, then M is. □

Proposition 5.2. Let R be commutative, and M be an R-module, then TFAE:

1. M is **Noetherian**.
2. M satisfies the **ascending chain condition**. (sequence of submodules.)
3. Every nonempty family of submodules has a maximal element with respect to inclusion.

Proof. Noetherian implies acc: given $N_1 \subset N_2 \subset \ldots$, then $N = \bigcup_i N_i$ is finitely generated. □

Proposition 5.3 (Hilbert's basis theorem)**.** Let R be a Noetherian ring, then $R[x_1, \ldots, x_n]$ is Noetherian. This is the same as If R is Noetherian, then $R[x]$ is also Noetherian.

Proposition 5.4. Let $a, b \in R$, then $(a) = (b)$ iff $a = ub$ for some unit u.

Definition 5.1 (prime, irreducible elements)**.** Let R be commutatie

1. Let R be an integral domain, an element $a \in R$ is **prime** if the ideal (a) is prime.
2. 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 5.5. Let R be an **integral domain**, then

$$\text{nonzero prime elements} \Rightarrow \text{ irreducible}$$

Definition 5.2 (factorization). $r \in R$ has a factorization if there exists **finite** irreducibles $q_1, \ldots, q_n$ such that

$$r = q_1 \ldots q_n$$

Proposition 5.6. Let R be an integral domain, and let r be a nonzero, nonunit element of R. Assume that every ascedning chain of principal ideals,

$$(r) \subset (r_1) \subset (r_2) \ldots$$

stabilizes. Then r has a factorization into irreducibles.

Of course if a ring is ACC, then factorizations exist.

Proposition 5.7. Factorization exists in Noetherian rings.

Example 5.1. A non-Noetherian ring but factorization still exists:

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

Proposition 5.8. Let R be Noetherian and I be an ideal, then R/I is also Noetherian.

5.1 UFD, PID, ED

Definition 5.3 (gcd). Let $a, b \in R$, then the gcd of a, b is d such that (d) is the smallest principal ideal such that

$$(a, b) \subset (d)$$

Proposition 5.9. Let R ba UFD, and $a, b, c \in R$ be nonzero, then

$$(a) \subset (b) \iff m(b) \subset m(a)$$

where $m(a)$ is the multiset of irreducible factors of a. Moreover, the irreducible factors of bc are the collection of irreducible factors of b and c.

Proposition 5.10. Let R be a UFD, then gcd of any a, b exsits.

Example 5.2. There exists Noetherian rings that are not UFD.

$$\frac{\mathbb{C}[x, y, z, w]}{(xw - yz)}$$

since $r = xw = yz$.

Proposition 5.11. In UFD, a is irreducible implies a is prime.

Proof. Assume $bc \in (a)$, then $(bc) \subset (a)$, hence the multiset of irreducible factors of a is contained in the multiset of b, c, but a is irreducible implies that a must be among the factors of b or c. □

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 5.12. If R is a PID, and $a, b \in R$, then $d = \gcd(a, b)$ iff $(a, b) = (d)$. In other words, there exists $r, s \in R$, such that

$$d = ra + sb$$

Example 5.3. UFD but not PID:

$$\mathbb{Z}[x]$$

Definition 5.4 (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.

5.2 $R(x)$ and Field of Fractions

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

Example 5.4. $\mathbb{Z}[x], \mathbb{Z}[x_1, \ldots, x_n]$ are UFD.

Definition 5.5 (Field of fractions). Let R be an integral domain, then the field of fractions is

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

where $\frac{a}{r}$ is the equivalence given by $\frac{a}{r} \sim \frac{b}{s} \iff as = br$.

Definition 5.6. The field of fractions $R[x]$ is the field of rational functions with coefficients in R: elements are of the form

$$\frac{p(x)}{q(x)}, q(x) \neq 0$$

denoted as $R(x)$.

Definition 5.7 (primitive). Let R be a UFD, f is primitive if and only if $\gcd(a_0, \ldots, a_d) = 1$.

Proposition 5.13. 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 in $K[x]$.

5.3 Irreducibility

Proposition 5.14. Let R be an ID, then $f \in R[x]$ of degree d can have at most d roots.

This is not true for non-ID, for example, $x^2 + 2$ over $\mathbb{Z}/6\mathbb{Z}$.

Proposition 5.15. Let k be a field, then $f \in k[x]$ of degree 2 or 3 is irreducible iff it has no root in k.

Example 5.5. $t^2 + t + 1$ is irreducible over $\mathbb{F}_2$ (therefore over $\mathbb{Q}$).

Proposition 5.16 (rational root theorem). Let R be a UFD, and K be its field of fractions, let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$$

if $\frac{p}{q} \in K$ is a root, ($\gcd(p, q) = 1$), then

$$p \text{ divides } a_0, q \text{ divides } a_n$$

Proposition 5.17. Let k be a field, and $f(t) \in k[t]$ be a nonzero irreducible polynomial. Then

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

is a field, where k embeds into F. Moreover, $f(x) \in k[x]$ has a root in F, which is

$$t + (f(t))$$

Proposition 5.18. A field is algebraically closed

$$\begin{aligned} k \text{ is algebraically closed} &\iff \text{all irreducible polynomials in } k[x] \text{ have degree } 1 \\ &\iff \text{every nonconstant polynoimal } f \text{ factors completely into linear factors} \\ &\iff \text{every nonconstant } f \text{ has a root in } k \end{aligned}$$

Proposition 5.19. Finite fields are not algebraically closed. In other words, if a field k is algebraically closed, then it is infinite.

Example 5.6. The nonconstant irreducible polynomials of $\mathbb{R}[x]$ are precisely those of degree 1 and quadratic $f = ax^2 + bx + c$ where $b^2 - 4ac < 0$.

Proposition 5.20. Let $f \in \mathbb{Z}[x]$ be such that $\gcd(a_0, \dots, a_n) = 1$, and let p be prime. If $f \mod p$ has the same degree as f, and is irreducible over $\mathbb{F}_p$, then f is irreducible over $\mathbb{Z}$.

Warning 5.3. This is important! We can show a polynomial is irreducible over $\mathbb{Z}$ by showing it is irreducible over $\mathbb{F}_p$ for some p.

Example 5.7. There exists reducible polynomial over $\mathbb{Z}$ but irreducible over $\mathbb{F}_p$ for every prime p: x^4+1. (Hint: Legendre symbol).

Proposition 5.21 (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 $\deg(f)$.

Warning 5.4. Generalized Eisenstein works for commutative rings! Some examples:

$$\mathbb{C}[x, y], \frac{\mathbb{C}[x_1, x_2, x_3, x_4]}{(x_1x_2 - x_3x_4)}$$

Example 5.8. For all n and all primes p, the polynomial $x^n - p$ is irreducible over $\mathbb{Z}$.

Example 5.9. Let p be a prime, then the cyclotomic polynomial $\Phi_p(x)$ is irreducible.

$$1 + x + x^2 + \cdots + x^{p-1}$$

Proof.

$$f(x) = \frac{x^p - 1}{x - 1} f(x+1) \qquad = \frac{(x+1)^p - 1}{x}$$

We see that coefficients are now

$$\binom{p}{k}, k = 1, \dots, p-1$$

hence p divides all but leading coefficient. ☐

5.4 CRT

Theorem 5.5 (CRT). Let $I_1, \dots, I_k$ be ideals of R such that $I_i + I_j = (1)$ for all $i \neq j$. Then

$$\frac{R}{I_1 \cap \cdots \cap I_k} = \frac{R}{I_1 I_2 \dots I_k} \cong \frac{R}{I_1} \times \cdots \times \frac{R}{I_k}$$

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

Proposition 5.22 (CRT in PID)**.** Let R be a PID, and let $a_1, \ldots, a_k$ be elemnts such that $\gcd(a_i, g_j) = 1$, let $a = a_1 \ldots a_k$, then

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

Chapter 6

Linear Algebra I

This corresponds to Aluffi Chapter VI, excluding Section 4-5.

6.1 basis, free modules, IBN

Proposition 6.1 (Zorn's). Every module M has maximal linealry independent set. In other words, let $S \subset M$ be a linearly independent subset. Then there exists a maximal linealry independent subset of M containing S.

Definition 6.1 (basis). A subset $S \subset M$ is a basis if it is linearly independent and generates M. Every element in M can be written as

$$m = \sum_{s_i \in S} r_i s_i$$

where only finitely many terms are nonzero.

((2) $\subset \mathbb{Z}$ is maximal but not a basis).

Proposition 6.2. Regarding basis,

1. An R-module M is free iff it admits a basis. (Any vector space is free as a k-module).
2. The converse holds when $R = k$: let B be a maximal linearly independent subset of $M = V$, then B is a basis.
3. When $R = k$, let S be a linearly independent subset, then there exists a basis B of V containing S. If B is a minimal generating set for V, then B is also a basis.

Proposition 6.3. Let R be an **integral domain**, and M a free R-module, let B be a maximal linearly independent subset of M. If S is any independent subset, then

$$|S| \leq |B|$$

Example 6.1. The basis $\mathbb{C}[x]$ over $\mathbb{C}$ is $\{1, x, \dots\}$, hence an uncountable subset of $\mathbb{C}[x]$ is necessarily linearly dependent.

