Graduate Algebra

Concise Notes

Konstantinos Bizanos

Columbia, Missouri
June 9, 2026

Contents

Preface

This set of notes is based on the Graduate Algebra course taught by Professor Dan Edidin during both the Fall and Spring semesters. The notes follow, to a large extent, the structure of Hungerford's book Algebra; however, an important number of sections have been modified.

This set of notes is far from being well written and, at this point, cannot be considered a proper set of notes for independent study, since it is not even completed yet (:( ). Some fundamental definitions and results from group and ring theory, such as the definition of a group and a ring, normal subgroups and ideals, Lagrange's Theorem, the First Isomorphism Theorem, etc., have been omitted from these notes. They can, however, be found in Hungerford's book.

These notes are still under construction, and it is expected that some important sections concerning polynomial rings, field theory, and the Fundamental Theorem of Galois Theory will be incorporated in future versions.

For any typos or (vital) mistakes, feel free to contact me at: kbfg6@missouri.edu

Chapter 1

Group Theory

1.1 Group Actions

Definition 1.1.1 (Action of a group on a set)**.** An **action** of a group G on a set S is a function $G \times S \to S$ (usually denoted by $(g, x) \mapsto gx$) such that for all $x \in S$ and $g_1, g_2 \in G$:

$$ex = x \qquad \text{and} \qquad (g_1 g_2)x = g_1(g_2 x).$$

When such an action is given, we say that G acts on the set S.

Since there may be many different actions of a group G on a given set S, the notation gx is ambiguous. In context, however, this will not cause any difficulty.

In the following examples we are going to demonstrate some actions which are going to be used multiple times either in the proofs of some theoretical results or exercise.

Example 1.1.1. An action of the symmetric group S_n on the set $\mathrm{I}_n = \{1, 2, \ldots, n\}$ is given by

$$(\sigma, x) \mapsto \sigma(x).$$

Example 1.1.2. Let G be a group and H a subgroup. An action of the group H on the set G is given by

$$(h, x) \mapsto hx,$$

where hx is the product in G. The action of $h \in H$ on G is called a (left) translation. If K is another subgroup of G and S is the set of all left cosets of K in G, then H acts on S by translation:

$$(h, xK) \mapsto hxK.$$

Example 1.1.3. Let H be a subgroup of a group G. An action of H on the set G is given by

$$(h, x) \mapsto hxh^{-1};$$

to avoid confusion with the product in G, this action of $h \in H$ on G is always denoted by hxh^{-1} and not hx. This action of $h \in H$ on G is called conjugation by h and the element hxh^{-1} is said to

be a conjugate of x.

If K is any subgroup of G and $h \in H$, then hKh^{-1} is a subgroup of G isomorphic to K. Hence H acts on the set S of all subgroups of G by conjugation:

$$(h, K) \mapsto hKh^{-1}.$$

The group hKh^{-1} is said to be conjugate to K.

Theorem 1.1.1. Let G be a group that acts on a set S.

a. The relation on S defined by

$$x \sim x' \iff gx = x' \quad \text{for some } g \in G$$

is an equivalence relation.

b. For each $x \in S$, $G_x = \{g \in G \mid gx = x\}$ is a subgroup of G.

Proof. Problem 1.1 □

The equivalence classes of the equivalence relation of Theorem 1.1.1 are called the **orbits** of G on S; the orbit of $x \in S$ is denoted $\mathscr{O}(x)$. The subgroup G_x is called variously the **subgroup fixing** x, the **isotropy group** of x or the **stabilizer** of x.

Example 1.1.4. If a group G acts on itself by conjugation, then the orbit

$$\mathscr{O}(x) = \{gxg^{-1} \mid g \in G\}$$

of $x \in G$ is called the **conjugacy class** of x. If a subgroup H acts on G by conjugation the isotropy group

$$H_x = \{h \in H \mid hxh^{-1} = x\} = \{h \in H \mid hx = xh\}$$

is called the **centralizer** of x in H and is denoted $\mathrm{C}_H(x)$. If $H = G$, $\mathrm{C}_G(x)$ is simply called the **centralizer** of x. If H acts by conjugation on the set S of all subgroups of G, then the subgroup of H fixing $K \in S$, namely

$$\{h \in H \mid hKh^{-1} = K\},$$

is called the **normalizer** of K in H and denoted $\mathrm{N}_H(K)$. The group $\mathrm{N}_G(K)$ is simply called the **normalizer** of K. Clearly every subgroup K is normal in $\mathrm{N}_G(K)$; K is normal in G if and only if $\mathrm{N}_G(K) = G$.

Theorem 1.1.2. If a group G acts on a set S, then

$$|\mathscr{O}(x)| = [G : G_x] \tag{1.1}$$

Proof. Let $g, h \in G$. Since

$$gx = hx \iff g^{-1}hx = x \iff g^{-1}h \in G_x \iff hG_x = gG_x,$$

it follows that the map given by $gG_x \mapsto gx$ is a well-defined bijection of the set of cosets of G_x in G onto the orbit $\mathscr{O}(x)$. Hence, $|\mathscr{O}(x)| = [G : G_x]$. □

Corollary 1.1.1. Let G be a finite group and K a subgroup of G.

a. The number of elements in the conjugacy class of $x \in G$ is $[G : \mathrm{C}_G(x)]$, which divides $|G|$;

b. if $\mathscr{O}(x_1), \ldots, \mathscr{O}(x_n)$ $(x_i \in G)$ are the distinct conjugacy classes of G, then

$$|G| = \sum_{i=1}^{n} [G : \mathrm{C}_G(x_i)];$$

c. the number of subgroups of G conjugate to K is $[G : \mathrm{N}_G(K)]$, which divides $|G|$.

Proof. Problem 1.2. □

The equation

$$|G| = \sum_{i=1}^{n} [G : \mathrm{C}_G(x_i)] \tag{1.2}$$

as in Corollary 1.1.1 is called the **class equation** of the finite group G.

Theorem 1.1.3. If a group G acts on a set S, then this action induces a homomorphism $G \to A(S)$, where $A(S)$ is the group of all permutations of S.

Proof. Problem 1.3. □

Corollary 1.1.2 (Cayley)**.** If G is a group, then there is a monomorphism $G \to A(G)$. Hence, every group is isomorphic to a group of permutations. In particular, every finite group is isomorphic to a subgroup of S_n with $n = |G|$.

Proof. Let G act on itself by left translation and apply Theorem 1.1.3 to obtain a homomorphism $\tau : G \to A(G)$. So that this homomorphism is injective. To prove the last statement note if $|G| = n$, then $A(G) \cong S_n$. □

Corollary 1.1.3. Let G be a group.

a. For each $g \in G$, conjugation by g induces an automorphism of G.

b. There is a homomorphism $G \to \operatorname{Aut} G$ whose kernel is

$$\mathrm{C}(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

Proof. Consider the action of G in G by conjugation and the corresponding group homomorphism

$$\tau \colon G \to A(G), \quad g \mapsto \tau_g \quad \left[\tau_g(x) = gxg^{-1}\right]$$

Show that τ_g is an automorphism, for all $g \in G$, and that $\ker \tau = \mathrm{C}(G)$. □

Remark 1.1.1. The automorphism τ_g of 1.1.3 is called the **inner automorphism** induced by g. The normal subgroup $\mathrm{C}(G) = \ker \tau$ is called the **center** of G. An element is in the center if and only if it commutes with all elements in G, i.e., its orbit under the conjugacy action is a singleton. Consequently, the class equation of G may be written

$$|G| = |\mathrm{C}(G)| + \sum_{i=1}^{m} [G : \mathrm{C}_G(x_i)], \tag{1.3}$$

where $\mathscr{O}(x_1), \ldots, \mathscr{O}(x_m)$ are distinct conjugacy classes of G and each $[G : \mathrm{C}_G(x_i)] > 1$.

Remark 1.1.2. Inner automorphisms do not exhaust the group of automorphisms over a fixed group G. For example, over $\mathbb{Z}$, the map $n \mapsto -n$ is an automorphism, nevertheless it is not inner. However, there are some important groups such as $\mathfrak{S}_n$, where all automorphisms are inner (Problem 1.17). In Problem 1.16 one can show that the group of inner automorphisms $\operatorname{Inn}(G)$ is a normal subgroup of $\operatorname{Aut}(G)$. The quotient $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ is called the **group of outer automorphisms of** G. .

Proposition 1.1.1. Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proof. Show that the kernel of the corresponding homomorphism $G \to A(G/H)$ is the normal subgroup $K = \bigcap_{x \in G} xHx^{-1}$, which is obviously contained in H. □

Corollary 1.1.4. If H is a subgroup of index n in a group G and no nontrivial normal subgroup of G is contained in H, then G is isomorphic to a subgroup of $\mathfrak{S}_n$.

Proof. Apply Proposition 1.1.1, and use the fact that the kernel of the induced homomorphism is a normal subgroup which is contained in H. □

Corollary 1.1.5. If H is a subgroup of a finite group G of index p, where p is the smallest prime dividing the order of G, then H is normal in G.

Proof. Let $S = G/H$ be the set of all left cosets of H in G. Then $A(S) \cong \mathfrak{S}_p$, since $[G : H] = p$. If K is the kernel of the homomorphism $G \to A(S)$ of Proposition 1.1.1, then K is normal in G and contained in H. Furthermore, G/K is isomorphic to a subgroup of $\mathfrak{S}_p$. Hence, by Lagrange's theorem

$$|G : K| \,|\, |\mathfrak{S}_p| = p!$$

But every divisor of $|G/K| = [G : K]$ must divide $|G|$, so no number smaller than p (except 1) can divide $|G|$ [1], and we must have $|G/K| = p$ or 1. However

$$|G/K| = [G : K] = [G : H][H : K] = p[H : K] \geq p.$$

Therefore $|G/K| = p$ and $[H : K] = 1$, whence $H = K$. But K is normal in G. □

1.2 Sylow Theorems

Lemma 1.2.1. If a group H of order p^n (p prime) acts on a finite set S and if

$$S_0 = \{x \in S \mid hx = x \text{ for all } h \in H\},$$

then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $|\mathscr{O}(x)| = [H : H_x]$, then

$$\mathscr{O}(x) = \{x\} \iff H = H_x \iff x \in S_0$$

Hence S can be written as a disjoint union

$$S = S_0 \cup \mathscr{O}(x_1) \cup \cdots \cup \mathscr{O}(x_k),$$

with $|\mathscr{O}(x_i)| > 1$ for all i. Hence

$$|S| = |S_0| + |\mathscr{O}(x_1)| + \cdots + |\mathscr{O}(x_k)|.$$

[1] Check it in the case where $|G| = 75$ and $p = 3$. What does it mean that $[G : K] \mid 3$!? If you have convinced yourself, feel free to move to the general case.

Now $p \mid |\mathcal{O}(x_i)|$ for each i since

$$|\mathcal{O}(x_i)| = [H : H_{x_i}]\,|H|$$

and $|H| = p^n$. Therefore $|S| \equiv |S_0| \pmod{p}$. [2] □

Theorem 1.2.1 (Cauchy)**.** If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

Proof. Let S be the set of p-tuples of group elements

$$S = \{(a_1, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}.$$

Since a_p is uniquely determined by $(a_1 \cdots a_{p-1})^{-1}$, it follows that $|S| = n^{p-1}$, where $|G| = n$. Since $p \mid n$, $|S| \equiv 0 \pmod{p}$.

Let $\mathbb{Z}_p$ act on S by cyclic permutation:

$$\overline{k} \cdot (a_1, \ldots, a_p) = (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k).$$

This defines a group action. Now $(a_1, \ldots, a_p) \in S_0$ if and only if $a_1 = \cdots = a_p$. Since $(e, \ldots, e) \in S_0$, we have $|S_0| \neq 0$. By Lemma 1.2.1,

$$0 \equiv |S| \equiv |S_0| \pmod{p}.$$

Hence there are at least p elements in S_0, so there exists $a \neq e$ such that $(a, \ldots, a) \in S_0$, and hence $a^p = e$. Since p is prime, $|a| = p$. □

Corollary 1.2.1. The center $\mathrm{C}(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Problem 1.4. □

Lemma 1.2.2. If H is a p-subgroup of a finite group G, then

$$[\mathrm{N}_G(H) : H] \equiv [G : H] \pmod{p}.$$

[2] This is an interesting fact because the set S_0 or $\mathrm{Fix}(G)$ appears frequently in the group theory. For example if G acts with conjugacy in G, then $\mathrm{Z}(G) = \mathrm{Fix}(G)$. If H acts with left multiplication to the left coset G/H, then $\mathrm{Fix}(G) = N_G(H)/H$.

Proof. Let S be the set of left cosets of H in G. Then $|S| = [G : H]$. Let H act on S by left translation. Then

$$xH \in S_0 \iff hxH = xH, \quad \text{for all } h \in H \iff x^{-1}hx \in H, \quad \text{for all } h \in H \iff x \in \mathrm{N}_G(H).$$

Thus $|S_0| = [\mathrm{N}_G(H) : H]$. By Lemma 1.2.1,

$$[\mathrm{N}_G(H) : H] \equiv [G : H] \pmod{p}.$$

□

Corollary 1.2.2. If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $\mathrm{N}_G(H) \neq H$.

Proof.

$$0 \equiv [G : H] \equiv [\mathrm{N}_G(H) : H] \pmod{p}.$$

Hence $[\mathrm{N}_G(H) : H] > 1$ and so $\mathrm{N}_G(H) \neq H$. □

Theorem 1.2.2 (First Sylow Theorem)**.** Let G be a group of order $p^n m$, with p prime and $(p, m) = 1$.

Then G contains a subgroup of order p^i for each $0 \leq i \leq n$, and every subgroup of order p^i is normal in some subgroup of order p^{i+1}.

A subgroup P of G is called a **Sylow p-subgroup** if it is maximal among p-subgroups.

Corollary 1.2.3. Let G be a group of order $p^n m$ with $(p, m) = 1$ and H a p-subgroup.

a. H is Sylow if and only if $|H| = p^n$.

b. Conjugates of Sylow subgroups are Sylow.

c. If there is a unique Sylow subgroup, it is normal.

Proof. Problem 1.5 □

Theorem 1.2.3 (Second Sylow Theorem)**.** If H is a p-subgroup of G and P is a Sylow p-subgroup, then there exists $x \in G$ such that

$$H \subseteq xPx^{-1}.$$

In particular, any two Sylow p-subgroups are conjugate.