Proposition 6.4. Let R be an **integral domain**, let m, n be nonnegative integers,

$$R^m \cong R^n \iff m = n$$

If R satisfies the above, we say it satisfies the invariant basis number property. (All commutative rings satisfy this)!

Definition 6.2 (rank of a module). Let R be an integral domain, the rank of a free module M is the size of the maximal linearly independent subset of M.

Proposition 6.5. Let R be an integral domain, and let M be a free R-module, assume that M is generated by S: $M = \langle S \rangle$, then S contains a maximal linearly independent subset of M.

6.2 Homomorphisms $R^n \to R^m$

Proposition 6.6. Let $\alpha : M \to N$ be a homomrophism of finitely generated modules, and let P be a matrix representing it wrt any basis of M, N, then with respect to any other choice of bases of M, N, α is of the form

$$N_1 \cdot P \cdot N_2$$

where N_1, N_2 are invertible matrices.

Proposition 6.7. Two matrices $P, Q \in M_n(R)$ are equivalent if they are the same up to elementary operations, i.e., iff the same up to multiplications by elementary matrices. In other words, M, N are equivalent if there exists invertible P_1, P_2 such that

$$M = P_1 N P_2$$

Example 6.2. The matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

interchanges the second and fourth row of a $4 \times n$ matrix. Multiplying on the right by

$$\begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

adds to the third column of a $m \times 3$ matrix the c-multiple of the first column.

Proposition 6.8. Let k be a field, then $\mathrm{GL}_n(k)$ is generated by elementary matrices!

Proposition 6.9. Over a field, every $m \times n$ matrix is equivalent to a matrix is equivalent to a matrix of the form:

$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

In other words, up to multiplying some invertible matrix N_1, N_2 on the left and right, every matrix is of the above form.

Proposition 6.10. Let R be commutative, a square matrix A is invertible iff $\det(A)$ is a unit in R; The determinant is a homomorphism $\det : \mathrm{GL}_n(R) \to (R^*, \cdot)$, and for $A, B \in M_n(R)$,

$$\det(AB) = \det(BA)$$

Proposition 6.11. The row rank of a matrix over a field is equal to its column rank, recall that every matrix is equivalent to a matrix of the form

$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

From this we also know that

$$\dim V = \text{ rank of } \alpha + \text{ nullity of } \alpha$$

Definition 6.3 (adjoint matrix)**.** Let M be an $n \times n$ matrix, the adjoint matrix adj(A) is such that

$$A \cdot \text{adj}(A) = \text{adj}(A)A = \det(A)I_n$$

Proposition 6.12 (Nakayama's lemma)**.** (Different versions of the same lemma).

1. Let R be a commutative ring, M and R-module, and let $a \in R$ be a nilpotent element, then

$$M = 0 \iff aM = M$$

2. Let J be the Jacobson radical of R, where M is finitely generated R-module. If $M = JM + N$, then $M = N$. (A special case is when R is a local ring and $\mathfrak{m} = J$).

6.3 Invariants in Linear Transformations

Definition 6.4 (similar matrix)**.** Two matrices A, B are similarly iff there exists invertible P such that

$$A = PBP^{-1}$$

For example, A is similar to A^t.

Proposition 6.13. Similar implies equivalent, but equivalent does not imply similar.

Proposition 6.14. Let α be a linear transformation of R^n, a free R-module, then

$$\det(\alpha) \neq 0 \iff \alpha \text{ is injective}$$

Proposition 6.15. For $A, B \in M_n(R)$,

$$\text{tr}(AB) = \text{tr}(BA)$$

If A, B are similar, then

$$\text{tr}(A) = \text{tr}(B)$$

Definition 6.5 (characteristic polynomial). Let $\alpha \in \text{End}(F)$, where $F = R^n$, then the characteristic polynomial of α is

$$P_\alpha(t) = \det(tI - \alpha)$$

Proposition 6.16. Let $\alpha \in \text{End}(F)$, and $F = R^n$, let $P_\alpha(t) = t^n + a_{n-1}t^{n-1} \cdots + a_0$ be characteristic polynomial,

1. $P_\alpha(t)$ is of degree n.
2. $a_{n-1}t^{n-1}$ is such that $a_{n-1} = -\text{tr}(\alpha)$.
3. $a_0 = (-1)^n \det(\alpha)$.
4. If α, β are similar, then $\det(\alpha) = \det(\beta)$.
5. We have
$$P_\alpha(t) = t^n - \text{tr}(\alpha) + \cdots + (-1)^n \det(\alpha)$$

Example 6.3. Having the same characteristic polynoimal does not guarantee they are similar:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

are not similar.

Definition 6.6 (annihilator ideal). Given $\alpha \in \text{End}(F)$, and $f(x) \in R[x]$, the annihilator ideal of α is

$$\mathcal{A}(\alpha) = \{f \in R[x] : f(\alpha) = 0\}$$

Definition 6.7. Let k be a field, the minimal polynomial of α is the monic generator $m_\alpha(t)$ of $\mathcal{A}(\alpha) = ((m_\alpha(t)))$.

Proposition 6.17. If α, β are similar, then

$$\mathcal{A}(\alpha) = \mathcal{A}(\beta)$$

Proposition 6.18 (Cayley-Hamilton). Let $P_\alpha(t)$ be the characteristic polynomial of α, then

$$P_\alpha(\alpha) = 0$$

Proposition 6.19. If α, β are similar, then they have the same eigenvalues. Moreover, $\lambda \in R$ is an eigenvalue of α iff it is a root of the characteristic polynomial of α.

Proposition 6.20. If R is algebraically closed, then α has exactly n eigenvalues; more generally, it has at most n eigenvalues.

Proposition 6.21. The dimension of the eigenspace wrt λ is always less than or equal to its algebraic multiplicity $(t-\lambda)^k$. If for each λ, they are equal, then α is diagonalizable with respect to an eigenbasis.

6.4 The canonical form

Proposition 6.22. Recall: every finitely generated module over a PID ($[x]$) is a direct sum of cyclic modules.

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

is cyclic viewed as a $k[t]$-module.

Proposition 6.23. There is a one-to-one correspondence

$$\{(\text{V},\alpha) : \alpha : V \to V\} \leftrightarrow \{k[t] - \text{modules of } V\}$$

The isomorphism $(\rightarrow)$ is given by

$$(V, \alpha) \mapsto (k[t] \to \text{End}(V) : t \mapsto \alpha)$$

and $(\leftarrow)$ is given by

$$(\varphi : k[t] \to \text{End}(V)) \mapsto (V, \varphi(t))$$

Proposition 6.24. Let k be a field, and V finite dimensional vector space, let α be a linear transformation, endow V with the $k[t]$-structure, there exists distinct monic irreducible polynomials $p_i(t) \in k[t]$ such that

$$V \cong \bigoplus_{i,j} \frac{k[t]}{(p_i(t)^{r_{ij}})}$$

as $k[t]$-modules. Moreover, there exists monic $f_1, \ldots, f_m$ such that

$$V \cong \frac{k[t]}{(f_1(t))} \oplus \cdots \oplus \frac{k[t]}{(f_m(t))}$$

as $k[t]$-modules, where $f_1(t) \mid \cdots \mid f_m(t)$. The characteristic and minimal polynomials are such that

$$P_\alpha(t) = f_1(t) \ldots f_m(t) = \prod_{i,j} p_i(t)^{r_{ij}}$$

and

$$m_\alpha(t) = f_m(t)$$

Proposition 6.25. If $P_\alpha(t)$ factors completely over k, i.e.,

$$P_\alpha(t) = \prod_{i=1}^{s} (t - \lambda_i)^{m_i}$$

where λ_i are distinct eigenvalues of α, then

$$V \cong \bigoplus_{i=1}^{s} \frac{k[t]}{(t - \lambda_i)^{m_i}}$$

where $m_i = \sum_j r_{ij}$ in the above expression. Moreover,

$$m_\alpha(t) = \prod_{i=1}^{s} (t - \lambda_i)^{\max_j \{r_{ij}\}}$$

Example 6.4. One use of the Jordan canonical form is the enumeration of all possible similarity classes of transformations with given eigenvalues. For example, there are 5 similarity classes of linear transformations with a single eigenvalue λ with algebraic multiplicity 4, over a 4-dimensional vector space: indeed, there are 5 different ways to stack together Jordan blocks corresponding to the same eigenvalue, within a 4×4 square matrix:

$$\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix},$$
$$\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}.$$

Proposition 6.26. Two matrices are similar if and only if they have the same Jordan form.

Proposition 6.27. The dimension of the eigenspace with respect to λ is the **number** of the Jordan blocks with respect to λ.

Proposition 6.28. Assume $P_\alpha(t)$ factors completely over k, then α is diagonalizable iff either of following :

1. The dimension of eigenspace=algebraic multiplicity of λ for all eigenvalues λ of α.
2. Minimal polynomial $m_\alpha(t)$ has no repeated roots.

Warning 6.1. This is important.

Proposition 6.29. Let k be algebraically closed, the minimal polynomial coincide with the characteristic iff the Jordan form has a single Jordan block for each distinct eigenvalue.

Chapter 7

Linear Algebra II

This corresponds to Aluffi Chapter VIII. (Section 2.1, 2.2 Section 3 Section 4)

7.1 Tensor

Definition 7.1 (bilinear). Let M, N, P be R-modules. A function $\varphi : M \times N \to P$ is R-bilinear if

1. For all $m \in M$, $n \mapsto (m, n)$ is an R-module homomorphism $N \to P$.
2. For all $n \in N$, $m \mapsto (m, n)$ is an R-module homomorphism $M \to P$.

In other words,

$$\varphi(m, r_1 n_1 + r_2 n_2) = r_1 \varphi(m, n_1) + r_2 \varphi(m, r_2)$$

similarly for $M \to P$.

Proposition 7.1 (Tensor product). The tensor product can be constructed as follows:

1. Take the **free** R**-module** generated by symbols $\{m \otimes n \mid m \in M, n \in N\}$.
2. **Quotient** by the submodule generated by the relations (to enforce bilinearity):
   - $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$,
   - $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$,
   - $(r \cdot m) \otimes n = m \otimes (r \cdot n) = r \cdot (m \otimes n)$ for $r \in R$.

Thus, elements of $M \otimes_R N$ are finite sums of the form $\sum_i m_i \otimes n_i$, subject to the above rules.

Key Properties of Tensor Products

1. **Bilinearity**: The map $\otimes : M \times N \to M \otimes_R N$ is R-bilinear.
2. **Functoriality**: If $f : M \to M'$ and $g : N \to N'$ are R-linear, there is an induced map:
$$f \otimes g : M \otimes_R N \to M' \otimes_R N', \quad (f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$
3. **Associativity**: $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$.
4. **Commutativity**: $M \otimes_R N \cong N \otimes_R M$ (if R is commutative).
5. **Base Change**: If S is an R-algebra, then $M \otimes_R S$ is an S-module.

Proposition 7.2 (universal property). Every R-bilinear map $\varphi : M \times N \to P$ factors uniquely through the tensor product $M \otimes_R N$,

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[d, "\otimes"'] & P \\ M \otimes_R N \arrow[ur, "\exists!\overline{\varphi}"'] & \end{tikzcd}$$

in such a way that the map $\overline{\varphi}$ is unique.

Example 7.1. For all R-modules,

1. $R \otimes_R N \cong N$.
2. $M \otimes_R N \cong N \otimes_R M$.

Proposition 7.3. Let $\alpha, \beta : M \otimes N \to P$, if

$$\alpha(m \otimes n) = \beta(m \otimes n)$$

for all $m \in M, n \in N$, then $\alpha = \beta$. (This means it suffices to check on pure tensors).

7.2 Hom and Tensor

Proposition 7.4. Let $\alpha : M_1 \to M_2$ be an R-module homomorphism, let N be an R-module, there is an induced R-linear map

$$\alpha \otimes N : M_1 \otimes_R N \to M_2 \otimes_R N$$

On pure tensors, this map is given by

$$m \otimes n \mapsto \alpha(m) \otimes \alpha(n)$$

Proposition 7.5. For all R-modules M, N, P, there is an isomorphism of R-modules

$$\mathrm{Hom}_R(M, \mathrm{Hom}(N, P)) \cong \mathrm{Hom}_R(M \otimes_R N, P)$$

Proof. This says any bilinear map from $M \times N$ comes from $M \otimes_R N$. □

Proposition 7.6. For all R-modules, M_1, M_2, N, we have

$$(M_1 \oplus M_2) \otimes_R N \cong (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$$

The same statement is true for $\sum_\alpha M_\alpha \otimes N$. This also implies that

$$R^{\oplus n} \otimes_R R^{\oplus m} \cong R^{\oplus nm}$$

Proposition 7.7. Let M, N be free R-modules of rank m, n, then $M \otimes_R N$ has rank mn. (Let $e_1, \ldots, e_m$ generate M, $v_1, \ldots, v_n$ generate N, where M, N are free R-modules, then $M \otimes_R N$ is generated by $e_i \otimes v_j$, and these mn elements are the basis for $M \otimes_R N$.)

Proposition 7.8. Let N be an R-module, and I be an ideal of R, then

$$\frac{R}{I} \otimes_R N \cong \frac{N}{IN}$$

($R \otimes_R N \cong N$). Moreover, let $J \subset R$ also be an ideal, then

$$\frac{R}{I} \otimes_R \frac{R}{J} \cong \frac{R}{I+J}$$

Warning 7.1. The next example is important.

Example 7.2. We have

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{\gcd(m,n)}$$

(Recall that $(m) + (n) = \gcd(m, n)$ in $\mathbb{Z}$, and $(m) \cap (n) = (\text{lcm}(m, n))$). For example,

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{3\mathbb{Z}} = 0$$

So if $\gcd(m, n) = 0$, then

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}} = 0$$

Definition 7.2 (reduced ring)**.** Let R be a ring, it is **reduced** if there are no nonzero nilpotent elements.

7.3 Multilinear Algebra: Wedge and Symmetric Product

Every $\varphi : M_1 \times \cdots \times M_k \to P$ factors unique through $M_1 \otimes \cdots \otimes M_k$, and we will denote

$$M^{\otimes k} := M \otimes_R \cdots \otimes_R M \; k \text{ times}$$

Definition 7.3 (symmetric and alternating map)**.** Let $\varphi : M^k \to P$, then it is called **symmetric** if for all $\sigma \in S_k$, and all $m_1, \ldots, m_k$, we have

$$\varphi(m_{\sigma(1)}, \ldots, m_{\sigma(k)}) = \varphi(m_1, \ldots, m_k)$$

And $\varphi : M^k \to P$ is called **alternating** if

$$\varphi(m_1, \ldots, m_k) = 0 \text{ whenever } m_i = m_j \text{ for some } i \neq j$$

Proposition 7.9. Let $\varphi : M^k \to P$ be R-multilinear, then

1. If φ is alternating, then for all $\sigma \in S_k$,

$$\varphi(m_{\sigma(1)}, \ldots, m_{\sigma(k)}) = (-1)^\sigma \varphi(m_1, \ldots, m_k)$$

2. If 2 is a unit in R, and for all $\sigma \in S_k$, $\varphi(m_{\sigma(1)}, \ldots, m_{\sigma(k)}) = (-1)^\sigma \varphi(m_1, \ldots, m_k)$, then φ is alternating.

It suffices to reduce to the case where $k = 2$.

Definition 7.4 (Wedge product). The module $\bigwedge^k(M)$ is generated by pure alternating tensors:

$$e_{i_1} \wedge \cdots \wedge e_{i_k}$$

where $1 \leq i_1 < \cdots < i_l \leq r$. For example, suppose $M = V$ is a 3-dimensional vector space, then $V \wedge V$ has a basis

$$v_1 \wedge v_2, v_1 \wedge v_3, v_2 \wedge v_3$$

The dimension of $V \wedge V$ is $\frac{n(n-1)}{2}$ if $\dim(V) = n$.

Next we generalize it.

Proposition 7.10. Let R be commutative, and M a free R-module of rank n, then

$$\bigwedge^k(M) \text{ is a free } R\text{-module of rank } \binom{n}{k}$$

Example 7.3. If M is a free module of rank n, then

$$\bigwedge^n(M) \cong R$$

where the isomorphism $\varphi : (e_{i1}, \ldots, e_{in}) \mapsto \begin{cases} \pm 1 \text{ if } i_1, \ldots, i_n \text{ are distinct} \\ 0 \end{cases}$

Proposition 7.11. Let $\mathrm{Sym}^n(V)$ be the **symmetric product**. A basis for $\mathrm{Sym}^n(V)$ is given by the **monomials**:

$$\left\{ e_1^{k_1} e_2^{k_2} \cdots e_d^{k_d} \;\middle|\; k_1 + \cdots + k_d = n,\ k_i \geq 0 \right\},$$

where $e_i^{k_i}$ denotes the symmetric product $e_i \ldots e_i$ (k_i times). The **Dimension** is the number of such monomials, $\binom{n+d-1}{d-1}$.

Proposition 7.12. Let V have dimension n with basis $\{e_1, \dots, e_n\}$, then $\mathrm{Sym}^k(V)$ is spanned by basis:

$$\{e_{i_1} \dots e_{i_k}, 1 \leq i_1 \leq \dots \leq i_k \leq n\}$$

(It contains the equality case compared to the wedge product). Moreover, the dimension of $\mathrm{Sym}^k V$ is

$$\binom{n+k-1}{k}$$

Example 7.4. $\mathrm{Sym}^2(V)$ for $\dim V = 2$ Let V have basis $\{e_1, e_2, e_3\}$. Then:

$$\mathrm{Sym}^2(V) = \mathrm{span}\{e_1 e_1,\ e_1 e_2,\ e_2 e_2\},$$

where:

$$\begin{aligned} e_1 \odot e_1 &= e_1 \otimes e_1, \\ e_1 \odot e_2 &= \frac{1}{2}(e_1 \otimes e_2 + e_2 \otimes e_1), \\ e_2 \odot e_2 &= e_2 \otimes e_2. \end{aligned}$$

Dimension: $\binom{2+2-1}{2-1} = 3$.