Proof. Let S be the set of left cosets of P. Let H act by left translation. Observe that $xP \in S_0$ if and only if $H \subseteq xPx^{-1}$. Hence, it suffices to show that $|S_0| > 1$. Now, since H is a p - group by Lemma 1.2.1 we get

$$|S_0| \equiv |S| \equiv |G/P| \pmod{p}.$$

But $p \nmid |G : P|$ since P is a Sylow p - subgroup of G, therefore $|S_0| > 1$. Hence there exists x such that $H \subseteq xPx^{-1}$. □

Theorem 1.2.4 (Third Sylow Theorem)**.** If G is a finite group and p a prime, then the number of Sylow p-subgroups divides $|G|$ and is of the form $kp+1$. In particular, if n_p is the number of Sylow p - subgroups then

$$n_p \equiv 1 \pmod{p} \tag{1.4}$$

Proof. By the second Sylow theorem, the number of Sylow p-subgroups is the number n_p of conjugates of any one of them, say P. But this number is $[G : \mathrm{N}_G(P)]$, a divisor of $|G|$. By Corollary 1.2.2 :

$$[\mathrm{N}_G(P) : P] \equiv [G : P] \pmod{p}$$

Hence, $[\mathrm{N}_G(P) : P] = [G : P] + kp$. Therefore, using the equality :

$$[G : P] = [G : \mathrm{N}_G(P)] \cdot [\mathrm{N}_G(P) : P]$$

we obtain

$$[G : P] = n_p \cdot ([G : P] + kp) \iff [G : P] \cdot (1 - n_p) = kp$$

Using the fact that $p \nmid [G : P]$, since P is a Sylow p - subgroup, we conclude that $p|1 - n_p$, and in particular

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

□

Theorem 1.2.5. If P is a Sylow p-subgroup of a finite group G, then

$$\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P).$$

Proof. Since P is normal in $\mathrm{N}_G(P)$, it is the unique Sylow p-subgroup of $\mathrm{N}_G(P)$. Now, for all $x \in \mathrm{N}_G(\mathrm{N}_G(P))$ we get :

$$P \subseteq \mathrm{N}_G(P) \Rightarrow xPx^{-1} \subseteq x\mathrm{N}_G(P)x^{-1} = \mathrm{N}_G(P).$$

Since xPx^{-1} is a Sylow p - subgroup of $\mathrm{N}_G(P)$, from the uniqueness part that we mentioned above we get $xPx^{-1} = P$. Therefore, $\mathrm{N}_G(\mathrm{N}_G(P)) \subseteq \mathrm{N}_G(P)$. The converse inclusion is obvious, thus we obtain the desired result. □

1.3 Nilpotent Groups

We already know that the center $\mathrm{C}(G)$ of a group G is a normal subgroup. Define $\mathrm{C}_0(G) = \langle e \rangle$, and $\mathrm{C}_i(G)$ the inverse image of $\mathrm{C}(G/\mathrm{C}_{i-1}(G))$ under the canonical projection $G \to G/\mathrm{C}_{i-1}(G)$, for $i = 1, 2, \ldots$. There is the ascending central series of G:

$$\mathrm{C}_0(G) = \langle e \rangle \leq \mathrm{C}_1(G) = \mathrm{C}(G) \leq \mathrm{C}_2(G) \leq \cdots .$$

In general, if $\mathrm{C}_i \leq \mathrm{C}_{i+1} \leq G$, and $\mathrm{C}_i \triangleleft G$, and in addition

$$\mathrm{C}_{i+1}/\mathrm{C}_i \triangleleft G/\mathrm{C}_i \quad \text{then} \quad \mathrm{C}_{i+1} \triangleleft G.$$

In particular, the last result follows from the subgroups correspondence between the normal subgroups of G and G/C_i. Therefore, $\mathrm{C}_i(G) \triangleleft G$ for all $i = 1, 2, \ldots,$ by induction. Also, for $i = 1, 2, \ldots,$

$$\mathrm{C}_i(G) = \{x \in G \mid xyx^{-1}y^{-1} \in C_{i-1}(G) \text{ for all } y \in G\}.$$

Definition 1.3.1. A group G is **nilpotent** if $\mathrm{C}_n(G) = G$ for some $n \in \mathbb{N}$.

Example 1.3.1. i. Every abelian group G is nilpotent since $\mathrm{C}_1(G) = \mathrm{C}(G) = G$.

ii. Every subgroup or homomorphic image of a nilpotent group is nilpotent. For the first claim, given a subgroup H of a nilpotent group G, intersect the ascending central series of G with H and the desired result follows immediately. For the second claim, check the Problem 1.30.

Theorem 1.3.1. Every finite p-group G is nilpotent.

Proof. We assume that $|G| = p^n$. If G is an abelian group, then we are done. Now, every nontrivial quotient group of G is a finite p-group. In particular, from Corollary 1.2.1 we get that $G/\mathrm{C}(G)$ is a non trivial p - group, and $|G/\mathrm{C}(G)| = p^k < p^n$. Continuing the process inductively, if $G/\mathrm{C}_i(G)$ is nontrivial, then $\mathrm{C}(G/\mathrm{C}_i(G))$ is nontrivial, so that $\mathrm{C}_i(G) \subsetneqq \mathrm{C}_{i+1}(G)$. Hence $\mathrm{C}_n(G) = G$ for some $n \in \mathrm{N}$. □

Theorem 1.3.2. If $G = G_1 \times \cdots \times G_k$, then G is nilpotent if and only if all G_j are nilpotent.

Proof. Problem 1.29. □

Lemma 1.3.1. Assume G is nilpotent. If $H \lneqq G$, then $H \lneqq \mathrm{N}_G(H)$.

Proof. Let n be the largest integer such that $\mathrm{C}_n(G) \leq H$. Choose $a \in \mathrm{C}_{n+1}(G) \setminus H$. This [3] and then for $h \in H$,

$$aha^{-1}h^{-1} \in \mathrm{C}_n(G) \leq H.$$

Thus $aha^{-1} \in H$. Hence $a \in N_G(H) \setminus H$. □

[3] Such n there exists because $H \subsetneqq G$ and there is m such that $\mathrm{C}_m(G) = G$, since G is nilpotent,

Theorem 1.3.3. A finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups.

Proof. If G is a direct product of Sylow subgroups, then G is nilpotent by Theorems 1.3.1 and 1.3.2. Conversely, suppose G is nilpotent. For every Sylow subgroup P of G, by Theorem 1.2.5 we obtain :

$$\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P).$$

Therefore, by the previous lemma, $\mathrm{N}_G(P) = G$. Hence P is normal in G. Suppose that $|G|$ has distinct prime factors $p_1, p_2, \ldots, p_k$. For each p_i, there is a unique Sylow p_i-subgroup $P_i \triangleleft G$. Then

$$\langle P_1, P_2, \ldots, P_k \rangle = P_1 P_2 \cdots P_k.$$

Moreover,

$$P_i \cap (P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_k) = \{e\}$$

by investigating the possible orders of its elements. Therefore,

$$P_1 P_2 \cdots P_k = P_1 \times P_2 \times \cdots \times P_k.$$

Thus, $G = P_1 \times P_2 \times \cdots \times P_k$ by comparing their orders. □

Corollary 1.3.1. If G is a finite nilpotent group, then G contains a subgroup of order n for any factor n of $|G|$.

1.4 Solvable Groups

Definition 1.4.1. Let G be a group. For $a, b \in G$, the element $aba^{-1}b^{-1}$ is called a **commutator** . The subgroup of G generated by all commutators:

$$G' := \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$$

is called the **commutator subgroup** of G.

Theorem 1.4.1.

a. The commutator group G' is a characteristic subgroup of G, i.e. for all $\in \mathrm{Aut}(G)$, then $\varphi(G') \subseteq G'$. In particular, G' is a normal subgroup of G.

b. Moreover, G' is the smallest normal subgroup such that G/G' is abelian. Precisely, if $N \subseteq G$ is a normal subgroup, then G/N is abelian if and only if $G' \leq N \leq G$.

Proof. Problem 1.32. □

Definition 1.4.2. For a group G, let $G^{(0)} := G$ and $G^{(k)} := \left(G^{(k-1)}\right)'$, for $i = 1, 2, \ldots$. Then

$$G^{(0)} = G \geq G^{(1)} = G' \geq G^{(2)} \geq \cdots,$$

where $G^{(k)}$ is called the k-th **derived subgroup** of G. It can be shown that $G^{(k)} \triangleleft G$ for all k. (Problem 1.33).

Definition 1.4.3. A group G is said to be **solvable** if $G^{(n)} = \langle e \rangle$, for some $n \in \mathbb{N}$.

Proposition 1.4.1. Every nilpotent group is solvable.

Proof. Since $\mathrm{C}_i(G)/\mathrm{C}_{i-1}(G)$ is abelian, from Theorem 1.4.1 we have $\mathrm{C}_i(G)' \leq \mathrm{C}_{i-1}(G)$. If $\mathrm{C}_n(G) = G$, then

$$G^{(n)} = (\mathrm{C}_n(G))^{(n)} \leq (\mathrm{C}_{n-1}(G))^{(n-1)} \leq \cdots \leq \mathrm{C}_0(G) = \langle e \rangle.$$

□

Theorem 1.4.2. The following hold:

a. Every subgroup or homomorphic image of a solvable group is solvable.

b. If N is a normal subgroup of G, and N and G/N are solvable, then G is solvable. In other words, solvability is closed under extensions.

Proof. a. Suppose that G is solvable. If H is a subgroup of G, then $H^{(k)} \leq G^{(k)}$. One can check this for $k = 1$, since every commutator of H is a commutator of G. The result then follows immediately by induction on k. Hence, H is solvable.

If $f : G \to H$ is a group homomorphism, then it is left as an exercise to show that $f\left(G^{(k)}\right) = f(G)^{(k)}$, for all $k \in \mathbb{N}$. Hence, $f(G)$ is solvable.

b. Assume that N is a normal subgroup of G, and N and G/N are solvable. Then

$$N = N^{(0)} > N^{(1)} > \cdots > N^{(s)} = \langle e \rangle$$

and

$$G/N = (G/N)^{(0)} > (G/N)^{(1)} > \cdots > (G/N)^{(t)} = \{N\}$$

for some $s, t \in \mathbb{N}$. Show that $G^{(k)}N/N = (G/N)^{(k)}$, so that $G^{(t)} = N$. Therefore, consider the series :

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(t)} = N \supseteq G^{(t+1)} = N^{(1)} \supseteq \cdots \subseteq G^{(t+s)} = N^{(s)} = \langle e \rangle.$$

Hence, G is a solvable group.

□

Corollary 1.4.1. The symmetric group $\mathfrak{S}_n$ for $n \geq 5$ is not solvable.

A generalization of the Sylow theorems for finite solvable groups is below.

Proposition 1.4.2 (P. Hall)**.** Let G be a finite solvable group of order mn, with $\gcd(m, n) = 1$. Then:

1. G contains a subgroup of order m; conversely, if G is a finite group such that whenever $|G| = mn$ with $\gcd(m, n) = 1$, G has a subgroup of order m, then G is solvable.
2. Any two subgroups of G of order m are conjugate.
3. Any subgroup of G of order k, where $k \mid m$, is contained in a subgroup of order m.

The proof is skipped. P. Hall also showed that if G is a finite group having a p-complement for every prime factor p of $|G|$, then G is solvable.

1.5 Problems

Problem 1.1. Prove Theorem 1.1.1.

Problem 1.2. Prove Corollary 1.1.1

Problem 1.3. Prove 1.1.3.

Problem 1.4. Prove Corollary 1.2.1.

Problem 1.5. Prove Corollary 1.2.3.

Problem 1.6. a. Let p be a fixed prime. Let $\mathbf{R}_p$ be the set of rational numbers whose denominator is relatively prime to p. Likewise let $\mathbf{R}^p$ be the set of rational numbers whose denominator is a non-negative power of p.

Prove that $\mathbf{R}_p$ and $\mathbf{R}^p$ are both subgroups of the additive group $(\mathbb{Q}, +)$.

b. Show that

$$\mathbb{Z}(p^\infty) = \left\{ \frac{a}{b} \in \mathbb{Q}/\mathbb{Z} \;\middle|\; a, b \in \mathbb{Z} \text{ and } b = p^n,\ n \geq 0 \right\}$$

is a subgroup under addition.

Problem 1.7. a. Prove that if

$$a^2 = e, \quad \text{for all } a \in G$$

then G is abelian.

b. Prove that any group of order four is abelian. Show that there are exactly two such groups.

Problem 1.8. a. Write down 8 matrices that represent the dihedral group d_4 as a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

b. Prove that the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by the matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

is a non-abelian group of order 8 which is not isomorphic to the dihedral group d_4. This group is called the **quaternion group** Q_8.

Problem 1.9. Show that the matrix

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

has order 4 and the matrix

$$b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

has order 3, but the product ab has infinite order.

Problem 1.10. Let Z_n be a cyclic group of order n (written multiplicatively) and for each integer a let

$$\sigma_a : Z_n \to Z_n, \qquad \sigma_a(x) = x^a, \ \forall x \in Z_n.$$

a. Prove that $\sigma_a \in \mathrm{Aut}(Z_n)$ if and only if $(a, n) = 1$.

b. Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.

c. Prove that every automorphism of Z_n is equal to σ_a for some integer a.

d. Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism from $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ to $\mathrm{Aut}(Z_n)$.

Problem 1.11. Show that if G is a finite group of even order, then G contains an element $a \neq e$ such that $a^2 = e$.

Problem 1.12. List all subgroups of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Problem 1.13. Compute the automorphism groups of $\mathbb{Z}_6$, $\mathbb{Z}_{12}$ and $\mathbb{Z}_{27}$. Are any of them cyclic?

Problem 1.14. Let a, b, c be elements of a group G. Show that

$$|a| = |a^{-1}|, \qquad |ab| = |ba|, \qquad |cac^{-1}| = |a|.$$

Problem 1.15. a. If H and K are subgroups of a group G, then

$$[H \vee K : H] \geq [K : H \cap K].$$

b. Suppose $q < p$ are primes. Use the inequality of the first part to prove that a group of order pq has at most one subgroup of order p.

Problem 1.16. Let G be a group. Define a map $\Phi : G \to \mathrm{Aut}(G)$ by setting $\Phi(g) : G \to G$ to be the automorphism of G given by conjugation with g, i.e.

$$x \mapsto gxg^{-1}.$$

a. Prove that Φ is a homomorphism and that Φ is a monomorphism if and only if the center $Z(G)$ is trivial.

The image subgroup $\Phi(G)$ is denoted $\mathrm{Inn}(G)$ and called the **group of inner automorphisms.**

b. Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the **group of outer automorphisms.**

Problem 1.17. The goal of this set of exercises is to show that if $n > 6$ then

$$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \simeq S_n.$$

1. Prove that if $n > 2$, $\Phi : S_n \to \mathrm{Aut}(S_n)$ is a monomorphism.
2. Prove that for any group, if $f \in \mathrm{Aut}(G)$ and $\Psi \subset G$ is a conjugacy class in G, then $f(\Psi)$ is also a conjugacy class in G with necessarily the same number of elements.
3. Use the fact that if $n > 2$ and $n \neq 6$ then the conjugacy class of a transposition is the unique conjugacy class with $\binom{n}{2}$ elements of order two to conclude that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) = S_n$.

Problem 1.18. (a) Prove that if G is a subgroup of S_n and $A_n \cap G = \{e\}$ then $|G| = 2$. Give an example to show that this occurs.

(b) Use the first part to prove that if $n \geq 5$ then A_n is the unique normal subgroup of S_n.

Problem 1.19. (a) Show that a group of order 12 has a normal Sylow subgroup.

(b) Exhibit all 2-Sylow subgroups of the 12 element group D_6.

Problem 1.20. Prove that if a group contains a proper subgroup of finite index then it also contains a proper normal subgroup of finite index.

Problem 1.21. Let G be a group. A subgroup $P < G$ is *characteristic* if for every $\varphi \in \mathrm{Aut}(G)$, $\phi(P) = P$.

(a) Show that any characteristic subgroup is normal and give an example of a normal subgroup which is not characteristic.

(b) Prove that a p-Sylow subgroup is normal if and only if it is characteristic.

Problem 1.22. Prove that every group of order p^2 is abelian and prove that if G is non-abelian and $|G| = p^3$ then

$$Z(G) = [G, G]$$

where $[G, G]$ is the subgroup generated by the set of commutators

$$\{aba^{-1}b^{-1} \mid a, b \in G\}.$$

Problem 1.23. a. Prove that a finitely generated abelian group where 0 is the only element of finite order is necessarily free abelian.

b. Determine with proof how many subgroups of order p^2 does the abelian group $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ contain?

Problem 1.24. Let $g_1, \ldots, g_r$ be representatives of the conjugacy classes of a finite group G and assume that these elements pairwise commute. Prove that G is abelian.

Problem 1.25. (a) Prove that a group of order 105 has a normal 5-Sylow subgroup and a normal 7-Sylow group.

(b) Classify all groups of order 105 that have a normal 3-Sylow subgroup.

Problem 1.26. Let $G = GL_n(\mathbb{F}_q)$, the group of invertible $n \times n$ matrices over the finite field $\mathbb{F}_q$ with $q = p^r$, p a prime. Let $U = U_n(\mathbb{F}_q)$ be the subgroup of G of upper triangular matrices with 1's on the diagonal.