Definition 7.5 (determinant). Let F be a free R-module of rank n, then

$$\bigwedge^n F$$

is called the determinant of F, $\det(F)$. (In other words, it is the top exterior power). Recall that

$$\bigwedge^n F \cong R$$

since it is one-dimensional and spanned by $\{e_1 \wedge \dots \wedge e_n\}$.

Warning 7.2. Again, two matrices are similar if and only if they have the same jordan normal form!

Warning 7.3. Let M be an $n \times n$ matrix over k, then factor its characteristic polynomial $p(t)$ over its algebraic closure

$$p(t) = (t - \lambda_1) \dots (t - \lambda_d)$$

where λ_i are its eigenvalues in $\bar{k}$. Then

$$\mathrm{tr}(M) = \sum_i \lambda_i, \quad \det(M) = \prod_i \lambda_i$$

Proposition 7.13. Let $M \in \mathrm{GL}_n(k)$, then M is triangularizable iff the characteristic polynomial factors completely into linear factors. This is

Chapter 8

Field Theory

Aluffi Chapter VII.

Definition 8.1 (radical). The **radical** of an ideal $I \subset R$ is

$$\mathrm{rad}(I) = \sqrt{I} = \{a \in R : a^n \in I \text{ for some } n\}$$

An ideal is called radical if for any $a \in R$, $a^n \in I$ for some n, then $a \in I$.

Proposition 8.1. The radical $\sqrt{I}$ of an ideal I in R is an ideal. Moreover, $\sqrt{I}$ is radical.

Example 8.1. The nilradical of R is $\sqrt{(0)}$, i.e., the radical of the zero ideal.

Proposition 8.2. Any ring homomorphism from a field to a nonzero ring is injective.

Proposition 8.3. The characteristic of a field is either 0 or a prime number. (This is also true for integral domains). Moreover, let $k \subset E$ be an extension, then $\mathrm{char}(k) = \mathrm{char}(E)$. Moreover, for such extension, E is a vector space over k.

Definition 8.2 (finite field extension). A field extension $k \subset F$ is finite of degree n, if F has is a dimension n vector space over k. We denote

$$[F : k] = \dim_k(F)$$

Example 8.2. Let k be a field, and f is an irreducible polynomial over k, then

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

is an extension in which f has a root. (To see this is a field, we see $f(t)$ is irreducible, which is prime, which is maximal in $k[t]$).

Definition 8.3 (simple extension). A field extension $k \subset F$ is simple if there exists $\alpha \in F$ such that $F = k(\alpha)$, where $k(\alpha)$ is the smallest field containing α and k. If $k(\alpha)/k$ is a finite extension, then α is algebraic, if infinite, then α is called transcendental.

Example 8.3. The extension $k \subset \frac{k[t]}{(f(t))}$ is simple because

$$\frac{k[t]}{(f(t))} \cong k(\alpha)$$

for some α such that $f(\alpha) = 0$.

Proposition 8.4. 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., α is algebraic, thus there exists a monic irreducible polynomial p such that

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

And ε is injective iff α is transcendental.

Proposition 8.5 (lifting). Let $k_1 \subset k_1(\alpha_1), k_2 \subset k(\alpha_2)$ be two simple finite extensions, then let p_1, p_2 be the minimal polynomials of α_1, α_2, let $i : k_1 \to k_2$ be an isomorphism such that

$$i(p_1(t)) = i(p_2(t))$$

Then there exists a unique isomorphism $j : k_1(\alpha_1) \to k_2(\alpha_2)$ such that $j = i$ on k_1 and

$$j(\alpha_1) = \alpha_2$$

This says that we can extend isomorphisms between fields into their simple extensions provided that this isomorphism agrees with the structure of the extensions.

Definition 8.4 (Aut group). Let $k \subset F$ be an extension, then the group of automorphisms of this extension, denoted $\mathrm{Aut}_k(F)$ is the group of automorphisms $\varphi : F \to F$ that fixes k, $\varphi(x) = x$ for all $x \in k, \varphi \in \mathrm{Aut}_k(F)$.

Proposition 8.6. Let $k \subset k(\alpha)$, and $p(x)$ be the minimal polynomial over k, then

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

and

$$|\mathrm{Aut}_k(k(\alpha))| \leq [k(\alpha) : k] = \deg(p)$$

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

Proposition 8.7. Let $k \subset k(\alpha) = F$, then $\mathrm{Aut}_k F$ acts faithfully and transitively on the set of roots of $p(t)$ in F.

Definition 8.5 (algebraic extension). Let $k \subset F$, and $\alpha \in F$, then α is algebraic over k iff $k(\alpha)$ is a finite extension; this is equivalent to saying there exists a nonzero $f(x) \in k[x]$ such that $f(\alpha) = 0$. If $k(\alpha)/k$ is not finite, then α is transcendental.

If α is algebraic over k, then every element in $k(\alpha)$ can be written as a polynomial in α.

Proposition 8.8. Finite extensions are algebraic.

Proof. Let $k \subset F$ be finite, then consideer $\alpha \in F$, we have $k \subset k(\alpha) \subset F$, hence $k(\alpha)$ is also finite. □

Proposition 8.9. Let $k \subset E \subset F$, then $k \subset F$ is finite iff both E/k and F/E are finite, in this case

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

This implies: let $k \subset F$ be finite, and E be an intermediate field, then both $[E : k], [F : E]$ divide $[F : k]$.

Example 8.4. Let $k \subset F$, let $\alpha \in F$ be an algebraic element of odd degree over k. Then α can be written as a polynomial in α^2. It suffices to show that $k(\alpha^2) = k(\alpha)$. We consider

$$k \subset k(\alpha^2) \subset k(\alpha)$$

We see that $k(\alpha)/k(\alpha^2)$ has degree at most 2 because $t^2 - \alpha^2$, and the degree must divide $[k(\alpha) : k]$, thus it must be 1.

Definition 8.6 (finitely generated field extensions)**.** A field extension $k \subset F$ is finitely generated if there exists $\{\alpha_i\} \subset F$ such that

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

Proposition 8.10. Let $k \subset k(\alpha_1, \dots, \alpha_n)$ be finitely generated, then F/k is algebraic iff F/k is finite iff all α_i are algebraic over k. (Thus given a finitely generated extension, to show that it is finite, it suffices to show each α_i is algebraic).

Proposition 8.11. If α, β are algebraic over k, then

$$\alpha + \beta, \alpha\beta, \alpha\beta^{-1}$$

are all algebraic over k. (For example, $k(\alpha + \beta) \subset k(\alpha, \beta)$). This implies that given $k \subset F$,

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

is a field.

Proposition 8.12. (Composite algebraic extensions are algebraic). Let $k \subset E \subset F$, then $k \subset F$ is algebraic iff both $k \subset E$ and $E \subset F$ are algebraic.

Example 8.5. $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

8.1 Algebraic Closure

Proposition 8.13. Recall that k is algebraically closed iff all irreducible polynomials in $k[x]$ have degree 1, iff every polynomial factors into linear factors, iff every maximal ideal is of the form $(x - c)$ for some $c \in k$.

Proposition 8.14. Field k is algebraically closed iff k has no nontrivial algebraic extensions, iff if $k \subset F$, and $\alpha \in F$ is algebraic over k, then $\alpha \in k$.

Definition 8.7 (algebraic closure)**.** The $\bar{k}$ of k is such that $\bar{k}$ is an algebraic extension and $\bar{k}$ is algebraically closed. (The requirement that $\bar{k}/k$ is algebraic is to ensure there is no intermediate field that is also algebraically closed). Equivalently, $\bar{k}$ is the smallest field that is algebraically closed containing k.

8.2 splitting, normal, separable

Definition 8.8 (splitting field)**.** Let $f(x) \in k[x]$ be a polynomial of degree d, the splitting field of f over k is an extension F/k such that f factors into linear factors over F. In other words,

$$F = k(\alpha_1, \ldots, \alpha_d)$$

where α_i are roots of f.

Proposition 8.15. Small fact: let $n =$even, then the nth root of unity such that $\omega_n^n = 1$ also satisfies

$$\omega_n^{\frac{n}{2}} + 1 = 0$$

For example, the 8th root of unity $\omega_8 = e^{\frac{2\pi i}{8}}$ is also a root of

$$f(x) = x^4 + 1$$

which is irreducible over $\mathbb{Q}$.

Proposition 8.16. Splitting field of f is unique up to isomorphisms, and

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

Proposition 8.17. The polynomial $x^n - 1$ is not irreducible over $\mathbb{Q}$ for any $n \geq 2$. The polynomial $x^n + 1$ is only irreducible if $n = 2^k$ for some integer k.

Proposition 8.18. Let $f(x) \in k[x]$, the splitting field F of f is such that

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

Example 8.6. The splitting field of $f(x) = x^3 - 2$ is $\mathbb{Q}(\sqrt[3]{2}, \omega_3)$, which is a degree $6 = (\deg f)! = 3!$ extension.

Example 8.7. The splitting field of $x^8 - 1$ is $\mathbb{Q}(\omega_8)$, and the minimal polynomial for $\omega_8 = e^{\frac{2\pi i}{8}}$ is

$$f(x) = x^4 + 1$$

Thus $[Q(\omega_8) : \mathbb{Q}] = 4$. (The splitting field for $x^8 - 1$ is the same as $x^4 + 1$). Moreover, the Galois group is

$$\mathbb{Q}(\omega_8) = \mathbb{Q}(i, \sqrt{2})$$

is

$$\text{Gal}(\mathbb{Q}(\omega_8)/\mathbb{Q}) = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Example 8.8. The splitting field for $x^4 + 2$ is

$$\mathbb{Q}(\sqrt[4]{2}, i)$$

and the Galois group is

$$\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4$$

because it is an order 8 subgroup of S_4.

Warning 8.1. Galois group doesn't act transitively on the roots of a random polynomial! They act transitively on the roots of the irreducible factors.

Definition 8.9 (normal). A field extension $k \subset F$ is normal if every **irreducible** polynomial f has a root in F iff f splits into product of linear factors over F. (If it contains one root, then it contains all the other roots).

Proposition 8.19. A field extension $k \subset F$ is **finite and normal** iff F is the **splitting field** of some polynomial $f \in k[x]$.

Example 8.9. If a complex root of an irreducible polynomial can be expressed as a polynomial in i, $\sqrt[4]{2}$, then all the roots can be expressed as a polynomial in them.

Proof: $\mathbb{Q}(i, \sqrt[4]{2})$ is the splitting field of $x^4 + 2$, thus is normal.

Definition 8.10 (separable). Let k be a field, $f \in k[x]$ is separable if it has no multiple factors over its splitting field.

Warning 8.2. This following is a classic example. All the bad examples arise from this one (inseparable).

Example 8.10 (irreducible but not separable). Let $\mathbb{F}_p(t)$ be the field of rational functions in t over $\mathbb{F}_p$. Then the polynomial

$$f(x) = x^p - t \in \mathbb{F}_p(t)[x]$$

is irreducible, but not separable (cannot be factored into distinct linear factors in its algebraic closure). Let $u = t^{1/p}$ be a root of f in its algebraic closure, then we see

$$f(x) = x^p - t = (x - u)^p$$

Proposition 8.20. Let $f \in k[x]$, then f is separable iff f, f' are relatively prime. If it is inseparable, then $f' = 0$.

Proposition 8.21. Irreducible polynomials are separable in characteristic 0.

Proposition 8.22. Let k be a field of characteristic p, then the Frobenius homomorphism

$$x \mapsto x^p$$

is a surjective map over finite fields. (It is the identity over $\mathbb{F}_p$).

Proposition 8.23. Every irreducible polynomial in $k[x]$ is separable $\iff$ char$(k) = 0$ **or** the Frobenius homomorphism is surjective. This implies that every irreducible polynomial is separable in finite fields **or** $\mathbb{Q}$.

Remark: the reason the example $x^p - t \in \mathbb{F}_p(t)[x]$ works is because $\mathbb{F}_p(t)$ is not a finite field.

Definition 8.11 (separable element)**.** Let $k \subset F, \alpha \in F$, then α is called separable iff the minimal polynomial of α is separable over k. An extension is called separable if every $\alpha \in F$ is separable. For example, all extensions of $\mathbb{Q}$ or finite fields are separable.

Definition 8.12 (separable degree)**.** Let $k \subset F \subset \bar{k}$, the separable degree of F/k is the number of different homomorphisms/embeddings $\varphi : F \to \bar{k}$ (such that $\varphi|_k = \mathrm{id}_k$), denoted $[F : k]_s$.

Proposition 8.24. Let $k \subset k(\alpha)$ be a simple algebraic extension, then $[k(\alpha) : k]_s =$ number of distinct roots in $\bar{k}$ of the minimal polynomial p_α of α. Moreover,

$$[k(\alpha) : k]_s \leq \deg(p_\alpha)$$

the equality holds iff α i.e., p_α is separable over k.

Example 8.11. For separability degree:

1. Every separability degree is equal to the degree of extension over $\mathbb{Q}$ and finite fields.
2. $x^p - t \in \mathbb{F}_p(t)[x]$ has separability degree 1 but degree of extension p.

Proposition 8.25. Let $k \subset F$ be a finite extension, then F is finitely generated: you can just take a basis of F/k.

8.3 Finite fields

Proposition 8.26. For every prime power q, there is a unique field F_q of size q, up to isomorphisms. (This is the splitting field of $x^q - x$ over $\mathbb{F}_p$.)

Proof. Existence: we claim that

$$\{x \in \bar{\mathbb{F}}_p : x^q = x\}$$

is a field of q elements. One can show this is a subring, hence an integral domain, hence is a field because it is finite. Moreover, F has at most q elements, but $f(x) = x^q - x$ is separable because f, f' are relatively prime.

Uniqueness: for every $F_p \subset F$, this is a finite, hence algebraic extension, thus it can be embedded into $\bar{\mathbb{F}}_p$. And we claim that there's exactly one subfield of $\bar{F}_p$ with q elements:

$$F \subset 0 \cup \{x \in \bar{\mathbb{F}}_p : x^q = x\}$$

This implies $F = RHS$.

□

Proposition 8.27. Fix a prime p, then

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

iff $d \mid e$. Moreover, $\mathbb{F}_{p^e}$ contains a unique copy of $\mathbb{F}_{p^d}$. (Nothing like $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega_3)$ will happen).

Example 8.12. An extension embedding tree looks like

$$\begin{tikzcd}
 & & \mathbb{F}_{p^{36}} & & \\
 & \mathbb{F}_{p^{12}} \arrow[ur] & & \mathbb{F}_{p^{18}} \arrow[ul] & \\
\mathbb{F}_{p^4} \arrow[ur] & & \mathbb{F}_{p^6} \arrow[ul] \arrow[ur] & & \mathbb{F}_{p^9} \arrow[ul] \\
 & \mathbb{F}_{p^2} \arrow[ul] \arrow[ur] & & \mathbb{F}_{p^3} \arrow[ul] \arrow[ur] & \\
 & & \mathbb{F}_p \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

Proposition 8.28. There exist a surjective map $\varphi : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/e\mathbb{Z}$ iff $e \mid d$.

Proposition 8.29. The Galois group $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ is cyclic of order d, and it is generated by the Frobenius transformation

$$\sigma : x \mapsto x^p$$

More generally, let q be a prime power, then

$$\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \sigma : x \mapsto x^q \rangle$$

is cyclic of order d. In other words,

$$|\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d})| = d$$

In particular, $\mathbb{F}_q$ is fixed by σ: for all $x \in \mathbb{F}_q$, we must have

$$x^q = x$$

(also by Fermat). This completely describes $\mathbb{F}_q$:

$$\mathbb{F}_q = \{x \in \bar{\mathbb{F}}_q : x^q = x\}$$

Proposition 8.30. Let n be a positive integer, then over $\mathbb{F}_q$, we have

$$x^{q^n} - x = \prod_{f:\deg(f)|n} f(x)$$

where f is irreducible and monic. (All you need to do is to find all the irreducible polynomials of degree dividing n).

These polynomials factor completely over $\mathbb{F}_{q^n}$.

Example 8.13. We will do a few examples:

1. Over $\mathbb{F}_2$,
$$x^2 - x = x(x+1)$$
consisting of all irreducible polynomials of degree 1 over $\mathbb{F}_2$.

2. Over $\mathbb{F}_2$, we have
$$x^4 - x = x(x+1)(x^2+x+1)$$
consisting of all irreducible polynomials of degree $1, 2$. ($n = 2$).

3. Over $\mathbb{F}_2$, when $n = 3$, we factor
$$x^8 - x = x(x+1)(x^3+x^2+1)(x^3+x+1)$$
consisting of irreducible polynomials of degree $1, 3$.

4. over $\mathbb{F}_2$, when $n = 6$, we factor
$$x^{64} - x$$
into two polynomials of degree 1, one degree 2, two degree 3, and 9 degree 6 polynomials.

8.4 Cyclotomic

Definition 8.13 (nth cyclotomic polynomial)**.** Let $\omega_n = e^{2\pi i/n}$ be the primitive nth root, then ω_n^m is also a primitive nth root iff $\gcd(m, n) = 1$. This implies that there are $\phi(n)$ primitive rootsof 1, and the polynomial

$$\Phi_n(x) = \prod_{1\le m\le n, \gcd(m,n)=1} (x - \omega_n^m)$$

taking over all the primitive roots of n, is called the nth cyclotomic polynomial. For example,

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

Proposition 8.31. The cyclotomic polynomials $\Phi_n(x)$ satisfy:

1. When $n = p$ for some prime, then
$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + 1$$
2. When n not prime,
$$x^n - 1 = \prod_{1 \leq d, d|n} \Phi_d(x)$$

Proof. Note that the proof involves
$$x^n - 1 = \prod_{1 \leq d, d|n} \prod_{d\text{th root of unity}} (x - \omega) = \prod_{1 \leq d, d|n} \Phi_d(x)$$
□

Proposition 8.32. For all n, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. (And they have integer coefficients).

The proof is hard.

Definition 8.14 (nth cyclotomic field)**.** Let $\omega_n = e^{\frac{2\pi i}{n}}$, then the splitting field $\mathbb{Q}(\omega_n)$ of $x^n - 1$ is called the nth cyclotomic field.