(a) Find $|G|$ and $|U|$. Conclude that U is a p-Sylow subgroup of G.

(b) Show that $g \in G$ has order a power of p if and only if $g = I_n + N$ with N an $n \times n$ matrix such that $N^n = 0$. [Hint: Use part (a).]

Problem 1.27. Determine up to isomorphism all abelian groups of order 64 and 96 respectively.

Problem 1.28. Show that if G is a group which contains an element x with $|x| > 2$ (possibly infinity) then G has a non-trivial automorphism.

Problem 1.29. Prove Theorem 1.3.2.

Problem 1.30. Prove that homomorphic image of a nilpotent groups is nilpotent.

Problem 1.31. (a) Prove that if G is a finite group and P is Sylow-p subgroup and M contains $\mathrm{N}_G(P)$ then $\mathrm{N}_G(M) = M$.

(b) If every maximal proper subgroup of a finite group is normal then G is nilpotent.

Problem 1.32. Prove Theorem 1.4.1.

Problem 1.33. Show that $G^{(k)} \lhd G$, for all $k \in \mathbb{N}$.

Problem 1.34. Prove or give a counter-example (Most, but not all, of these are false).

1. If every proper subgroup of a group G is abelian then G is abelian.
2. If K is a normal subgroup of G then any subgroup of K is normal in G.
3. If G is a group then any subgroup of the center $C(G)$ is normal in G.
4. If G is an infinite group then G has an element of infinite order.
5. A group with a finite number of subgroups must be finite.
6. If $x \in G$ and $y \in G$ have finite order then xy has finite order.
7. Any subgroup of a finitely generated group is finitely generated.

8. Every solvable group is finite.
9. The automorphism group of an abelian group is abelian.
10. If p, q are distinct primes then every nilpotent group of order pq is abelian.
11. The center of a group is a normal subgroup.
12. Give an example of a non-abelian nilpotent group.
13. Give an example of a solvable group which is not nilpotent.
14. If G is a group and $x, y \in G$ are elements of finite order that commute then $|xy| = \text{lcm}(|x|, |y|)$.
15. Let $H < G$ be a subgroup. If $\pi \subseteq G$ is a conjugacy class in G then $\pi \cap H$ is a conjugacy class in H.

Problem 1.35. Find the maximum order of an element of $\mathfrak{S}_7$.

Problem 1.36. Prove, just using the definition of group, that every group of order 4 is abelian.

Problem 1.37. List all abelian groups of order 180.

Problem 1.38. Prove that if $H < G$ is a subgroup such that $[G : H] = 2$ then H is normal in G.

Problem 1.39. Prove that if $G/\operatorname{C}(G)$ is cyclic then G is abelian.

Problem 1.40. If $|G| = p^n q$ with $p > q$ prime then G contains a unique normal subgroup of index q.

Problem 1.41. Prove that if $|G| = p^n q$ with $p > q$ prime, then G is solvable.

Problem 1.42. Prove that if G contains a subgroup H of finite index then it contains a normal subgroup of finite index.

Problem 1.43. Prove that if G is a finite abelian p-group then it is generated by its elements of maximum order.

Problem 1.44. How many elements of order 7 are there in a simple group of order 168?

Problem 1.45. How many subgroups isomorphic to $\mathbb{Z}_4$ does

$$G = \mathbb{Z}_8 \oplus \mathbb{Z}_{16}$$

have? (Hint: First count how many elements of order 4 there are in G.)

Problem 1.46. Prove that a group of order p^n contains normal subgroups of order p^k for $k = 0, \ldots, n$. (Hint: use induction and Corollary II5.4.)

Problem 1.47. Prove that if G is finite and 2 does not divide $|G|$ then there are no non-trivial homomorphisms

$$G \to \{\pm 1\}.$$

Problem 1.48. Prove that sgn is the only non-trivial homomorphism

$$S_n \to \{\pm 1\}.$$

Problem 1.49. Prove that if $\varphi : G \to H$ is a homomorphism with H abelian, then φ is constant on conjugacy classes.

Problem 1.50. Use the previous problem to prove that A_n is the unique subgroup of index 2 in $\mathfrak{S}_n$.

Problem 1.51. Let $H < G$ be a maximal proper subgroup which is normal. Prove that $[G : H]$ is prime. Do not assume that G is finite.

Problem 1.52. Prove that every automorphism of $\mathfrak{S}_3$ is inner.

Chapter 2

Ring Theory

2.1 Factorization in Commutative Rings

Definition 2.1.1. A nonzero element a of a commutative ring R is said to **divide** an element $b \in R$ (notation: $a \mid b$) if there exists $x \in R$ such that $ax = b$. Elements a, b of R are said to be **associates** if $a \mid b$ and $b \mid a$.

Virtually all statements about divisibility may be phrased in terms of principal ideals as we now see.

Theorem 2.1.1. Let a, b and u be elements of a commutative ring R with identity.

a. $a \mid b$ if and only if $(b) \subseteq (a)$.

b. a and b are associates if and only if $(a) = (b)$.

c. u is a unit if and only if $u \mid r$ for all $r \in R$.

d. u is a unit if and only if $(u) = R$.

e. The relation "a is an associate of b" is an equivalence relation on R.

f. If $a = br$ with $r \in R$ a unit, then a and b are associates. If R is an integral domain, the converse is true.

Proof. Problem ?? □

Definition 2.1.2. Let R be a commutative ring with identity. An element c of R is **irreducible** provided that:

i. c is a nonzero nonunit;

ii. $c = ab \implies a$ or b is a unit.

An element p of R is **prime** provided that:

i. p is a nonzero nonunit;

ii. $p \mid ab \implies p \mid a$ or $p \mid b$.

Example 2.1.1. a. If p is an ordinary prime integer, then both p and $-p$ are irreducible and prime in $\mathbb{Z}$.

b. In the ring $\mathbb{Z}_6$, the element 2 is easily seen to be a prime. However, $2 \in \mathbb{Z}_6$ is not irreducible since $2 = 2 \cdot 4$ and neither 2 nor 4 are units in $\mathbb{Z}_6$.

Theorem 2.1.2. Let p and c be nonzero elements in an integral domain R.

a. p is prime if and only if (p) is a nonzero prime ideal;

b. c is irreducible if and only if (c) is maximal in the set $\mathscr{S}$ of all proper principal ideals of R.

c. Every prime element of R is irreducible.

d. If R is a principal ideal domain, then p is prime if and only if p is irreducible.

e. Every associate of an irreducible [resp. prime] element is irreducible [resp. prime].

f. The only divisors of an irreducible element of R are its associates and the units of R.

Proof. Problem ?? □

We have now developed the analogues in an arbitrary integral domain of the concepts of divisibility and prime integers in the ring $\mathbb{Z}$. Recall that every element in $\mathbb{Z}$ is a product of a finite number of irreducible elements (prime integers or their negatives) according to the Fundamental Theorem of Arithmetic. Furthermore this factorization is essentially unique (except for the order of the irreducible factors). Consequently, $\mathbb{Z}$ is an example of:

2.2 Unique Factorization Domains and P.I.D.'s

Definition 2.2.1. An integral domain R is a **unique factorization domain** (U.F.D.) provided that:

a. every nonzero nonunit element a of R can be written $a = c_1 c_2 \cdots c_n$, with $c_1, \ldots, c_n$ irreducible;

b. if $a = c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_m$, where c_i, d_i are irreducible, then $n = m$ and for some permutation σ of $\{1, 2, \ldots, n\}$, c_i and $d_{\sigma(i)}$ are associates for every i.

Remark 2.2.1. Every irreducible element in a unique factorization domain is necessarily prime by (b). Consequently, irreducible and prime elements coincide by Theorem 2.1.2.

Lemma 2.2.1. If R is a principal ideal ring and

$$(a_1) \subseteq (a_2) \subseteq \cdots$$

is a chain of ideals in R, then for some positive integer n, $(a_j) = (a_n)$ for all $j \geq n$. In other words, every P.I.D. satisfies the **ascending chain condition**.

Proof. Let

$$A = \bigcup_{i \geq 1} (a_i).$$

Is left as an exercise to show that A is an ideal. By hypothesis A is principal, say $A = (a)$. Since $a \in A = \bigcup(a_i)$, $a \in (a_n)$ for some n. Hence, $(a) \subseteq (a_n)$. Therefore, for every $k \geq n$,

$$A = (a) \subseteq (a_n) \subseteq (a_j) \subseteq A,$$

whence $(a_k) = (a_n)$. □

Theorem 2.2.1. Every principal ideal domain R is a unique factorization domain.

Remark 2.2.2. The converse of Theorem 3.7 is false. For example the polynomial ring $\mathbb{Z}[x]$ can be shown to be a unique factorization domain, but $\mathbb{Z}[x]$ is not a principal ideal domain.

Proof. Let $\mathscr{S}$ be the set of all nonzero nonunit elements of R which cannot be factored as a finite product of irreducible elements. We shall first show that $\mathscr{S}$ is empty, whence every nonzero nonunit element of R has at least one factorization as a finite product of irreducible elements.

Suppose $\mathscr{S}$ is not empty and $a \in \mathscr{S}$. Then (a) is a proper ideal, hence is contained in a maximal ideal (c). The element c is irreducible by Theorem 2.1.1. Since $(a) \subseteq (c)$, c divides a, i.e. there is $x_a \in R$ such that $a = x_a c$. If x_a is a unit, then a is associating to an irreducible element, so it is irreducible, hence $a \notin \mathscr{S}$ and that is a contradiction. So $x_a \in \mathscr{A}$ and $(a) \subsetneq (x_a)$. Continuing the same process as before we can construct a strictly ascending chain of ideal, and this is a contradiction by Theorem 2.2.1. Finally if

$$c_1 c_2 \cdots c_n = a = d_1 d_2 \cdots d_m$$

with c_i, d_i irreducible, then c_1 divides some d_j, since in a P.I.D. every irreducible is prime. Since c_1 is a nonunit, it must be an associate of d_j. The proof of uniqueness is now completed by a routine inductive argument. □

2.3 Euclidean Domains

Definition 2.3.1. Let R be a commutative ring. R is a **Euclidean ring** if there is a function $\varphi : R \setminus \{0\} \to \mathbb{N}$ such that:

a. if $a, b \in R$ and $ab \neq 0$, then $\varphi(a) \leq \varphi(ab)$;

b. if $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$:

$$a = qb + r, \quad \text{with } r = 0, \text{ or } r \neq 0 \text{ and } \varphi(r) < \varphi(b).$$

A Euclidean ring which is an integral domain is called a **Euclidean domain**.

Example 2.3.1. a. The ring $\mathbb{Z}$ of integers with $\varphi(x) = |x|$ is a Euclidean domain.

b. If F is a field, let $\varphi(x) = 1$ for all $x \in F$, $x \neq 0$. Then F is a Euclidean domain.

c. If F is a field, then the ring of polynomials in one variable $F[x]$ is a Euclidean domain with $\varphi(f) = \deg f$.

d. Let $\mathbb{Z}[i]$ be the following subset of the complex numbers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

$\mathbb{Z}[i]$ is an integral domain called the domain of Gaussian integers. Define

$$\varphi(a + bi) = a^2 + b^2.$$

Clearly $\varphi(a+bi) \neq 0$ if $a+bi \neq 0$; it is also easy to show that condition (a) of the Definition is satisfied. The proof that φ satisfies condition (b) is left to the reader.

Theorem 2.3.1. Every Euclidean ring R is a principal ideal ring with identity. Consequently every Euclidean domain is a unique factorization domain.

Proof. If I is a nonzero ideal in R, choose $a \in I$ such that $\varphi(a)$ is the least integer in the set of nonnegative integers

$$\{\varphi(x) \mid x \neq 0,\ x \in I\}.$$

If $b \in I$, then $b = qa + r$ with $r = 0$ or $r \neq 0$ and $\varphi(r) < \varphi(a)$. Since $b \in I$ and $qa \in I$, r is necessarily in I. Since $\varphi(r) < \varphi(a)$ would contradict the choice of a, we must have $r = 0$, whence $b = qa$. Consequently, $I = (a)$ and, in particular, I is the principle. □

2.4 Greatest Common Divisors

Definition 2.4.1. Let X be a nonempty subset of a commutative ring R. An element $d \in R$ is a **greatest common divisor** (g.c.d.) of X provided:

a. $d \mid a$, for all $a \in X$;

b. $c \mid a$ for all $a \in X \implies c \mid d$.

Greatest common divisors do not always exist. For example, in the ring E of even integers 2 has no divisors at all, whence 2 and 4 have no greatest common divisor. Even when a greatest common divisor of $a_1, \ldots, a_n$ exists, it need not be unique. However, any two greatest common divisors of X are clearly associates by (b). Furthermore any associate of a greatest common divisor of X is easily seen to be a greatest common divisor of X. If R has an identity and $a_1, a_2, \ldots, a_n$ have 1_R as a greatest common divisor, then $a_1, a_2, \ldots, a_n$ are said to be relatively prime.

Theorem 2.4.1. Let $a_1, \ldots, a_n$ be elements of a commutative ring R with identity.

a. $d \in R$ is a greatest common divisor of $\{a_1, \ldots, a_n\}$ such that

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

for some $r_i \in R$ if and only if

$$(d) = (a_1) + (a_2) + \cdots + (a_n).$$

b. If R is a principal ideal ring, then a greatest common divisor of $a_1, \ldots, a_n$ exists and every one is of the form

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

with $r_i \in R$.

c. If R is a unique factorization domain, then there exists a greatest common divisor of $a_1, \ldots, a_n$.

Sketch of proof. Part (a) and (b) is left as an exercise. For (c), each a_i has a factorization

$$a_i = c_1^{m_{i1}} c_2^{m_{i2}} \cdots c_t^{m_{it}},$$

with $c_1, \ldots, c_t$ distinct irreducible elements and each $m_{ij} \geq 0$. Show that

$$d = c_1^{k_1} c_2^{k_2} \cdots c_t^{k_t}$$

is a greatest common divisor of $a_1, \ldots, a_n$, where

$$k_j = \min\{m_{1j}, m_{2j}, m_{3j}, \ldots, m_{nj}\}.$$

□

2.5 Localization

Definition 2.5.1. Let R be a ring and let $S \subseteq R$. We say that S is **multiplicative** if:

(a) $1_R \in S$, and

(b) for every $a, b \in S$, we have $a \cdot b \in S$.

Let R be a ring and let $S \subseteq R$ be multiplicative. On the set $R \times S$, we define a relation $\sim$ by

$$(r, s) \sim (r', s') \iff \exists u \in S : u(rs' - r's) = 0. \tag{2.1}$$

It is easily verified that the above relation is an equivalence relation, and the corresponding equivalence class of (r, s) will be denoted by $\frac{r}{s}$. The quotient set

$$S^{-1}R = (R \times S)/\sim$$

obtains a ring structure with operations:

- $(+)\colon \dfrac{r}{s} + \dfrac{r'}{s'} = \dfrac{rs' + r's}{ss'}$,
- $(\bullet)\colon \dfrac{r}{s} \bullet \dfrac{r'}{s'} = \dfrac{rr'}{ss'}$.

Remark 2.5.1. We have the ring homomorphism

$$R \to S^{-1}R, \quad r \mapsto \frac{r}{1},$$

which is called the **natural homomorphism**.

Example 2.5.1 (Field of Fractions)**.** One important example of localization arises in the case of R be an integral domain. If we consider the set $S = R \setminus \{0\}$ one can show that is multiplicative. The set $S^{-1}R$ is called the **field of fractions of** R and is denoted by $\mathrm{Frac}(R)$. Explicitly,

$$\mathrm{Frac}(R) = \left\{ \frac{a}{b} \mid a \in R, b \in R \setminus \{0\} \right\}.$$

Example 2.5.2 (Localization at a prime ideal)**.** Let R be a ring and let $\mathfrak{p}$ be a prime ideal of R. Then the set $S = R \setminus \mathfrak{p}$ is multiplicative, and we denote

$$S^{-1}R = R_{\mathfrak{p}} = \left\{ \frac{r}{s} \mid r \in R,\ s \in R \setminus \mathfrak{p} \right\}.$$

Example 2.5.3 (Localization over the powers of an element)**.** If R is a commutative ring and $r \in R$, we consider the set $S = \{1, r, r^2, r^3, \dots\}$. Then S is multiplicative and the corresponding localization $S^{-1}R$ is denoted by $R_{(r)}$. Explicitly,

$$R_{(r)} = \left\{ \frac{a}{r^n} \mid a \in R,\ n \in \mathbb{Z}_{\geq 0} \right\}.$$

Proposition 2.5.1. Let R be a ring and let $\mathfrak{p} \lhd R$ be a prime ideal of R. Then:

(a) The following equality holds :

$$U(R_{\mathfrak{p}}) = \left\{ \frac{r}{s} \in R_{\mathfrak{p}} \mid r \notin \mathfrak{p} \right\},$$

where $U(R_{\mathfrak{p}})$ denotes the invertible elements of $R_{\mathfrak{p}}$.

(b) The ring $R_{\mathfrak{p}}$ is local, with maximal ideal

$$\mathfrak{m} = \left\{ \frac{r}{s} \in R_{\mathfrak{p}} \mid r \in \mathfrak{p} \right\}.$$

Proof. (a) If $\frac{r}{s} \in U(R_{\mathfrak{p}})$, then there exist $r' \in R$ and $s' \notin \mathfrak{p}$ such that

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'} = 1.$$

Therefore, there exists $u \notin \mathfrak{p}$ such that

$$u(rr' - ss') = 0 \Rightarrow urr' = uss'.$$

If $r \in \mathfrak{p}$, then $uss' \in \mathfrak{p}$, which is impossible since $u, s, s' \notin \mathfrak{p}$. Conversely, if $r \notin \mathfrak{p}$, then $\frac{s}{r} \in R_{\mathfrak{p}}$, and hence

$$\frac{r}{s} \cdot \frac{s}{r} = 1.$$

(b) From part (a), it follows that the non-invertible elements of the ring $R_{\mathfrak{p}}$ form the set

$$\mathfrak{m} = \left\{ \frac{r}{s} \in R_{\mathfrak{p}} \mid r \in \mathfrak{p} \right\}.$$

It is easily verified that $\mathfrak{m}$ is an ideal of $R_{\mathfrak{p}}$ and a proper subset of $R_{\mathfrak{p}}$, which contains every maximal ideal of $R_{\mathfrak{p}}$.[1] Since we also know that $\mathfrak{m}$ is contained in a maximal ideal, the desired result follows.

□

[1] We know the existence of at least one maximal ideal of $R_{\mathfrak{p}}$, which is proved using Zorn's lemma.

Definition 2.5.2. Let $\varphi\colon R \to R'$ be a ring homomorphism, with $I \lhd R$ and $J \lhd R'$.

(a) The **contraction** of J through φ is the ideal of R

$$J^c = \varphi^{-1}(J) = \{r \in R \mid \varphi(r) \in J\}.$$

(b) The **extension** of I through φ is the ideal I^e of R' generated by the set $\varphi(I)$.

Theorem 2.5.1. Let S be a multiplicative subset of R. The following correspondences are inverse to each other, hence they are one-to-one and onto:

$$\{\mathfrak{p} \in \mathrm{Spec}R : \mathfrak{p} \cap S = \emptyset\} \underset{\mathfrak{q}^c \leftarrow \mathfrak{q}}{\overset{\mathfrak{p} \mapsto \mathfrak{p}^e}{\rightleftarrows}} \mathrm{Spec}\,(S^{-1}R)$$

via the natural homomorphism $R \to S^{-1}R, \quad r \mapsto \frac{r}{1}$.

where with Spec we denote the set of the prime ideals of a ring.

2.6 Problems

Problem 2.1. (a) Show that if R is a commutative ring then the set of nilpotent elements is an ideal. This ideal is called the nilradical.

(b) Given an example to show that this is false if R is not commutative.

(c) Show that if R is a commutative ring then the nilradical is the intersection of all prime ideals of R.

Problem 2.2. Let R be a commutative ring and let S be the ring of $n \times n$ matrices with entries in R.

a. Prove that $J \subset S$ is a two-sided ideal if and only if J is the set of $n \times n$ matrices with entries in an ideal I of R.

b. Show that if $n > 1$ and R is an integral domain then 0 is a prime ideal of S but there exists $a, b \neq 0$ such that $ab = 0$.

Problem 2.3. Let $f : R \to S$ be a homomorphism of (unital) rings.

a. Prove that if $f(1_R) = 0$ then $f = 0$.

b. Prove that if $f : R \to S$ is a non-zero homomorphism of commutative rings and S has no zero divisor then $f(1_R) = 1_S$.

c. Given an example of a non-zero homomorphism of commutative rings $f : R \to S$ such that $f(1_R) \neq 1_S$.

Problem 2.4. Let $f : R \to S$ be a homomorphism of commutative rings.

a. Prove that if $I \subseteq S$ is an ideal then $f^{-1}(I)$ is an ideal of R.

b. What hypothesis is required on f to ensure that $f(J)$ is an ideal of S for every ideal $J \subseteq R$?

c. Prove that if $\mathfrak{q} \subset R$ is prime then $f^{-1}(\mathfrak{q})$ is prime.

Problem 2.5. Prove that if R is a domain then there are no non-zero rings R_1, R_2 such that $R \simeq R_1 \times R_2$.

Problem 2.6. An element e in a ring R is idempotent if $e^2 = e$. Two idempotents e_1, e_2 are orthogonal if $e_1 e_2 = 0$.

a. Let R be the ring of 2×2 matrices with coefficients in $\mathbb{C}$. Describe all idempotents in R, and give an example of a pair of orthogonal idempotents.

b. Show that if $e_1, \ldots, e_n$ are central (i.e. they commute with all elements of R) orthogonal idempotents with $e_1 + \cdots + e_n = 1_R$ then $R \simeq R_1 \times \cdots \times R_n$ where $R_i = e_i R$.

c. Conversely if $R \simeq R_1 \times \cdots \times R_n$ then there are central orthogonal idempotents $e_1, \ldots, e_n$ such that $e_1 + \cdots + e_n = 1_R$ and $R_i = e_i R$.

d. Show if R is the ring of 2×2 matrices with coefficients in $\mathbb{C}$ then R is not isomorphic to a product $R_1 \times R_2$ with R_1, R_2 both non-zero.

Problem 2.7. a. Prove that the Gaussian integers $\mathbb{Z}[i]$ with $\varphi(a+bi) = a^2+b^2$ form a Euclidean domain.

b. Prove that a positive integer p is prime in $\mathbb{Z}[i]$ if and only if p is a prime integer and $p \equiv 3 \pmod 4$.

Problem 2.8. a. Show that if I is primary then $\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n > 0\}$ is prime. The ideal $\sqrt{I}$ is called the radical of I.

b. Show that if R is a PID then every primary ideal is of the form $I = (p^f)$ for some irreducible $p \in R$.

c. Show that in a PID every ideal I can be written as a product $I = P_1 \cdots P_r$ with P_i primary ideals such that $P_i + P_j = R$ for $i \neq j$.

Problem 2.9. Determine the complete ring of fractions of $\mathbb{Z}_n$ for $n \geq 2$.

Problem 2.10. Let R be an integral domain. If $\mathfrak{p}$ is a prime ideal then we can view the localization $R_\mathfrak{p}$ as a subring of the quotient field F. Likewise, we can view R as a subring of F. Prove that

$$\bigcap_{\mathfrak{m} \text{ maximal}} R_\mathfrak{m} = R$$

as subrings of F.

Problem 2.11. Give an example of a non-zero commutative ring with a unique prime ideal which is not a field.

Problem 2.12. A ring R is called semi-local if it has a finite number of maximal ideals.

a. Show that $R = \mathbb{Q}[x]/(x^3 - 1)$ is a semi-local ring and determine the maximal ideals.

b. Show that $R_\mathfrak{m}$ is a field for every maximal ideal $\mathfrak{m}$ of R.

Problem 2.13. a. Let F be a field. Show that if $f(x)$ is any non-zero polynomial then $R = F[x]/(f(x))$ is a semi-local ring.

b. What condition on $f(x)$ ensures that $R_\mathfrak{m}$ is a field for every maximal ideal $\mathfrak{m}$?

c. Show that if $R = F[x]/(f(x))$ has maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ then the natural map

$$R \to R_{\mathfrak{m}_1} \times \cdots \times R_{\mathfrak{m}_n}$$

is an isomorphism.

d. Show that if $R = \mathbb{C}[x]/(x^3 - 1)$ then there is a natural isomorphism

$$R \simeq \mathbb{C} \times \mathbb{C} \times \mathbb{C}$$

and determine the images of the elements $1, x, x^2$ respectively under this isomorphism.

Problem 2.14. Recall that a ring is Noetherian if every ideal is finitely generated. Show that a Noetherian local domain whose maximal ideal is principal is a PID.

Problem 2.15. Let $R = \mathbb{C}[x, y]/(y^2 - x^3)$.

a. Describe the maximal ideals of R.

b. Show that if $M = (\overline{x} - a, \overline{y} - b)$ is a maximal ideal of R with $(a, b) \neq (0, 0)$, then R_M is a PID by showing that the maximal ideal of R_M is principal. What is a generator for this maximal ideal?

c. Show that if $M = (\overline{x}, \overline{y})$ then the maximal ideal of R_M is not principal, so R_M is not a PID.

Problem 2.16. 1. If F is a field, then every nonzero element of $F[[x]]$ is of the form $x^k u$, with $u \in F[[x]]$ a unit.

2. $F[[x]]$ is a principal ideal domain whose only ideals are 0, $F[[x]] = (1_F) = (x^0)$, and (x^k) for each $k \geq 1$.

Problem 2.17. 1. If D is an integral domain and c is an irreducible element in D, then $D[x]$ is not a principal ideal domain. **Hint:** Consider the ideal (x, c) generated by x and c.

2. $\mathbb{Z}[x]$ is not a principal ideal domain.

3. If F is a field and $n \geq 2$, then $F[x_1, \ldots, x_n]$ is not a principal ideal domain. **Hint:** Show that x_1 is irreducible in $F[x_1, \ldots, x_{n-1}]$.

Problem 2.18. Let R be a commutative ring with identity and

$$f = \sum_{i=0}^{n} a_i x^i \in R[x].$$

Then f is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent elements of R.

Hint: If f is a unit, then is a unit on $R/\mathfrak{p}[x]$, for every prime ideal of R. What are units on $R/\mathfrak{p}[x]$? For the converse implication, note that if $a_1, \ldots, a_n$ nilpotent, then $h(x) = a_1 x + \cdots + a_n x^n$ so is.

Problem 2.19. If

$$f = \sum a_i x^i \in \mathbb{Z}[x]$$

and p is prime, let

$$\overline{f} = \sum \overline{a_i} x^i \in \mathbb{Z}_p[x],$$

where $\overline{a_i}$ is the image of a_i under the canonical epimorphism $\mathbb{Z} \to \mathbb{Z}_p$.

a. If f is monic and $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$ for some prime p, then f is irreducible in $\mathbb{Z}[x]$.

b. Give an example to show that (a) may be false if f is not monic.

c. Extend (a) to polynomials over a unique factorization domain.

Problem 2.20. a. Let D be an integral domain and $c \in D$. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$ and

$$f(x-c) = \sum_{i=0}^{n} a_i (x-c)^i \in D[x].$$

Then $f(x)$ is irreducible in $D[x]$ if and only if $f(x-c)$ is irreducible.

b. For each prime p, the cyclotomic polynomial $f = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Z}[x]$.

Problem 2.21. Let R be a commutative ring with identity and $c, b \in R$, with c a unit.

1. Show that the assignment
$$x \mapsto cx + b$$
induces a unique automorphism of $R[x]$ that is the identity of R. What is its inverse?

2. If D is an integral domain, then show that every automorphism of $D[x]$ that is the identity on D is of the type described in (a).

Problem 2.22. Prove or give a counter–example.

i. If R is a domain and (f) is prime, then f is irreducible.

ii. If R is a domain and $f \in R$ is irreducible, then f is prime.

iii. If R and S are domains, then $R \times S$ is a domain.

iv. Every maximal ideal is prime.

v. Every prime ideal is maximal.

vi. Let $f : R \to S$ be a ring homomorphism. If P is a prime ideal in R, then $f(P)$ is a prime ideal in S.

vii. Let $f : R \to S$ be a ring homomorphism. If Q is a prime ideal in S, then $f^{-1}(Q)$ is a prime ideal in R.

viii. Let $f \in \mathbb{Z}[x]$ be a primitive polynomial. If prime is prime, let f_p be the image of f under the map $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Then f is irreducible if and only if f_p is irreducible in $\mathbb{Z}_p[x]$ for some prime p.

ix. Every Euclidean domain is a Principal Ideal Domain.

x. Every Unique Factorization Domain is a Principal Ideal Domain.

xi. If $S \subset R$ is a multiplicatively closed subset, then the natural map

$$R \to S^{-1}R$$

is injective.

xii. The set of nilpotent elements in a ring forms an ideal.

xiii. The set of zero-divisors in a ring forms an ideal.

Chapter 3

Galois Theory

3.1 Algebraically Closed/Closures and Separability

Definition 3.1.1. Let K be a field and let $f \in K[x]$ be a non-constant polynomial. An extension $K \subseteq F$ is called a **splitting field** of f if

i. f splits into linear factors in $F[x]$, i.e.

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_m)$$

ii. $F = K(\alpha_1, \ldots, \alpha_m)$.

Theorem 3.1.1. Let K be a field and $f(x) \in K[x]$ with $\deg f = m \geq 1$. Then there exists a splitting field F of f over K such that $[F : K] \leq m!$.

Corollary 3.1.1. Let $f \in K[x]$ and let F, F' be two splitting fields of f over K. Then there exists a field isomorphism $\sigma : F \to F'$ such that $\sigma(c) = c$ for all $c \in K$.

Example 3.1.1. There are cases where two splitting fields are isomorphic but not equal. Let

$$f(x) = x^2 - 2 \in \mathbb{Q}[x].$$

Then $L_1 = \mathbb{Q}\left(\sqrt{2}\right)$ is a splitting field of f. Also consider $L_2 = \mathbb{Q}[x]/(x^2 - 2)$. If $\alpha = \overline{x} \in \mathbb{Q}[x]/\langle x^2 - 2\rangle$ then $f(\alpha) = 0$, so $\mathbb{Q}(\alpha)$ is also a splitting field of f and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Hence

$$L_1 \xrightarrow{\cong} L_2, \quad \sqrt{2} \mapsto \alpha,$$

but $L_1 \neq L_2$.

Corollary 3.1.2. By induction, if S is a set of polynomials in $K[x]$, then there exists a splitting field for S, unique up to isomorphism.

Theorem 3.1.2. The following are equivalent : F is a field :

a. Every non-constant polynomial f in $F[x]$, has a root in F.

b. Every non constant polynomial splits into linear factors.

c. Every irreducible polynomial in $F[x]$ is linear.

d. F has no non-trivial algebraic extensions.

e. There exists $K \subseteq F$ such that F is algebraic over K and every $f(x) \in K[x]$ splits in F.

Definition 3.1.2. F is **algebraically closed** if it satisfies any of the previous theorem's condition.

Theorem 3.1.3. Let K be a field and $K \subseteq F$. The following are equivalent:

a. F is algebraically closed.

b. F is a splitting field of all irreducible polynomials in $K[x]$.

Given a field K, a field F satisfying the equivalences of Theorem 3.1.3, then D is called an **algebraic closure** of F.