Proposition 8.33. We have

1. $$[\mathbb{Q}(\omega_n) : \mathbb{Q}] = \phi(n)$$
2. $\Phi_n(x)$ is the minimal polynomial of ω_n.
3. $$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega_n)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$
where $(\mathbb{Z}/n\mathbb{Z})^\times$ is the group of units under multiplication.

Example 8.14. $\mathbb{Q}(\omega_8)/\mathbb{Q}$ is a degree 4 extension, with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\Phi_8(x) = x^4 + 1$.

Warning 8.3. Important theorem.

Proposition 8.34. Finite + separable $\Rightarrow$ simple extension.

Proposition 8.35. Transitive subgroups of S_4 are as follows:
$$S_4, A_4, D_8, \frac{\mathbb{Z}}{4\mathbb{Z}}, \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Corollary 8.1. Let $F = \mathbb{F}_q$, then

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

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

Proposition 8.36. Every finite extension of $\mathbb{Q}$ or of finite fields $\mathbb{F}_q$ is simple.

Proof. Finite+separable$\Rightarrow$ simple. □

8.5 Galois I

Definition 8.15 (Galois Correspondence). Let $k \subset F$, and $G = \mathrm{Aut}_k(F)$, let $H \subset G$ be a subgroup, then H corresponds to an intermediate field extension

$$k \subset F^H \subset F$$

where

$$F^H = \{x \in F : h \cdot x = x \text{ for all } h \in H\}$$

the fixed elements of F by H. Conversely, given $k \subset E \subset F$, we can identify a subgroup of G

$$H := \mathrm{Aut}_E(F) \subset \mathrm{Aut}_k(F)$$

This establishes a one-to-one correspondence.

Proposition 8.37. We have the following trivial inclusions:

$$E \subset F^{\mathrm{Aut}_E(F)}, \quad H \subset \mathrm{Aut}_{F^H}(F)$$

Let E_1E_2 denote the smallest subfield of F containing E_1, E_2, and $\langle H_1, H_2\rangle$ denote the smallest subgroup containing $H_1, H_2 \subset \mathrm{Aut}_k(F)$, then

$$\mathrm{Aut}_{E_1E_2}(F) = \mathrm{Aut}_{E_1}(F) \cap \mathrm{Aut}_{E_2}(F)$$

and

$$F^{\langle G_1, G_2\rangle} = F^{G_1} \cap F^{G_2}$$

Proposition 8.38. Let $k \subset F$ be finite. The degree of the field extension $[F : E]$ is the index of the subgroup $\mathrm{Aut}_E(F)$ in $\mathrm{Aut}_k(F)$. Equivalently, the size of $H \subset \mathrm{Aut}_k(F)$ is the degree $[F : F^H]$, and

$$H = \mathrm{Aut}_{F^H}(F)$$

Proposition 8.39. Let $k \subset F$ be finite, and let $H \subset \mathrm{Aut}_k(F)$ be a subgroup, then $F^H \subset F$ is finite and separable, hence simple, and also normal.

Definition 8.16 (Galois extension). $k \subset F$ is Galois iff any of the following holds:

1. F is the splitting field of a separable polynomial $f \in k[t]$.
2. $k \subset F$ is normal and separable.
3. $|\mathrm{Aut}_k(F)| = [F : k]$.
4. $k = F^{\mathrm{Aut}_k(F)}$.
5. The Galois correspondence $H \mapsto F^H$, $E \mapsto \mathrm{Aut}_E(F)$ is a bijection.
6. $k \subset F$ is separable, and if $k \subset F \subset K$ is an algebraic extension and $\sigma \in \mathrm{Aut}_k(K)$, then $\sigma(F) = F$.

Proposition 8.40. If $k \subset F$ is finite and separable, if it is not Galois, then it can be embedded into some larger field $k \subset K$ in many possible ways, i.e., the last criterion of Galois: $\sigma_1(F) \neq \sigma_2(F)$. If $k \subset F$ is Galois, then all the images of embeddings coincide.

Example 8.15. The extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is not Galois because there are three embeddings into $\mathbb{C}$ and they do not coincide.

Example 8.16. Some examples of Galois extensions:

1. $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Z}/2\mathbb{Z}$.
2. $\mathbb{Q}(\omega_8)/\mathbb{Q}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
3. Splitting field of $x^4 + 2$, D_4.
4. Galois fields such as
$$\frac{\mathbb{F}_2[x]}{(x^3 + x^2 + 1)}/\mathbb{F}_2$$
with $\mathbb{Z}/3\mathbb{Z}$.
5. $\mathbb{F}_p \subset \mathbb{F}_{p^d}$, cyclic $\mathbb{Z}/d\mathbb{Z}$.
6. $\mathbb{Q}(\omega_n)$ as splitting field of $x^n - 1$, which is separable, with $(\mathbb{Z}/n\mathbb{Z})^\times$ under multiplication.

Proposition 8.41. Let $k \subset F$ be Galois, and $k \subset E \subset F$, then
$$[F : E] = |\mathrm{Aut}_E(F)|$$
and $E \subset F$ is also Galois. Moreover,
$$[E : k] = [\mathrm{Aut}_k(F) : \mathrm{Aut}_E(F)]$$

Proposition 8.42. The Galois correspondence is inclusion-reversing:

$$\begin{tikzcd} F \arrow[d, dash] & & \mathrm{Aut}_F(F) = \{e\} \arrow[d, dash] \\ E \arrow[d, dash] & & \mathrm{Aut}_E(F) \arrow[d, dash] \\ k & & \mathrm{Aut}_k(F) \end{tikzcd}$$

Note that

$$|\mathrm{Aut}_E(F)| = [F : E]$$

Example 8.17. The extension

$$\mathbb{F}_2 \subset \mathbb{F}_8 \subset \mathbb{F}_{64}$$

corresponds to subgroup

$$\mathrm{Aut}_{\mathbb{F}_8}\mathbb{F}_{64} = [\mathbb{F}_{64} : \mathbb{F}_8] \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Proposition 8.43. Let $k \subset F$ be Galois, then $k \subset E \subset F$, $k \subset E$ is Galois iff $\mathrm{Aut}_E(F)$ is normal in $\mathrm{Aut}_k(F)$. In this case,

$$\mathrm{Aut}_k(E) \cong \frac{\mathrm{Aut}_k(F)}{\mathrm{Aut}_E(F)}$$

Recall that

$$[E : k] = [\mathrm{Aut}_k(F) : \mathrm{Aut}_E(F)]$$

Proposition 8.44. Consider $k \subset F$ Galois, and $k \subset K$ any finite extension, then $K \subset KF$ is Galois, and

$$\mathrm{Aut}_K(KF) \cong \mathrm{Aut}_{K\cap F}(F)$$

$$\begin{tikzcd} & KF \arrow[dl, dash] \arrow[dr, dash, "\text{Galois}"] & \\ F \arrow[dr, dash, "\text{Galois}"'] & & K \arrow[dl, dash] \\ & F \cap K \arrow[d, dash] & \\ & k & \end{tikzcd}$$

8.6

Definition 8.17 (symmetric functions)**.** Consider $P_n(x) = (x - t_1)\dots(x - t_n) \in \mathbb{Z}[t_1, \dots, t_n]$, and consider its coefficients

$$P_n(x) = x^n - s_1(t_1, \dots, t_n)x^{n-1} + \cdots + (-1)^n s_n(t_1, \dots, t_n)$$

are elementary symmetric functions of $t_1, \dots, t_n$. For example, when $n = 3$, the symmetric functions are

$$s_1 = t_1 + t_2 + t_3, s_2 = t_1t_2 + t_1t_3 + t_2t_3, s_3 = t_1t_2t_3$$

Proposition 8.45. Let k be a field, and $\varphi \in k(t_1, \dots, t_n)$, then φ is symmetric iff φ is a rational function of elementary symmetric functions $s_1, \dots, s_n$.

Proof. Let $k' = k(s_1, \dots, s_n)$ and $F = k(t_1, \dots, t_n)$, then $k' \subset F$ is Galois because F is the splitting field of the separalbe polynomial $P_n(x)$ over k'. The symmetric group S_n acts on F by permuting $t_1, \dots, t_n$, and S_n is the identity on k'. Thus S_n is a subgroup of $\mathrm{Aut}_{k'}(F)$, i.e., $n! \leq [F : k'] \leq n!$, where the second inequality follows from degree of $P_n(x)$. This implies that

$$\mathrm{Aut}_{k'}(F) = S_n, k' = k(s_1, \dots, s_n) = F^{S_n}$$

We reiterate:

$$k(s_1, \dots, s_n) \subset k(t_1, \dots, t_n)$$

is Galois, with Galois group S_n. □

Proposition 8.46. As a corollary, every finite group G can be realized as the Galois group of some extension.

Proposition 8.47. Next we construct Galois extension with Galois group A_n: recall

$$\Delta = \prod_{1 \leq i < j \leq n} (t_i - t_j)$$

Then

$$k(s_1, \dots, s_n)(\Delta) \subset k(t_1, \dots, t_n)$$

is Galois, with Galois group A_n.