Theorem 3.1.4. Every field K has an algebraic closure. Also, any two algebraic closures of K are isomorphic. If K is a field, we will sometimes write $\overline{K}$ for the algebraic closure.

Example 3.1.2. By the Fundamental theorem of Algebra we get $\overline{\mathbb{R}} = \mathbb{C}$, and

$$\mathbb{C} \supset \mathbb{R} \qquad \text{and} \qquad [\overline{\mathbb{R}} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2.$$

In general,

$$[L : K] = \infty \quad \text{for algebraic closures.}$$

For example $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Definition 3.1.3. A polynomial $f \in K[x]$ is **separable** if it factors into distinct linear factors in a splitting field. In particular, if f is irreducible then

$$f \text{ is separable} \iff (f, f') = 1.$$

In particular, if f is irreducible, then f is separable $\iff f \neq 0$.

Definition 3.1.4. An algebraic extension $K \subseteq F$ is called **separable** if for any $\alpha \in F$, the polynomial $\text{Irr}(\alpha, K)$ is separable.

3.2 Primitive Element Theorem

Theorem 3.2.1 (Primitive Element Theorem)**.** If $K \subseteq F$ is a finite (hence algebraic) separable extension with $|K| = \infty$, then $F = K(\alpha)$, for some $\alpha \in F$, i.e. F has a primitive element.

Proof. By hypothesis $F = K(\alpha_1, \ldots, \alpha_t)$. By induction on the generators we may assume that

$$K(\alpha_1, \ldots, \alpha_{t-1}) = K(\beta)$$

for some primitive element β. Thus it suffices to show that $K(\alpha, \beta)$ has a primitive element. We will show that for all but finitely many $c \in K$, the element $\gamma = \alpha + c\beta$ is a primitive element, i.e.

$$K(\gamma) = K(\alpha, \beta)$$

If we show that $\alpha \in K(\gamma)$, then obviously $\beta = \gamma - \alpha/c \in K(\gamma)$. Since $K \subseteq K(\alpha, \beta)$ separable, then $K(\gamma) \subseteq K(\alpha, \beta)$ is separable, thus

$$f(x) = \text{Irr}(\alpha, K(\gamma)) \quad \text{and} \quad g(x) = \text{Irr}(\beta, K(\gamma))$$

are separable. Now, let $L \supseteq K(\beta)$ be a field such that f and g split into linear factors. Let

$$f(x) = (x - \alpha) \cdots (x - \alpha_n), \qquad g(x) = (x - \beta) \cdots (x - \beta_m).$$

where $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ are distinct. Now since

$$\gamma = \alpha + c\beta \Rightarrow \beta = \frac{\gamma - \alpha}{c}$$

if we set

$$h(x) = g\left(\frac{\gamma - x}{c}\right) \in K(\gamma)[x]$$

then $h(\alpha) = g(\beta) = 0$. Hence α is a common root of f and h. The other roots of h are $\gamma - c\beta_j$. If

$$x - \alpha \mid \gcd(f, h)$$

then α is a root of $\gcd(f, h)$. To compute $\gcd(f, h)$ in $L[x]$ write

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \quad \text{and} \quad h(x) = (x - \alpha)(x - \gamma + c\beta_j).$$

We need to show

$$\{\alpha_2, \ldots, \alpha_n\} \cap \{\gamma - \beta_2, \ldots, \gamma - \beta_m\} = \varnothing.$$

If these sets overlap then

$$\alpha_i = \alpha + c\beta - \beta_j$$

for some i, j. Hence if we choose

$$c \neq \frac{\alpha_j - \alpha_i}{\beta_i - \beta}.$$

which is possible since $|K| = \infty$, then Thus

$$c \notin \left\{ \frac{\alpha_j - \alpha_i}{\beta_i - \beta} \;\middle|\; i = 1, \ldots, n,\ j = 1, \ldots, m \right\}.$$

Therefore $\gcd(f, h) = x - \alpha$. Hence $\alpha \in K(\gamma)$. □

3.3 Galois Extensions

Definition 3.3.1 (Galois group)**.** Let $F \supseteq K$ be a field extension. The following group :

$$\mathrm{Aut}_K(F) = \{\sigma : F \xrightarrow{\cong} F \mid \sigma|_K = \mathrm{id}\}$$

is the **Galois group** of F over K, denoted $\mathrm{Gal}_K(F)$.

Theorem 3.3.1. Let $F \supseteq K$.

a. If $H \leq \mathrm{Aut}_K(F)$, then

$$F^H = \{\alpha \in F \mid \sigma(\alpha) = \alpha, \quad \text{for all } \sigma \in H\}$$

is a subfield of F containing K.

b. If $F \supseteq E \supseteq K$, then

$$H_E = \mathrm{Aut}_E F = \{\sigma \in \mathrm{Aut}_K(F) \mid \sigma|_E = \mathrm{id}\}$$

is a subgroup.

We obtain the correspondence

$$\begin{array}{ccc} F & \xleftarrow[F^{(-)}]{} & \{\mathrm{id}\} \\ \downarrow & & \downarrow \\ F^H & \xleftarrow[F^{(-)}]{} & H \\ \downarrow & & \downarrow \\ K & \xleftarrow[F^{(-)}]{} & \mathrm{Aut}_K F \end{array} \qquad \begin{array}{ccc} K & \xrightarrow{\mathrm{Aut}_{(-)}F} & \mathrm{Aut}_K F \\ \downarrow & & \uparrow \\ E & \xrightarrow{\mathrm{Aut}_{(-)}F} & \mathrm{Aut}_E F \\ \downarrow & & \uparrow \\ F & \xrightarrow{\mathrm{Aut}_{(-)}F} & \mathrm{Aut}_F F = \{\mathrm{id}\} \end{array}$$

Definition 3.3.2. An extension $K \subseteq F$ is **Galois** if $F^{\mathrm{Aut}_K(F)} = K$.

Example 3.3.1. We consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. Then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}\}$. Hence it is not Galois, since $F^{\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Q}\left(\sqrt[3]{2}\right) \neq \mathbb{Q}$. [1]

The **goal** is to prove the following theorem.

Theorem 3.3.2. Let $K \subseteq F$ be a finite extension. The following are equivalent :

[1] The equity

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}\}$$

comes from the fact that a field automorphism sends a root to its conjugates and the conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, where $\omega \in \mathbb{C} \setminus \mathbb{R}$.

a. $F^{\text{Aut}_K(F)} = K$ (i.e. $K \subseteq F$ is Galois)

b. F is a splitting field of a separable polynomial in $K[x]$

c. $[F : K] = |\text{Aut}_K(F)|$

Theorem 3.3.3. If $\sigma : K \to L$ is an isomorphism of fields and $f(x) \in K[x]$, then $\sigma(f) \in L[x]$. Let F be a splitting field of f, and M a splitting field of $\sigma(f)$. Then the number of isomorphisms

$$\tau : F \to M \quad \text{s.t. } \tau|_K = \sigma$$

is at most $[F : K] = [M : L]$. Equality holds if and only if f is separable.

Proof. Use induction on $[F : K] = [M : L]$.

- If $[F : K] = 1$, the statement is trivial.
- Given $\tau : F \to M$ an isomorphism which extends σ. For any $\alpha \in F$, let $\beta = \tau(\alpha) \in M$. Then τ restricts to an isomorphism $\sigma' : K(\alpha) \to L(\beta)$.

$$\begin{array}{ccc} F & \xrightarrow{\tau} & M \\ \cup & & \cup \\ K(\alpha) & \xrightarrow{\sigma'} & L(\beta) \\ \cup & & \cup \\ K & \xrightarrow{\sigma} & L \end{array}$$

  On the other hand, given any $\alpha \in F$, $\beta \in M$ and an isomorphism $\sigma' : K(\alpha) \to L(\beta)$, then we know that F and M are splitting fields over $K(\alpha)$ and $L(\beta)$ respectively. Hence σ' extends to an isomorphism $\tau : F \to M$ (i.e. $\tau|_{K(\alpha)} = \sigma'$).

The conclusion is that giving an isomorphism $\tau : F \to M$ extending σ is equivalent to giving an isomorphism $\sigma' : K(\alpha) \to L(\beta)$ extending σ and an isomorphism $F \to M$ extending σ'. Assuming $\alpha \notin K$ (which can be true since $[F : K] > 1$), we know $[F : K(\alpha)] < [F : K]$. Since F is a splitting field over $K(\alpha)$, by induction there are at most $[F : K(\alpha)]$ isomorphisms

$$\tau : F \to M$$

extending σ'. □

Theorem 3.3.4. Let F be a splitting field of $f(x) \in K[x]$. Then $|\text{Aut}_K(F)| \leq [F : K]$ with equality if and only if the extension is separable.

In order to prove this we prove the following.

Theorem 3.3.5. Let F be a splitting field over K of $f(x) \in K[x]$ and $\sigma : K \to L$ be an isomorphism. Let M be a splitting field of $\sigma(f)$ over L. Then

$$\#\{\tau : F \to M \text{ extending } \sigma\} \leq [F : K].$$

Proof. Use induction on $[F : K]$.

- If $[F : K] = 1$, the statement is trivial.
- Given $\tau : F \to M$ an isomorphism which extends σ. For any $\alpha \in F$, let $\beta = \tau(\alpha) \in M$. We restrict τ to obtain an isomorphism $\sigma' : K(\alpha) \to L(\beta)$.

$$\begin{array}{ccc} F & \xrightarrow{\tau} & M \\ \cup & & \cup \\ K(\alpha) & \xrightarrow{\sigma'} & L(\beta) \\ \cup & & \cup \\ K & \xrightarrow{\sigma} & L \end{array}$$

On the other hand any $\alpha \in F$, $\beta \in M$ and an isomorphism $\sigma' : K(\alpha) \to L(\beta)$, then we know that F and M are splitting fields over $K(\alpha)$ and $L(\beta)$ respectively. Hence, there exists an isomorphism $\tau : F \to M$ which extends σ'.

The conclusion is that giving an isomorphism $\tau : F \to M$ that extends σ is equivalent to giving an isomorphism $\sigma' : K(\alpha) \to L(\beta)$ that extends σ. Let $\tau : F \to M$ be an isomorphism extending σ and let $\alpha \in F \setminus K$ be a root of $f(x)$. We know $[F : K(\alpha)] < [F : K]$ and F is a splitting field over $K(\alpha)$. By induction,

$$\#\{\tau : F \to M \text{ extending } \sigma'\} \leq [F : K(\alpha)].$$

Since $\sigma'(\alpha) = \beta$ and α is a root of f, we have that β is a root of $\sigma(f)$. Hence there are at most

$$\deg(\sigma(f)) \leq [K(\alpha) : K]$$

possible choices. Therefore

$$\#\{\tau : F \to M \text{ extending } \sigma\} \leq [F : K(\alpha)]\,[K(\alpha) : K] = [F : K].$$

Equality holds $\Leftrightarrow \sigma(f)$ is separable. □

Theorem 3.3.6 (Characterization of Galois extensions)**.** Let F/K be a finite extension. The following are equivalent:

i. $F^{\mathrm{Aut}_K(F)} = K$

ii. F is a splitting field of a separable polynomial.

iii. $|\operatorname{Aut}_K(F)| = [F : K]$

Proof. (ii) $\rightarrow$ (iii) follows from the previous theorem.

(i) $\Rightarrow$ (ii) Let $\alpha \in F \setminus K$ and let $f(x) = \operatorname{Irr}(\alpha|K)$. Let $a_1, \ldots, a_r$ be the distinct roots of $f(x)$ **in** F and define

$$g(x) = (x - a_1) \cdots (x - a_r) \in F[x].$$

Show $g \in K[x]$. If $\sigma \in \operatorname{Aut}_K(F)$ then $\sigma(a_i) \in \{a_1, \ldots, a_r\}$. Since σ is an automorphism, $\sigma(g) = g$. Hence, by part (i) :

$$g \in F^{\operatorname{Aut}_K(F)}[x] = K[x].$$

Since $g(\alpha) = 0$ we have $f \mid g$. But $a_1, \ldots, a_r$ are roots of f, so $g \mid f$. Therefore $f(x) = g(x)$. Thus f is separable and F is a splitting field of f.

(iii) $\rightarrow$ (i) Let $K \subseteq E$, where $E = F^{\operatorname{Aut}_K(F)}$. We claim that

$$\operatorname{Aut}_E(F) = \operatorname{Aut}_K(F)$$

and F/E satisfies (1),(2),(3). Hence $|\operatorname{Aut}_E(F)| = [F : E]$ and $|\operatorname{Aut}_K(F)| = [F : K]$. Thus $[F : E] = [F : K]$ so $[E : K] = 1$ and therefore $E = K$. □

3.4 Towards to the Fundamental Theorem

Theorem 3.4.1 (Fundamental Theorem of Galois Theory)**.** Let $K \subseteq F$ be a Galois extension and $G = \operatorname{Aut}_K(F)$. Then there is a 1-1 inclusion reversing correspondence

$$\{\text{Intermediate extensions}\} \longleftrightarrow \{\text{subgroups of } G\}.$$

$$\begin{array}{ccc|c|ccc} F & \longleftrightarrow & \{1\} & & G & \longleftrightarrow & K \\ \cup & & \cup & & \cap & & \cap \\ E & \longleftrightarrow & \operatorname{Aut}_E(F) & & H & \longleftrightarrow & F^H \\ \cup & & \cup & & \cap & & \cap \\ K & \longleftrightarrow & G & & \{1\} & \longleftrightarrow & F \end{array}$$

a. Also $E \mapsto \operatorname{Aut}_E(F)$ and $H \mapsto F^H$ satisfy $F^{\operatorname{Aut}_E(F)} = E$ and $\operatorname{Aut}_{F^H}(F) = H$.

b. Moreover, the extension $K \subseteq E$ is Galois if and only if $\operatorname{Aut}_E F$ is a normal subgroup of G. Conversely, if $H \triangleleft G$ then $K \subseteq F^H$ is Galois and $\operatorname{Aut}_K(F^H) \cong G/H$.

Sketch of the proof

i. $K \subset E \Rightarrow F^{\operatorname{Aut}_E(F)} = E$.

ii. $H \leq G \Rightarrow \operatorname{Aut}_{F^H}(F) = H$.

Theorem 3.4.2 (Artin's Lemma)**.** Let F be a field and $G \leq \text{Aut}(F)$ be a finite subgroup. If

$$K = F^G = \{c \in F \mid \sigma(c) = c,\ \forall \sigma \in G\}$$

then

$$[F : K] \leq |G| < \infty.$$

3.5 Problems

Problem 3.1. Let $F > K$ be a field extension. Prove that $\alpha \in F$ is algebraic if and only if $K[\alpha] = K(\alpha)$, i.e. $K[\alpha]$ is a field.

Problem 3.2. Prove that if K is a field and α and β are roots of an irreducible polynomial $f \in K[x]$, then there is an isomorphism $K(\alpha) \to K(\beta)$ which restricts to the identity on K.

Problem 3.3. Prove that if K has characteristic 0, then any irreducible polynomial $f \in K[x]$ is separable.

Problem 3.4. If $\alpha \in F$ is algebraic over K of odd degree, then $K(\alpha) = K\left(\alpha^2\right)$.

Problem 3.5. If α, β are algebraic over K of degrees m, n respectively, then

$$[K(\alpha, \beta) : K] \leq mn,$$

with equality if $(m, n) = 1$.

Problem 3.6. What is the degree of the extension $\mathbb{Q}\left(i, e^{2\pi i/3}\right)$ over $\mathbb{Q}$? Find a primitive element for this extension. Find the Galois group of the extension. Is it Galois?

Problem 3.7. If $x^n - a \in K[x]$ is irreducible and $u \in F$ is a root of $x^n - a$, and if m divides n, then prove that the degree of u^m over K is $\frac{n}{m}$. What is the irreducible polynomial for u^m over K?

Problem 3.8. If F is a splitting field of S over K and E is an intermediate field, then F is a splitting field of S over E.

Problem 3.9. No finite field K is algebraically closed.

Hint: If $K = \{a_0, \ldots, a_n\}$, consider

$$a_1 + (x - a_0)(x - a_1) \cdots (x - a_n) \in K[x],$$

where $a_1 \neq 0$.

Problem 3.10. What is the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$?

Problem 3.11. Assume $\text{char}(K) = 0$ and let G be the subgroup of $\text{Aut}_K(K(x))$ generated by the automorphism induced by $x \mapsto x + 1_K$. Then G is an infinite cyclic group. Determine the fixed field E of G. What is $[K(x) : E]$?

Problem 3.12. In the extension of $\mathbb{Q}$ by $\mathbb{Q}(x)$, the intermediate field $\mathbb{Q}(x^2)$ is closed, but $\mathbb{Q}(x^3)$ is not.

Problem 3.13. If $K \subseteq F$ is a field extension such that $[F : K] = 2$, then F is normal over K.

Problem 3.14. If F is normal over an intermediate field E and E is normal over K, then F need not be normal over K.

Problem 3.15. Suppose that K is a subfield of $\mathbb{R}$ (so that we may view K as a subfield of $\mathbb{C}$), and that $f \in K[x]$ is irreducible of degree 3. Let D be the discriminant of f. Then:

a. $D > 0$ if and only if f has three real roots.

b. $D < 0$ if and only if f has precisely one real root.

Problem 3.16. Determine the Galois groups of the following polynomials over the indicated fields:

a. $x^4 - 5$ over $\mathbb{Q}$, $\mathbb{Q}\big(\sqrt{5}\big)$, and $\mathbb{Q}\big(\sqrt{5}\,i\big)$

b. $x^3 - x - 1$ over $\mathbb{Q}$ and $\mathbb{Q}\big(\sqrt{23}\,i\big)$

Problem 3.17. Let K be a subfield of the real numbers and let $f \in K[x]$ be an irreducible quartic. If f has exactly two real roots, then the Galois group of f is S_4 or D_4.

Problem 3.18. Give an example of a field extension $K \subset F$ such that $u, v \in F$ are transcendental over K, but $K(u, v) \ncong K(x_1, x_2)$.

Problem 3.19. Let L and M be intermediate fields in the extension $K \subset F$.

a. $[LM : K]$ is finite if and only if $[L : K]$ and $[M : K]$ are finite.

b. If $[LM : K]$ is finite, then $[L : K]$ and $[M : K]$ divide $[LM : K]$ and
$$[LM : K] \leq [L : K][M : K].$$

c. If $[L : K]$ and $[M : K]$ are finite and relatively prime, then
$$[LM : K] = [L : K][M : K].$$

d. If L and M are algebraic over K, then so is LM.

Problem 3.20. Let $f \in K[x]$ be a separable polynomial of degree n and let F be its splitting field over K. Show that
$$[F : K] \mid n!.$$

Problem 3.21. If $|K| = p^n$, then every element of K has a unique p-th root in K.

Problem 3.22. If $|K| = q$ and $(n, q) = 1$ and F is a splitting field of $x^n - 1_K$ over K, then $[F : K]$ is the least positive integer k such that $n \mid (q^k - 1)$.

Problem 3.23. If $n \geq 3$, then $x^{2^n} + x + 1$ is reducible over $\mathbb{Z}_2$.

Problem 3.24. If $f \in K[x]$ is monic irreducible, $\deg f \geq 2$, and f has all its roots equal (in a splitting field), then $\text{char}(K) = p \neq 0$ and $f(x) = x^{p^n} - a$, for some $n \geq 1$ and $a \in K$.

Problem 3.25. Let $\text{char}(K) = p \neq 0$ and assume
$$F = K(u, v)$$
where $u^p \in K$, $v^p \in K$ and $[F : K] = p^2$. Then F is not a simple extension of K. Exhibit an infinite number of intermediate fields.

Problem 3.26. Construct a field with 9 elements and give its addition and multiplication table.

Problem 3.27. Prove that every element of a finite field may be written as the sum of two squares.

Problem 3.28. Prove or give a counter–example.

a. If $F \supset K$ is Galois and E is an intermediate field, i.e. $F \supset E \supset K$, then $E \supset K$ is Galois.

b. If $F \supset K$ is Galois and E is an intermediate field, i.e. $F \supset E \supset K$, then $F \supset E$ is Galois.

c. Any finite extension of fields $F \supset K$ is algebraic.

d. If $F \supset K$ is a finite extension of fields, then F has a primitive element.

e. If $[F : K] > 1$, then $|\,\text{Aut}_K(F)| > 1$.

Chapter 4

Modules

4.1 Direct Sum and Direct Limits

Theorem 4.1.1 (Universal property of the external direct sum)**.** Let $\{A_i\}_{i\in I}$ be a family of submodules of A. The natural map

$$\Phi : \bigoplus_{i\in I} A_i \longrightarrow \sum_{i\in I} A_i$$

is an isomorphism if and only if

$$A_i \cap \sum_{j\neq i} A_j = 0 \qquad \text{for all } i \in I.$$

Corollary 4.1.1. Let $A_1, A_2 \leq A$. If $A_1 \cap A_2 = 0$, then $A_1 + A_2 \cong A_1 \oplus A_2$.

4.2 Exact sequences

Definition 4.2.1. Let

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

be morphisms of R-modules. The sequence is **exact at** B if $\text{im } f = \ker g$. A sequence of R-modules

$$\cdots \longrightarrow A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \longrightarrow \cdots$$

is **exact** if $\text{im } f_i = \ker f_{i+1}$, for all $i \in \mathbb{Z}$.

Example 4.2.1. a. The sequence $0 \longrightarrow B \xrightarrow{g} C$ is exact if and only if g is injective.

b. The sequence $A \xrightarrow{f} B \longrightarrow 0$ is exact if and only if f is surjective.

Definition 4.2.2. A **short exact sequence** is a sequence

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

such that f is injective, g is surjective, and $\ker g = \operatorname{im} f$. If $A \leq B$ is a submodule, we obtain the short exact sequence

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{\pi} B/A \longrightarrow 0.$$

Proposition 4.2.1. Let $f : A \to B$ be a homomorphism of R-modules. Then f factors as

$$A \xrightarrow{\pi} A/\ker f \xrightarrow{\overline{f}} B \xrightarrow{\rho} B/\operatorname{im} f,$$

and the sequence

$$0 \longrightarrow A/\ker f \xrightarrow{\overline{f}} B \xrightarrow{\rho} B/\operatorname{im} f \longrightarrow 0$$

is exact.

Definition 4.2.3. Let

$$\cdots \to A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \to \cdots$$

and

$$\cdots \to B_{i-1} \xrightarrow{g_i} B_i \xrightarrow{g_{i+1}} B_{i+1} \to \cdots$$

be exact sequences. A **map of exact sequences** is a family of homomorphisms $\varphi_\bullet = (\varphi_i : A_i \to B_i)_{i\in\mathbb{Z}}$ such that $\varphi_i \circ f_i = g_i \circ \varphi_{i-1}$, for all $i \in \mathbb{Z}$, i.e. each such square commutes

$$\begin{array}{ccc} A_i & \xrightarrow{f_i} & A_{i+1} \\ \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi_{i+1}} \\ B_i & \xrightarrow{g_i} & B_{i+1} \end{array}$$

Lemma 4.2.1 (Five lemma)**.** Consider a morphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

Then:

1. If α and γ are monomorphisms, then β is a monomorphism.
2. If α and γ are epimorphisms, then β is an epimorphism.
3. If α and γ are isomorphisms, then β is an isomorphism.

Proof. Proof by diagram chasing. □

Example 4.2.2. Consider the following (non commutative !) diagram :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 2} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{i_1} & \mathbb{Z} \oplus \mathbb{Z}_2 & \xrightarrow{\pi_2} & \mathbb{Z}_2 & \longrightarrow & 0 \end{array}$$

Even if id is an isomorphism, the Theorem 4.2.1 does not apply since, i.e. π is not an isomorphism, because the diagram does not commute.

4.3 Split Exact Sequences

Definition 4.3.1. Let A_1, A_2 be R-modules. The sequence

$$0 \longrightarrow A_1 \xrightarrow{i_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \longrightarrow 0$$

is called a **split exact sequence**.

Theorem 4.3.1. Let R be a ring and a short exact sequence of R - modules :

$$0 \longrightarrow A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \longrightarrow 0$$

The following are equivalent:

i. There exists $h : A_2 \to B$ such that $g \circ h = \mathrm{id}_{A_2}$.

ii. There exists $k : B \to A_1$ such that $k \circ f = \mathrm{id}_{A_1}$.

iii. There is an isomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{i_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \end{array}$$

where α, β, γ are isomorphisms.

Proof. Prove first (i) $\to$ (ii) and (ii) $\to$ (iii). For those implications, use the universal property of direct sum/product and the five lemma. The inverse implications follow immediately from the commutativity of the given diagram. □

Definition 4.3.2. A short exact sequence

$$0 \longrightarrow A_1 \longrightarrow B \longrightarrow A_2 \longrightarrow 0$$

is called **split exact** if any (equivalently all) of the conditions in Theorem 4.3.1 hold.

Example 4.3.1. Let k be a field and $V_1 \xrightarrow{f} V_2$ an injective linear map of k-vector spaces. Then

$$0 \longrightarrow V_1 \xrightarrow{f} V \longrightarrow V/\operatorname{im} f \longrightarrow 0$$

is a split exact sequence.

Proposition 4.3.1. If k is a division ring, every short exact sequence of k-vector spaces splits.

Group algebras

Let G be a finite group and k a field with $\operatorname{char}(k) \nmid |G|$. The **group algebra**

$$k[G] = \left\{ \sum_{i=1}^{n} a_i[g_i] \mid a_i \in k,\ g_i \in G \right\}$$

is a k-algebra. Addition is defined coefficientwise and multiplication by

$$[g_i][g_j] = [g_i g_j].$$

The algebra $k[G]$ is commutative if and only if G is abelian. If $H \leq G$ then

$$k[H] \subseteq k[G]$$

is a subalgebra. Modules over $k[G]$ correspond to representations of G over k.

Theorem 4.3.2 (Maschke)**.** Let G be a finite group and k a field such that $\operatorname{char}(k) \nmid |G|$. Then every short exact sequence of $k[G]$-modules splits.

4.4 Free Modules

Definition 4.4.1. Let A be an R-module. A subset $X \subseteq A$ is **linearly independent** if

$$\sum_{i=1}^{n} r_i x_i = 0 \quad \Rightarrow \quad r_i = 0 \text{ for all } i,$$

for distinct $x_1, \ldots, x_n \in X$.

Example 4.4.1. $k[x]$ is a k-vector space and $\{x^i \mid i \in \mathbb{N}\}$ is linearly independent.

Definition 4.4.2. Let A be an R-module. A set $X \subseteq A$ is a **basis** if X is linearly independent and $A = \langle X \rangle$.

Remark 4.4.1. Every element of A has a unique expression $\sum_{i=1}^{n} r_i x_i$, $r_i \in R$ and $x_i \in X$.

Example 4.4.2. If G is a finite group $G = \{g_1, \ldots, g_n\}$, then $K[G]$ is a K-vector space with basis $\{[g] : g \in G\}$.

Theorem 4.4.1. Let R be a ring and F an R-module. The following are equivalent:

i. F has a nonempty basis.

ii. F is an internal direct sum of cyclic R-modules isomorphic to R.

iii. F is isomorphic to an external direct sum of copies of R.

iv. There exists a set X and an injective map $\iota : X \to F$ with the following universal property:

For every R-module A and every function of sets $f : X \to A$, there exists a unique R-module map $\tilde{f} : F \to A$ such that $\tilde{f} \circ \iota = f$.

Proof. (i) $\to$ (ii) Let X be a basis. For $x \in X$, define $R \to F, \quad r \mapsto rx$. Its image is a cyclic submodule $Rx \cong R$. Clearly, $F = \sum_{x \in X} Rx$. To show the sum is direct: if $x \in X$, see that

$$Rx \cap \sum_{y \neq x} Ry = 0,$$

otherwise we get linear dependence.

(ii) $\to$ (iii) Internal and external direct sums agree up to isomorphism.

(i) $\to$ (iv) Let X be a basis. For $f : X \to A$, define $\tilde{f}\Big(\sum r_i x_i\Big) = \sum r_i f(x_i)$. Uniqueness follows from the uniqueness of linear combinations.

(iv) $\to$ (iii) Sketch: show $R^{(X)} = \bigoplus_{x \in X} R$ is free with basis $\{e_x\}$. Free objects are unique up to isomorphism.

(iii) $\to$ (i) If $F \cong \bigoplus_{x \in X} R$, then the standard generators form a basis. □

Definition 4.4.3 (Free Module)**.** An R-module F is **free** if it satisfies any of the equivalent conditions above.

Definition 4.4.4. An R-module A is **finitely generated** if there exists a finite set $X \subseteq A$ such that $A = \langle X \rangle$.

Corollary 4.4.1. Every R-module is a epimomorphic image of a free module. If A is finitely generated, it is an epimorphic image of a finitely generated free module.

Remark 4.4.2. Every subgroup of a free abelian group is free. This is false for arbitrary rings.

Example 4.4.3. Let $R = K[x, y]$. Then $F = R$ is free. Submodules of F are ideals of R. The ideal (x, y) is not free since it is not principal. Ideals are free if and only if they are principal.

4.5 Invariant Dimension Property

Lemma 4.5.1. If k is a division ring, then any maximal linearly independent subset of a k-module V is a basis.

Corollary 4.5.1. Every nonzero module over a division ring is free.

Corollary 4.5.2. Every exact sequence of modules over a division ring splits.

Theorem 4.5.1. If R is a ring and F is a free module with one infinite basis, then any other basis is infinite with the same cardinality.

Definition 4.5.1. A ring R satisfies the **invariant dimension property** if any two finite bases of a free R-module have the same cardinality.

Example 4.5.1. $\mathbb{Z}$, fields, and division rings satisfy the invariant dimension property. However, there exist rings where the size of finite bases is not constant. The I.D.P. does not hold for every ring. Let V be an infinite dimensional vector space and let $R = \text{End}(V)$. Then $A = R$ is a free R-module with basis $\{1_R\}$ (basis with one element). Define operators L_1, L_0 on the basis $\{e_1, e_2, e_3, \dots\}$ of V by

$$L_1 = \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ e_1 & 0 & e_2 & 0 & e_3 & \end{array}$$

and

$$L_0 = \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & e_1 & 0 & e_2 & 0 & \end{array}$$

To show $\{L_0, L_1\}$ spans A, it suffices to show id $\in \text{span}\{L_0, L_1\}$. Look for operators M, N such that id $= M \circ L_1 + N \circ L_0$. Define operators M, N by

$$M = \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ e_1 & e_3 & e_5 & e_7 & e_9 & \end{array}$$

and

$$N = \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ e_2 & e_4 & e_6 & e_8 & e_{10} & \end{array}$$

Then $M \circ L_1 + N \circ L_0 = \text{id}$. Hence L_0, L_1 generate A. Suppose $L \circ L_1 + L' \circ L_0 = 0$. Then applying to e_{2i} gives

$$(L \circ L_1 + L' \circ L_0)(e_{2i}) = L' \circ L_0(e_{2i}) = L'(e_i) = 0$$

Likewise $L = 0$.

Proposition 4.5.1. Any two bases of a vector space have the same cardinality. [1]

Definition 4.5.2. Let R satisfy the invariant dimension property and let F be a free R-module. Then the **rank** of F is defined as $\text{rank}(F) = |X|$, where X is a basis.

Lemma 4.5.2. Let R be a ring and I ideal of R. If F is a free R-module with basis X, then F/IF is a free R/I -module with basis $\pi(X)$ and $|\pi(X)| = |X|$.