Proof. Δ has degree 2 over $k(s_1, \dots, s_n)$ because

$$\Delta^2 = D = \prod_{i<j} (t_i - t_j)^2 \in k(s_1, \dots, s_n)$$

and the only transitive subgroup of index 2 is A_n. □

Proposition 8.48. Let k be a field of characteristic 0, and $f(x) \in k[x]$ be an irreducible polynomial. Then $f(x)$ is solvable by radicals iff its Galois group is solvable.

Proposition 8.49. (This may seem repetitive). Let $f(x) \in k[x]$ be an irreducible separable polynomial of degree n, then $\mathrm{Gal}_k(f(x))$ acts transitively on the set of roots of f in $\bar{k}$, i.e., $\mathrm{Gal}_k(f(x))$ can be identified as a subgroup of S_n.

Example 8.18. The only transitive subgroups of S_3: S_3 and A_3. This implie that an irreducible cubic separable polynomial can only have Galois group A_3 or S_3.

Example 8.19. The only transitive subgroups of S_4:

$$S_4, A_4, D_8, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$$

Definition 8.18 (discriminant). Let $f \in k[x]$ be separable, and $\alpha_1, \ldots, \alpha_n$ be its roots in some splitting field, then the **discriminant** of f is

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

We notice that D is always fixed by Galois group G, whereas Δ is fixed by G iff $G \subset A_n$.

Proposition 8.50. Let k be field of characteristic $\neq 2$, let $f(x) \in k[x]$ be a separable polynoimal, with discriminant D. Then the Galois group of $f(x)$ is contained in A_n iff D is a square in k, i.e., $\Delta \in k$.

Example 8.20. For S_3: the Galois group is A_3 if D is a square, and S_3 if it is not a square.

Proposition 8.51. Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p, where p is prime. Assume that f has exactly 2 complex roots, then the Galois group is S_p.

Proof. G is a subgroup of S_p: complex conjugation gives an order 2 element of G; we also know p divides $|G|$, thus there exists an element of order p, which is a p-cycle, i.e., they generate S_p. □

Proposition 8.52. 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 $p_i \equiv 1 \mod n_i$. Let $n = p_1 \ldots p_r$, 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 $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n))$, H corresponds to an intermediate field F, where

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

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

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

□

Warning 8.4. If you are just given irreducible f, asked to compute the Galois group of f: remember the degree of extension could be as large as $\deg(f)!$.

Warning 8.5. Sometimes we get asked to find Gal(f), if it's irreducible, then

Proposition 8.53. Let $k \subset F$ be Galois, fix $H \subset$ Gal(F/k), for any element $\alpha \in L$, then

$$\sum_{h \in H} h(\alpha), \quad \prod_{h \in H} h(\alpha)$$

are in L^H.

This is $\mathrm{tr}_{L/L^H}(m_\alpha)$, where m_α is the multiplication by α, and similarly the determinant.

Chapter 9

Field Theory-Hilbert's Nullstellensatz

This corresponds to Aluffi Chapter VII 2.2-2.3.

Proposition 9.1. For a field K, TFAE:

1. K is algebraically closed.
2. There is no algebraic extension over K except for the trivial one.
3. If $K \subset L$ is any extension, and $\alpha \in L$ is algebraic over K, then $\alpha \in K$.

Definition 9.1 (algebraic closure)**.** An algebraic closure of a field k is the algebraic extension such that $\bar{k}$ is algebraically closed.

Proposition 9.2 (Hilbert's Nullstellensatz)**.** Recall that if K is algebraically closed, then every maximal ideal in $K[x]$ is of the form $(x-\alpha), \alpha \in K$.

Proposition 9.3. Let K be algebraically closed, and $I \subset K[x_1, \ldots, x_n]$ be an ideal, then I is maximal iff

$$I = (x_1 - c_1, \ldots, x_n - c_n)$$

for some $c_1, \ldots, c_n \in K$.

Proposition 9.4 (normal basis theorem)**.** Let $k \subset K$ be a Galois extension of degree n, let $\{\sigma_1, \ldots, \sigma_n\}$ be the elements of the Galois group, then there exists $w \in K$ such that

$$\{\sigma_1(w), \ldots, \sigma_n(w)\}$$

forms a basis of K over k.

Proposition 9.5. Let $k \subset k(\alpha)$ be a simple extension, then for $f(\alpha) = 0$,

$$[k(\alpha) : k] \leq (\deg(f))$$

and the splitting field F

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

Chapter 10

Representation Theory of Finite Groups

Let k be a field and G be a finite group, a representation $\rho : G \to \mathrm{GL}(V)$ is such that

$$\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$$

And V is a $k[G]$-module, i.e., elements in $k[G]$ are of the form

$$\sum_{g \in G} a_g g$$

and they act on V by

$$\left(\sum_{g \in G} a_g g \right) \cdot v = \sum_{g \in G} a_g \left(\rho(g)(v) \right)$$

Proposition 10.1. The only two-sided ideals of $M_2(\mathbb{R})$ is $\{0\}$ and $M_2(\mathbb{R})$.

Proposition 10.2. Let k be a field, then every finite-dimensional k-algebra is left and right Noetherian and Artinian

Proposition 10.3. Let R be a commutative ring, then if R is Artinian, then R is Noetherian.

Hard proof.

Definition 10.1 (representation)**.** Representation of G over k is a homomorphism $\rho : G \to \mathrm{GL}(V)$ for some vector space V over k, a representation can also be defined as a kG-module, where elements in the ring kG are of the form

$$\sum_{g \in G} a_g g, a_g \in k$$

i.e., k-linear combinations of group elements.

An invariant subspace of $W \subset V$ is such that for all $w \in W, g \in G$, we have

$$\rho(g) w \in W$$

i.e., an kG-submodule.

Definition 10.2 (homomorphism between kG-modules)**.** Let $f : V \to W$ be kG-modules, then f is a homomorphism iff

$$f(\rho(g) v) = \rho(g) f(v)$$

Proposition 10.4 (Mascheke's theorem)**.** Let V be a representation of a finite group G over k, and let $|G|$ be invertible (nonzero in characteristic 0, and not divisible by p in char p). Let W be an invariant subspace of V, then there exists an invariant subspace W' such that

$$V = W \oplus W'$$

In other words, if V is not irreducible, then it can be decomposed into irreducible representations.

Definition 10.3 (semisimple)**.** A R-module M is semisimple iff M can be written as a finite direct sum of simple modules.

$$M \cong M_1 \oplus \cdots \oplus M_k$$

where M_i's are simple R-modules.

Proposition 10.5. Let k be a field and $|G|$ is invertible, then every finite-dimensional kG-module is semisimple: it can be decomposed into a finite direct sum of simple kG-submodules.

Proposition 10.6. Let ρ be a finite-dimensional representation of G over $\mathbb{C}$, then for every $g \in G$, the matrix $\rho(g)$ is diagonalizable.

Proposition 10.7 (Schur's lemma)**.** Let S_1, S_2 be simple R-modules, where R is a finite-dimensional algebra over k (finite-dimensional vector space but you can multiply things), then

$$\mathrm{Hom}_R(S_1, S_2) = \begin{cases} 0, & \text{if } S_1 \ncong S_2 \\ k, & \text{if } S_1 \cong S_2 \end{cases}$$

Equivalently, let V, W be irreducible representations of a finite group G, then V, W are kG-modules, where kG is a finite-dimensional k-algebra. Thus,

$$\mathrm{Hom}_k(V, W) = \begin{cases} k, V \cong W \\ 0, & \text{if not} \end{cases}$$

any map $\varphi : V \to V$ is a multiplication by scalar $\lambda \in k$.

Warning 10.1. This assumes k is algebraically closed!

Definition 10.4 (semisimple ring)**.** A ring R is semisimple iff

1. Every R-module is semisimple.
2. R can be writte as

$$R \cong I_1 \oplus \cdots \oplus I_k$$

where I_i are simple ideals.

Proposition 10.8 (Artin-Wedderburn). A **finite-dimensional k-algebra** R is semisimple iff

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

where $M_{n_i}(D_i)$ is the matrix rings over division rings D_i. If k is algebraically closed, then

$$R \cong M_{n_1}(k) \oplus \cdots \oplus M_{n_k}(k) \cong V_1 \oplus \cdots \oplus V_k$$

The **example for finite-dimensional k-algebra** is kG, where G is finite.

Proposition 10.9. Let k be algebraically closed, and G is finite, then

$$kG \cong M_{n_1}(k) \oplus \cdots \oplus M_{n_k}(k)$$

Thus

$$|G| = \sum_{i=1}^{k} n_i^2$$

where $n_i = \dim(V_i)$.

10.1 Characters

Proposition 10.10. Some basic properties of χ, let ρ be a representation of G over $\mathbb{C}$, and $\chi(g) = \text{tr}(\rho(g))$, then

1. $\chi(1) = \dim \rho$.
2. Let $g \in G$ have order n, then $\chi(g)$ is a sum of nth roots of unity.
3. $|\chi(g)| \leq \chi(1)$, with equality iff $\rho(g)$ is a multiplication by scalar.
4. $\chi(g) = \chi(1)$ iff $\rho(g) = \text{id}$.
5. $\chi(g^{-1}) = \overline{\chi(g)}$.
6. $\chi(g) = \chi(h)$ if g, h are conjugates.
7. If V, W are isomorphic $\mathbb{C}G$-modules, then $\chi_V = \chi_W$.