Proof. We note that

$$IF = \left\{ \sum s_i x_i \mid s_i \in I \right\} \subseteq F$$

is a submodule. If X is a basis, then $\pi(X) = \{x + IF \mid x \in X\}$ spans F/IF, since $F = \langle X \rangle$. We show that $\pi(X)$ is linearly independent. Suppose

$$\sum_i (r_i + I)(x_i + IF) = \sum_i r_i x_i + IF = 0.$$

Then $y = \sum r_i x_i \in IF$, hence $y = \sum_j s_j u_j$, where $s_j \in I$ and $u_j \in F$. Write

$$u_j = \sum t_{jk} x_k$$

so since I is an ideal we can consider that $s_j \in I$, therefore $y = \sum s_i x_i$ with $s_i \in I$. By the uniqueness of the representation with respect to the basis $\{x_i\}_{i \in I}$ we obtain

$$\sum r_i x_i = \sum s_i x_i \iff r_i = s_i \in I \iff r_i + I = 0$$

□

[1] More generally, any division ring satisfies the invariant dimension property.

Proposition 4.5.2. Let $R \to S$ be a ring epimorphism and suppose S satisfies the invariant dimension property. Then so does R.

Proof. Let $R \to S$ be a ring homomorphism such that $R/I \cong S$, for some ideal I. Then the isomorphism can be identified with the canonical projection $\pi\colon R \to R/I$. Let F be an R-free module. Then F/IF is an R/I-module with natural operations. By Lemma 4.5.2 if X and Y are two basis for F, then $\pi(X)$ and $\pi(Y)$ are two basis for F/IF. Since R/I has the I.D.P. then

$$|X| = |\pi(X)| = |\pi(Y)| = |Y|\,.$$

□

Corollary 4.5.3. If R is commutative then R satisfies the invariant dimension property.

Proof. Indeed, R has a maximal ideal $\mathfrak{m}$ and $\pi : R \to R/\mathfrak{m}$ is a ring epimorphism. Use the Proposition 4.5.2. □

4.6 Projective Modules

Remark 4.6.1. Suppose R is a ring and $0 \to A \to B \xrightarrow{g} F \to 0$ be a short exact sequence with F free. Then the sequence splits.

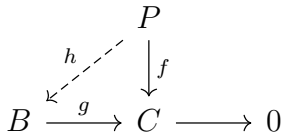
Proof. Exercise. □

Definition 4.6.1 (Definition I)**.** An R-module P is called **projective** if every short exact sequence

$$0 \to A \to B \to P \to 0$$

splits.

Definition 4.6.2 (Definition II)**.** An R-module P is **projective** if for every epimorphism $B \xrightarrow{g} C \to 0$ and every homomorphism $P \xrightarrow{f} B$, there exists $h : P \to A$ such that $g \circ h = f$, the following diagram commutes



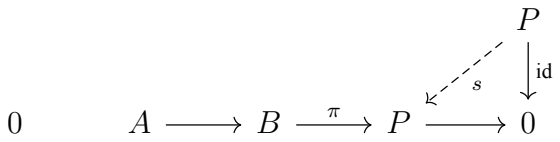
Theorem 4.6.1 (Characterization of Projective Modules)**.** The following are equivalent :

a. P satisfies **Definition 4.6.2**.

b. P satisfies **Definition 4.6.1**.

c. There exists a free module F and a module K such that $F \cong P \oplus K$.

Proof. (a) $\to$ (b) Let $0 \to A \to B \xrightarrow{\pi} P \to 0$ be exact. Since P is projective, the map $\mathrm{id}_P : P \to P$ lifts through π, i.e. there exists $s : P \to B$ with $\pi \circ s = \mathrm{id}_P$. Hence the sequence splits.



(b) $\to$ (a) Exercise.

(a) $\to$ (c) Take an epimorphism $\varepsilon : F \to P$, where F is free. Let $K = \ker(\varepsilon)$, so

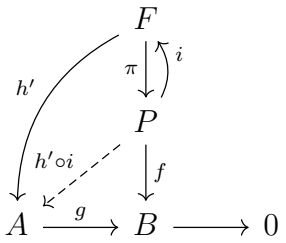
$$0 \longrightarrow K \longrightarrow F \xrightarrow{\varepsilon} P \longrightarrow 0$$

is exact. By (b) it splits, hence $F \cong P \oplus K$.

(c) $\to$ (a) Assume $F \cong P \oplus K$ with F free. We show P is projective. Let $g : A \twoheadrightarrow B$ be an epimorphism and let $f : P \to B$ be any map. Consider the composite

$$\tilde{f} := f \circ \pi_P : F \to B,$$

where $\pi_P : F \to P$ is the projection for $F \cong P \oplus K$.



If I can construct h' such that $g \circ h' = f \circ \pi$, we set $h = h' \circ i$ and $g \circ h = f$. So this implies that is suffice to prove that F is projective.

Since F is free, pick a basis X of F. For each $x \in X$, choose $a_x \in A$ with $g(a_x) = \tilde{f}(x)$ (possible since g is surjective). Define $h_X : X \to A$ by $h_X(x) = a_x$ and extend R-linearly to a homomorphism

$$h' : F \to A.$$

Then $g \circ h' = \tilde{f}$. □

example of Projectives Modules

Proposition 4.6.1. Let R be a ring and $\{P_i\}_{i\in I}$ a family of R-modules. Then

$$\bigoplus_{i\in I} P_i \text{ is projective } \iff P_i \text{ is projective for every } i \in I.$$

Proof. Exercise. □

Example 4.6.1.

a. If $R = k$ is a field, then every (nonzero) k-module is a vector space, hence free, hence projective.

b. If $R = \mathbb{Z}$, then every projective $\mathbb{Z}$-module is free. Indeed, if P is projective then P is a direct summand of a free abelian group F, and direct summands of free abelian groups are free.

c. If $R = k[x]$, every projective $k[x]$-module is free.

d. More generally, over a PID, every projective module is free.

e. If $R = k[x_1, \ldots, x_n]$, then every projective is free. This is highly nontrivial: this is the Quillen–Suslin theorem.

Example 4.6.2. Let

$$R = \frac{\mathbb{C}[x, y]}{(y^2 - (x^3 - x))},$$

the coordinate ring of the affine curve $y^2 = x^3 - x$ (the ideal $(y^2 - (x^3 - x))$ is prime). Let $I = (x, y) \subseteq R$. Then I is projective but not free.

Proof. I is not free of rank 1 because it is not principal (so it cannot be isomorphic to R as an ideal). Define a surjection $\pi : R^2 \to I$ by

$$\pi(e_1) = y, \qquad \pi(e_2) = x,$$

where (e_1, e_2) is the standard basis of R^2. Define $s : I \to R^2$ on the generators by

$$s(y) = \left(1 - x^2\right) e_1 + (xy)e_2, \qquad s(x) = (-y)e_1 + \left(x^2\right) e_2.$$

One checks s is well-defined (the relation $y^2 = x^3 - x$ is respected) and that it is a splitting:

$$\pi(s(x)) = (-y)\pi(e_1) + x^2\pi(e_2) = -y \cdot y + x^2 \cdot x = -y^2 + x^3 = x,$$

and

$$\pi(s(y)) = (1 - x^2)\pi(e_1) + (xy)\pi(e_2) = (1 - x^2)y + (xy)x = y - x^2y + x^2y = y.$$

Hence $\pi \circ s = \mathrm{id}_I$, so

$$0 \to \ker(\pi) \to R^2 \to I \to 0$$

splits and I is a direct summand of the free module R^2, therefore projective. □

Problem 4.1. Prove $\langle x, y\rangle \subset \mathbb{C}[x, y]$ is not projective.

Proof. We consider the R linear map $R^2 \xrightarrow{g} \langle x, y\rangle \to 0$ defined by

$$e_1 \mapsto x \quad \text{and} \quad e_2 \mapsto y$$

We want to show that g is not splitting. Try to define $h : \langle x, y\rangle \to R^2$ R-linear with $g \circ h = \text{id}$. If

$$x \mapsto \begin{pmatrix} p_1 \\ q_1 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} p_2 \\ q_2 \end{pmatrix}$$

then

$$xp_1 + yq_1 = x, \qquad xp_2 + yq_2 = y.$$

Using the first equality we obtain :

$$xp_1' + yq_1' = 0 \;\Rightarrow\; xyp_1'(x, y) + yxq_1(x, y) = 0$$

From the last equality, we conclude that

$$h(x) = \begin{pmatrix} 1 + yh(x, y) \\ -xh(x, y) \end{pmatrix}$$

and analogously, we prove that

$$h(y) = \begin{pmatrix} -y \cdot k(x, y) \\ 1 + x \cdot k(x, y) \end{pmatrix}$$

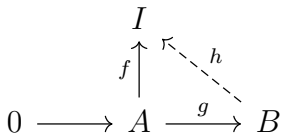
From this we get that

$$\begin{pmatrix} -xy \cdot k(x, y) \\ x + x^2 \cdot k(x, y) \end{pmatrix} = h(xy) = \begin{pmatrix} y + y^2 \cdot h(x, y) \\ -xy \cdot h(x, y) \end{pmatrix}$$

Looking the degrees of the first coordinate we conclude a contradiction. □

4.7 Injective modules

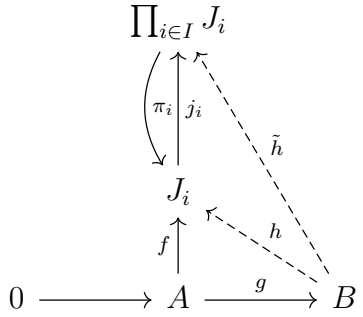
Definition 4.7.1. An R-module J is **injective** if for every monomorphism $A \xrightarrow{g} B$ and every homomorphism $f : A \to J$, there exists $h : B \to J$ such that $h \circ g = f$.



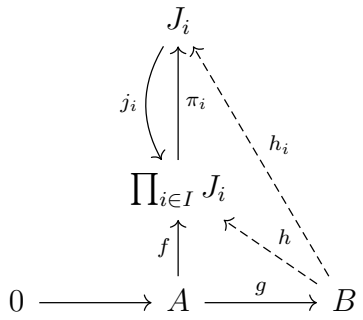
Proposition 4.7.1. Let $\{J_i\}_{i\in I}$ be R-modules. Then

$$\prod_{i\in I} J_i \text{ is injective } \iff J_i \text{ is injective for every } i \in I.$$

Proof. ($\Rightarrow$) Let $j_i : J_i \to \prod_j J_j$ be the inclusion into the ith slot and $\pi_i : \prod_j J_j \to J_i$ the projection. Check the following diagram :



($\Leftarrow$) Assume each J_i is injective. Given $A \xrightarrow{g} B$ and $f : A \to \prod_i J_i$, let $f_i = \pi_i \circ f : A \to J_i$. The injectivity of J_i gives $h_i : B \to J_i$ extending f_i. By the universal property of products, there is a unique $h : B \to \prod_i J_i$ with $\pi_i \circ h = h_i$, and then h extends f.



□

Theorem 4.7.1. Let R be a ring and J an R-module. The following are equivalent:

a. J is injective.

b. Every short exact sequence $0 \longrightarrow J \longrightarrow B \longrightarrow C \longrightarrow 0$ splits.

c. Whenever $J \subseteq B$ is a submodule, J is a direct summand of B.

Proof. (a) $\Rightarrow$ (b) : Given $0 \to J \xrightarrow{i} B \xrightarrow{p} C \to 0$, apply injectivity to $i : J \hookrightarrow B$ and $f = \mathrm{id}_J$. We get $r : B \to J$ with $r \circ i = \mathrm{id}_J$, hence i splits.

(b) $\Rightarrow$ (c) : If $J \subseteq B$, apply (b) to the exact sequence $0 \to J \to B \to B/J \to 0$. Splitting gives $B \cong J \oplus B/J$, so J is a direct summand.

(c) $\Rightarrow$ (a) : **Standard reduction using:**

- Products of injectives are injective iff each factor is injective by the Proposition 4.7.1.
- Every module embeds into an injective module (we will prove it later on the notes). Then J being a direct summand of an injective implies J is injective.

□

4.8 Divisible Modules

Definition 4.8.1. An abelian group D is **divisible** if for every $n \in \mathbb{Z}_{>0}$ the map $D \xrightarrow{\cdot n} D$ is surjective. Equivalently, for all $d \in D$ and $n \in \mathbb{Z}_{>0}$, there exists $\tilde{d} \in D$ such that $d = n \cdot \tilde{d}$.

Example 4.8.1. a. $\mathbb{Q}$ is divisible.

b. $\mathbb{Z}(p^\infty) \subseteq \mathbb{Q}/\mathbb{Z}$ is a torsion group, where $\mathbb{Z}(p^\infty) = \left\{ \dfrac{a}{p^k} \,\middle|\, k \geq 0,\ a \in \mathbb{Z} \right\}$.

Lemma 4.8.1. Let R be a ring and I an R-module. Then I is injective if and only if for every submodule $L \subseteq R$, every R-module homomorphism $L \to I$ extends to an R-module homomorphism $R \to I$. If R is commutative, it suffices to check this for ideals $L \subseteq R$.

Proof. The implication "$\Rightarrow$" is immediate. For "$\Leftarrow$", suppose we are given $0 \to A \xrightarrow{g} B$ and a morphism $f : A \to I$. Since g is an isomorphism onto $\operatorname{im} g$, we obtain a map

$$h_0 : \operatorname{im} g \to I$$

extending f. Let $\mathscr{S}$ be the set of pairs (C, h) where C is a submodule of B with $\operatorname{im} g \subseteq C$ and $h : C \to I$ satisfies $h \circ g = f$. Define a partial order on $\mathscr{S}$ by

$$(C_1, h_1) \leq (C_2, h_2) \quad \text{if} \quad C_1 \subseteq C_2 \text{ and } h_2|_{C_1} = h_1.$$

If $\{(C_i, h_i)\}$ is a chain, then

$$\left(\bigcup C_i, h \right)$$

with $h|_{C_i} = h_i$ is an upper bound. By Zorn's lemma, $\mathscr{S}$ has a maximal element (C, h). We claim that $C = B$. Let $b \in B$. Define

$$L = \{ r \in R : rb \in C \}.$$

Then L is a submodule of R, and $b \in C$ if and only if $L = R$. Define a map

$$\ell : L \to I, \qquad \ell(r) = h(rb).$$

By hypothesis, ℓ extends to a map

$$v : R \to I.$$

Now define

$$h' : C + Rb \to I, \qquad h'(a + rb) = h(a) + v(r).$$

One checks that h' is well defined and extends h. By maximality of C, we must have $C + Rb = C$, hence $Rb \subseteq C$, so $b \in C$. Therefore $C = B$, completing the proof. □

Lemma 4.8.2. Let D be an abelian group. Then D is an injective abelian group if and only if is divisible.

Proof. Suppose D is injective as a $\mathbb{Z}$-module. We want to show that D is divisible. Let $n \in \mathbb{Z} \setminus \{0\}$ and let $d \in D$. Consider the ideal $(n) = n\mathbb{Z} \subseteq \mathbb{Z}$ and define a $\mathbb{Z}$-module homomorphism

$$f : n\mathbb{Z} \to D, \quad f(mn) = md.$$

Since D is injective, there exists an extension $h : \mathbb{Z} \to D$ of f. Let $\tilde{d} = h(1)$. Then

$$d = f(n) = h(n) = nh(1) = n\tilde{d}.$$

Thus $d \in \text{im}\left(D \xrightarrow{\cdot n} D\right)$. Since $d \in D$ was arbitrary, the map $D \xrightarrow{\cdot n} D$ is surjective. Hence D is divisible. Conversely, suppose D is divisible. We want to show that D is injective as a $\mathbb{Z}$-module. By Lemma 4.8.1, it suffices to consider a homomorphism $f : I \to D$ where $I \subseteq \mathbb{Z}$ is an ideal, and show that f extends to a homomorphism $\mathbb{Z} \to D$. Any ideal of $\mathbb{Z}$ is of the form $I = (n) = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Let $d = f(n)$. Since D is divisible, there exists $\tilde{d} \in D$ such that $d = n\tilde{d}$. Define

$$h : \mathbb{Z} \to D, \quad h(1) = \tilde{d}.$$

Then for every $m \in \mathbb{Z}$,

$$h(mn) = mn\tilde{d} = md = f(mn),$$

so h extends f. Therefore D is injective as a $\mathbb{Z}$-module. □

4.9 Embeddings on Injectives

Lemma 4.9.1. Every abelian group is a subgroup of a divisible abelian group.