We can extend characters onto larger representations:

Proposition 10.11. Let V, W be finite dimensional representations of G over k of char 0, then

1. $V \oplus W$ has character $\chi_V \oplus \chi_W$.
2. $V \otimes W$ has character $\chi_V \cdot \chi_W$.
3. V^* has character $\chi_{V^*}(g) = \overline{\chi_V(g)}$.
4. $\text{Hom}_k(V, W)$ has character $\chi_{V^*} \cdot \chi_W$.

Proposition 10.12 (Row Orthogonality)**.** Let G be finite, and V, W be irreducible complex representations of G with characters χ_V, χ_W, then

$$\langle \chi_V, \chi_W \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)\overline{\chi_W(g)} = \begin{cases} 1, V \cong W \\ 0, \text{ otherwise} \end{cases}$$

Proposition 10.13. Let V be a $\mathbb{C}G$-module, then in any expression

$$V \cong S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$$

where S_i are non-isomorphic irreducible modules, we have

$$n_i = \langle \chi_V, \chi_{S_i} \rangle$$

where χ_V, χ_{S_i} are characters of V, S_i.

Warning 10.2. We can use the above to decompose any representation into irreducible ones, and the powers n_i can be determined by taking the inner product.

Example 10.1. Let V be the 2-dimensional representation of S_3, then we can consider $V \otimes V$, then $\chi_2 \otimes \chi_2$ is a character of $V \otimes V$, now we decompose $V \otimes V$ into irreducible representations:

$$\langle \chi_2 \otimes \chi_2, \chi_{\text{triv}} \rangle = 1$$

and similarly

$$\langle \chi_2 \otimes \chi_2, \chi_{\text{sgn}} \rangle = 1, \langle \chi_2 \otimes \chi_2, \chi_2 \rangle = 1$$

Thus we see

$$V \otimes V \cong \mathbb{C} \oplus S \oplus V$$

where V is the trivial and S is the sign representation.

Proposition 10.14. For finite dimensional complex representations V, W, then

$$V \cong W \iff \chi_V(g) = \chi_W(g), \text{ for all } g \in G$$

Moreover,

$$\langle \chi, \chi \rangle = 1$$

iff χ is irreducible.

Proof. We write $V \cong S_1^{n_1} \oplus \ldots S_k^{n_k}$, then the inner product being 1 implies

$$\sum_{i=1}^{k} n_i^2 = 1$$

which implies there exists only one nonzero $n_i = 1$, i.e., $V \cong S_i$. □

Proposition 10.15 (orthogonality)**.** Let $\chi_1, \dots, \chi_k$ be the irreducible complex characters of G, with dimensions $d_1, \dots, d_k$, then

1. $|G| = \sum_{i=1}^k d_i^2$.
2. $\sum_{i=1}^k d_i \chi_i(g) = 0$, if $g \neq 1$.

Proposition 10.16. For any commutative ring R, the center

$$Z(M_n(R)) = \{\lambda I : \lambda \in R\} \cong R$$

Proposition 10.17 (column orthogonality)**.** Let χ_i be the irreducible representations of G, then

$$\sum_{i=1}^k \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |Z_G(g)|, & \text{if } g, h \text{ are conjugates} \\ 0, & \text{if not} \end{cases}$$

where $Z_G(g)$ is the centralizer of g.

Proposition 10.18 (all orthogonality relations)**.** You have

1. Row orthogonality: $\sum_{g \in G} \chi_V(g)\overline{\chi_W(g)} = \begin{cases} |G|, & \text{if } V \cong W \\ 0, & \text{if not} \end{cases}$.
2. Dimension orthogonality: $\sum_{i=1}^k d_i \chi_i(g) = 0$.
3. Column orthogonality: $\sum_{i=1}^k \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |Z_G(g)|, & \text{if } g, h \text{ are conjugates} \\ 0, & \text{if not} \end{cases}$.

Proposition 10.19. The dimension of an irreducible complex representation divides $|G|$.

Proposition 10.20 (characters of cyclic groups)**.** Let $G = \langle g : g^n = 1 \rangle$ be cyclic, and ω_n be the primitive nth root of unity, then the irreducible complex characters of G are

$$\chi_i : g \mapsto \omega_n^i$$

where $0 \leq i \leq n-1$. These are exactly the n irreducible characters of G.

Example 10.2. Consider the character table for $\mathbb{Z}/4\mathbb{Z}$, $1 \mapsto 1, i, -1, -i$ defines 4 one-dimensional irreducible representations.

Proposition 10.21. Let $V_1, \dots, V_n$ and $W_1, \dots, W_m$ be the irreducible representations of G_1, G_2, then

$$V_i \otimes W_j$$

is the complete list of irreducible representations of $G_1 \times G_2$. As a consequence, the character table of $G_1 \times G_2$ is the tensor product of the character tables of G_1 and G_2.

Proposition 10.22. G is abelian iff all complex irreducible representations of G are one-dimensional.

Proof. We know cyclic groups have one-dimensional irreducible representations, and every finite abelian group is a direct product of cyclic groups, hence by the above, we know they are again one-dimension. Conversely, consider

$$|G| = \sum_{i=1}^{r} d_i^2$$

This implies $r = |G|$, i.e., every conjugacy class has size 1, i.e., G is abelian. □

Proposition 10.23. The one-dimensional irreducible representations of G exactly corresopnd to the one-dimensional representations of $G^{\text{ab}} = \frac{G}{[G:G]}$.

(You put 1's at $[G, G]$), think about D_8.

Proposition 10.24. Let $\chi_1, \ldots, \chi_n$ be pairwise distinct one-dimensional characters over k, then $\chi_1, \ldots, \chi_n$ are linearly independent over k.

10.2 Induction and Restriction

Definition 10.5 (Induced Representation). Let H be a subgroup of G, let V be a kG-module. Let $g_1H, \ldots, g_{[G:H]}H$ be the list of left cosets of G/H. Then

$$\text{Ind}_H^G(V) = \bigoplus_{i=1}^{[G:H]} g_i \otimes V$$

where

$$g_i \otimes V = \{g_i \otimes v : v \in V\}$$

note that if $g \in G$, then

$$g(g_i \otimes V) = g_j \otimes V$$

where $gg_i = g_jh$ for some $h \in H$. Note that $g_i \otimes V \cong V$ for each i.

The $g_i \otimes V$ submodules of $\text{Ind}_H^G(V)$ are permuted under the action of G, which is transitive.

Definition 10.6 (Induced character). Let H be a subgroup of G, let V be a $\mathbb{C}H$-module with character χ. Then the induced character on G is

$$\text{Ind}_H^G(\chi)(g) = \frac{1}{|H|} \sum_{t \in G : t^{-1}gt \in H} \chi(t^{-1}gt)$$

Example 10.3. Consider $G = S_3$, $H = \langle (123) \rangle$, and let χ be the trivial representation on H, then

$$\text{Ind}_H^G \chi(g) = \begin{cases} 2, g = e \\ 0, g = (12) \\ 2, g = (123) \end{cases}$$

Proposition 10.25 (Frobenius reciprocity)**.** Let $\mathrm{Res}_H^G(V)$ be the restriction of representation of V on G to H. Let $H \subset K \subset G$ be subgroups of G and V be a kH-module and W be a kG-module.

$$\mathrm{Hom}_{kG}(\mathrm{Ind}_H^G V, W) \cong \mathrm{Hom}_{kG}(V, \mathrm{Res}_H^G W)$$

and similarly,

$$\mathrm{Hom}_{kG}(W, \mathrm{Ind}_H^G V) \cong \mathrm{Hom}_{kG}(\mathrm{Res}_H^G W, V)$$

Proposition 10.26. Some more properties of induction and restriction:

1. $\mathrm{Ind}_K^G \mathrm{Ind}_H^K V \cong \mathrm{Ind}_H^G V$.
2. Similarly for restrictions.
3. $\mathrm{Ind}_H^G V \cong \mathrm{Hom}_{kH}(kG, V)$ as kG-modules.

Proposition 10.27 (Frobenius reciprocity for characters)**.** Let ψ, χ be complex characters of G.

$$\langle \mathrm{Ind}_H^G \chi, \psi \rangle_G = \langle \chi, \mathrm{Res}_H^G \psi \rangle_H$$

Proposition 10.28. Let V be a representation of G over k whose characteristic is not 2, then

$$V \otimes V \cong S^2(V) \oplus \wedge^2(V)$$

Moreover,

$$S^2\chi(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$$

and

$$\wedge^2(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$$

Warning 10.3. So how to construct character tables.

Proposition 10.29.

1. Find the number of conjugacy classes of G (to identify the size of the table).
2. Take the abelianization $G/[G, G]$ to find all the one-dimensional characters.
3. For characters of dimension greater than 1:
   (a) Find the natural representations.
   (b) Find representations lifted from quotient groups.
   (c) Representations induced from subgroups.
   (d) Tensor products of other representations.
   (e) Symmetric and alternating powers of representations.

Keep in mind of **Frobenius Reciprocity** and **Orthogonality Relations**.

Proposition 10.30. Suppose an abelian group G admits a faithful representation, then show G is cyclic.