Proof. Let A be an abelian group. Then there exists a surjection $F = \bigoplus_I \mathbb{Z} \twoheadrightarrow A$ from a free abelian group. Consider $D = \bigoplus_I \mathbb{Q}$. Since $\mathbb{Q}$ is divisible, D is divisible. We have an exact sequence

$$0 \to K \to F \to A \to 0.$$

Thus $A \simeq F/K$. Since $F \subseteq D$, we obtain

$$A \simeq F/K \hookrightarrow D/K$$

It remains to check that a homomorphic image of a divisible group is divisible. Consider the exact sequence

$$0 \to K \to D \to D/K \to 0.$$

Multiplication by n is surjective on D, hence also surjective on D/K. Therefore D/K is divisible. □

Let R be a ring and I an abelian group. Then $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ is an abelian group. Moreover $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ has a left R-module structure defined by $(r \cdot \varphi)(s) := \varphi(sr)$, for $r, s \in R$ and $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(R, I)$. One checks that $r_1 \cdot (r_2 \cdot \varphi) = (r_1 r_2) \cdot \varphi$.

Lemma 4.9.2. Let I be a divisible abelian group. Then $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ is an injective R-module.

Proof. Let $L \subseteq R$ be a submodule and $f : L \to \mathrm{Hom}_{\mathbb{Z}}(R, I)$ an R-module homomorphism. We want to extend f to

$$h : R \to \mathrm{Hom}_{\mathbb{Z}}(R, I).$$

Define a homomorphism of abelian groups

$$g : L \to I, \quad g(a) = f(a)(1_R).$$

Since I is divisible, it is injective as a $\mathbb{Z}$-module, so g extends to a homomorphism $\overline{g} : R \to I$. Define

$$h : R \to \mathrm{Hom}_{\mathbb{Z}}(R, I), \quad h(r)(x) = \overline{g}(xr).$$

If $r \in L$, then

$$h(r)(x) = \overline{g}(xr) = g(xr) = f(r)(x),$$

so h extends f. Finally,

$$h(r_1 + r_2)(x) = \overline{g}(x(r_1 + r_2)) = h(r_1)(x) + h(r_2)(x),$$

and

$$h(r_1 r_2)(x) = \overline{g}(x r_1 r_2) = r_1 \cdot h(r_2)(x),$$

so h is an R-module homomorphism. □

Proposition 4.9.1. Every R-module is a submodule of an injective R-module.

Proof. Let A be an R-module. By Lemma 4.9.1, A is a subgroup of a divisible abelian group I. Hence we have an injective homomorphism of abelian groups $A \hookrightarrow I$. Consider the map

$$\mathrm{Hom}_{\mathbb{Z}}(R, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, I), \quad \varphi \longmapsto \iota \circ \varphi,$$

where $\iota : A \hookrightarrow I$ is the inclusion. This map is injective and is a homomorphism of R-modules. Since $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ is an abelian subgroup of $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ which is stable under the R-action, it follows that $\mathrm{Hom}_R(R, A)$ is an R-submodule of $\mathrm{Hom}_{\mathbb{Z}}(R, I)$. By Lemma 4.9.2, $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ is an injective R-module. Define a map

$$\Phi : \mathrm{Hom}_R(R, A) \longrightarrow A, \quad \Phi(\varphi) = \varphi(1).$$

This map is an isomorphism. Indeed, given $a \in A$, define

$$\varphi_a : R \to A, \quad \varphi_a(r) = ra.$$

Then φ_a is an R-module homomorphism and $\Phi(\varphi_a) = a$. Conversely, every $\varphi \in \mathrm{Hom}_R(R, A)$ satisfies $\varphi(r) = r\varphi(1)$, so $\varphi = \varphi_{\varphi(1)}$. Thus Φ is bijective. Therefore $A \simeq \mathrm{Hom}_R(R, A)$ and hence A embeds into the injective module $\mathrm{Hom}_{\mathbb{Z}}(R, I)$. □

4.10 Hom

Let R be a ring and A, B two R-modules. Then $\mathrm{Hom}_R(A, B)$ has an abelian group structure. On the other hand, if R is a ring and Y an abelian group, then $\mathrm{Hom}_{\mathbb{Z}}(R, Y)$ is an R-module given by

$$(r\varphi)(x) := \varphi(xr).$$

Remark 4.10.1.

- R is left and right R-module or bimodule.
- If R is commutative, all modules are bimodules.

Given $A \xrightarrow{f} A'$ an R-module homomorphism, then we have a homomorphism of abelian groups

$$\varphi^* : \mathrm{Hom}_R(A', B) \to \mathrm{Hom}_R(A, B), \quad \varphi \mapsto \varphi \circ f.$$

Similarly we have

$$\varphi_* : \mathrm{Hom}_R(B, A) \to \mathrm{Hom}_R(B, A'), \qquad \varphi \mapsto f \circ \varphi.$$

Theorem 4.10.1. Let R, S be rings, ${}_RA$ a left R-module, ${}_RB_S$ a bimodule and ${}_RC_S$ an R-S-bimodule.

a. $\mathrm{Hom}_R(A, B)$ is a right S-module with $(\varphi s)(a) := \varphi(a)s$.

b. If $A \xrightarrow{f} A'$ is a homomorphism of left R-modules, then

$$\varphi^* \colon \mathrm{Hom}_R(A', B) \to \mathrm{Hom}_R(A, B), \quad \varphi \mapsto \varphi \circ f$$

is a homomorphism of right S-modules.

c. $\mathrm{Hom}_R(C, D)$ is a left S-module with $(s\varphi)(c) = \varphi(cs)$.

d. If $D \xrightarrow{g} D'$ is a homomorphism of R-modules, then

$$g_* \colon \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(C, D'), \quad \varphi \mapsto g \circ \varphi$$

is a homomorphism of left S-modules.

Theorem 4.10.2. Hom and direct sums/products:

$$\mathrm{Hom}_R\left(\bigoplus_{i \in I} A_i, B\right) = \prod_{i \in I} \mathrm{Hom}_R(A_i, B)$$

$$\mathrm{Hom}_R\left(A, \prod_{j \in J} B_j\right) = \prod_{j \in J} \mathrm{Hom}_R(A, B_j).$$

Theorem 4.10.3. The sequence $0 \to A \xrightarrow{\varphi} B \to C$ is exact if and only if for every R-module D

$$0 \to \mathrm{Hom}_R(D, A) \xrightarrow{\varphi_*} \mathrm{Hom}_R(D, B) \xrightarrow{\psi_*} \mathrm{Hom}_R(D, C)$$

is exact.

Example 4.10.1. This does not assert that ψ_* is surjective when ψ is surjective. For example consider the sequence :

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_2 \to 0$$

Take $D = \mathbb{Z}_2$. Then

$$0 \to \mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_2)$$

is not surjective.

Theorem 4.10.4 (Theorem 4.3)**.** The sequence $A \to B \xrightarrow{\psi} C \to 0$ is exact if and only if for every R-module D

$$0 \to \mathrm{Hom}(C, D) \xrightarrow{\psi^*} \mathrm{Hom}(B, D) \xrightarrow{\varphi^*} \mathrm{Hom}(A, D)$$

is exact.

Example 4.10.2. If we consider the sequence

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}_2 \to 0$$

Take $D = \mathbb{Z}_2$:

$$0 \to \mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_2) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_2) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_2).$$

Notice $(\cdot 2)^* = 0$, so it is not surjective.

Theorem 4.10.5. The sequence $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ is exact if and only if for every R-module D

$$0 \to \mathrm{Hom}_R(D, A) \xrightarrow{\varphi_*} \mathrm{Hom}_R(D, B) \xrightarrow{\psi_*} \mathrm{Hom}_R(D, C)$$

is exact.

Theorem 4.10.6. The sequence $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact if and only if for every R-module D

$$0 \to \mathrm{Hom}(C, D) \xrightarrow{g^*} \mathrm{Hom}(B, D) \xrightarrow{f^*} \mathrm{Hom}(A, D)$$

is exact.

Proof. First, we suppose that the sequence

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

is exact.It is straightforward to show that g^* is injective using the surjectivity of g. For the exactness in the middle: For a map $\varphi \in \mathrm{Hom}(C, D)$ we notice

$$f^* g^*(\varphi) = f^*(\varphi \circ g) = \varphi \circ g \circ f = 0.$$

therefore $\mathrm{Im}\, g^* \subseteq \ker f^*$. Conversely, let $\varphi \in \ker f^*$: Therefore

$$f^*(\varphi) = 0 \iff \varphi \circ f = 0 \iff \varphi\Big|_{\mathrm{Im} f} = 0 \iff \varphi\Big|_{\ker g} = 0$$

Define $\bar{\varphi} : B/\ker g \to D$ where $\bar{\varphi} \circ \pi = \varphi$. Since g is surjective, then there is an isomorphism $\bar{g}\colon B/\ker g \to C$ such that $g = \bar{g} \circ \pi$. If we define $\tilde{\varphi} = \bar{\varphi} \circ \tilde{g}^{-1}$, then check that $\varphi = \tilde{\varphi} \circ g = g^*(\tilde{\varphi}) \in \mathrm{Im}\, g^*$ and we are done.

Conversely, suppose that the following sequence is exact :

$$0 \to \mathrm{Hom}(C, D) \to \mathrm{Hom}(B, D) \to \mathrm{Hom}(A, D)$$

exact. If we take $D = C/\mathrm{Im}\, g$, it suffices to show that $\pi\colon C \to D$ is the zero map. It is obvious that $g^*(\pi) = \pi \circ g = 0$, therefore by the injectivity of g^* we are obtain that $\pi = 0$. Now from the fact $f^* \circ g^* = 0$ we can easily get that $g \circ f = 0$, hence $\mathrm{Im}\, f \subseteq \ker g$. Finally, if $D = B/\mathrm{Im}\, f$, then since $\pi\colon B \to D$ satisfies :

$$\pi \circ f = f^*(\pi) = 0$$

then $\pi \in \mathrm{Im}\, g^*$ i.e. there exists $\varphi\colon C \to D$ such that $\pi = \varphi \circ g$. Hence, for each $x \in \ker g$ we get

$$\pi(x) = \varphi \circ g(x) = 0 \iff x + \mathrm{Im}\, f = 0 \iff x \in \mathrm{Im}\, f$$

and we have shown that $\ker g \subseteq \mathrm{Im}\, f$ □

Theorem 4.10.7. The following conditions on a module P over a ring R are equivalent:

a. P is projective;

b. If $\psi : B \to C$ is any R-module epimorphism, then

$$\psi_* : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$$

is an epimorphism of abelian groups;

c. If

$$0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$$

is any short exact sequence of R-modules, then

$$0 \to \mathrm{Hom}_R(P, A) \xrightarrow{\varphi_*} \mathrm{Hom}_R(P, B) \xrightarrow{\psi_*} \mathrm{Hom}_R(P, C) \to 0$$

is an exact sequence of abelian groups.

Proof. $(a) \iff (b)$ The map

$$\psi_* : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C), \quad g \mapsto \psi g$$

is an epimorphism if and only if for every R-module homomorphism $f : P \to C$, there is an R-module homomorphism $g : P \to B$ such that the diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{g} & \downarrow{\scriptstyle f} & & \\ B & \xrightarrow{\psi} & C & \longrightarrow & 0 \end{array}$$

is commutative (that is, $f = \psi g = \bar{\psi}(g)$).

(b) $\Rightarrow$ (c) 4.10.5

(c) $\Rightarrow$ (b) Given an epimorphism $\psi : B \to C$, let $A = \ker \psi$ and apply (c) to the short exact sequence

$$0 \to A \to B \xrightarrow{\psi} C \to 0.$$

□

Proposition 4.10.1. The following conditions on a module J over a ring R are equivalent:

a. J is injective;

b. if $\vartheta : A \to B$ is any R-module monomorphism, then

$$\vartheta^* : \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J)$$

is an epimorphism of abelian groups;

c. if

$$0 \to A \xrightarrow{\vartheta} B \to C \to 0$$

is any short exact sequence of R-modules, then

$$0 \to \mathrm{Hom}_R(C, J) \to \mathrm{Hom}_R(B, J) \xrightarrow{\vartheta^*} \mathrm{Hom}_R(A, J) \to 0$$

is an exact sequence of abelian groups.

Proof. The proof is dual to the last theorem and is left as an exercise. □

4.11 Dual Modules

Definition 4.11.1. Let R be a ring and A be an R - module. The set $A^* = \mathrm{Hom}_R(A, R)$ is called the **dual module**. If A is a left R-module, then A^* is a right R-module.

Theorem 4.11.1. Let A, B, C be left modules over a ring R.

a. If $\varphi : A \to C$ is a homomorphism of left R-modules, then the induced map

$$\bar{\varphi} : C^* = \mathrm{Hom}_R(C, R) \to \mathrm{Hom}_R(A, R) = A^*$$

is a homomorphism of right R-modules.

b. There is an R-module isomorphism $(A \oplus C)^* \cong A^* \oplus C^*$.

c. If R is a division ring and $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ is a short exact sequence of left vector spaces, then $0 \to C^* \xrightarrow{\bar{\psi}} B^* \xrightarrow{\bar{\varphi}} A^* \to 0$ is a short exact sequence of right vector spaces.

4.12 Tensor Product

Let R be a commutative ring and A, B, C be R-modules. A map $f : A \times B \to C$ is **bilinear** if it is linear in each factor. $A \times B$ has a natural R-module structure given by

$$r(a, b) = (ra, rb),$$

and note that a bilinear map is not linear.

Example 4.12.1. If $R = \mathbb{Z}$, and $A = B = C = \mathbb{Z}$, we get

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto ab$$

is bilinear.

Definition 4.12.1. If R is not commutative and A, B, C are R-modules, then $f : A \times B \to C$ is **middle linear** if the condition $f(ra, b),\ f(a, b) = f(a, rb)$ is replaced by $f(ar, b) = f(a, rb)$.

The tensor product is characterized by a universal property: Let R be commutative and A, B two R-modules. There exists an R-module $A \otimes_R B$ and a bilinear map

$$A \times B \xrightarrow{i} A \otimes_R B$$

such that for any bilinear map $f : A \times B \to C$, there exists a unique R-linear map $\tilde{f} : A \otimes_R B \to C$ such that $f = \tilde{f} \circ i$. Equivalently, the following diagram commutes :

$$\begin{array}{ccc} A \times B & \xrightarrow{f} & C \\ {\scriptstyle i}\downarrow & \nearrow_{\exists! \tilde{f}} & \\ A \otimes_R B & & \end{array}$$

Let A, B be R-modules, and we consider $R^{A \times B}$, the free module with basis $A \times B$. An element of $R^{A \times B}$ is a finite sum

$$\sum_{i=1}^{n} r_i \cdot (a_i, b_i).$$

Let $\mathscr{R}$ be the submodule generated by elements of the form:

1. $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$,
2. $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$,
3. $(ra, b) - r(a, b)$,
4. $(a, rb) - (ar, b)$.

We define the **tensor product** of A and B be the quotient $A \otimes_R B := R^{A \times B}/\mathscr{R}$. A coset of (a, b) in $A \otimes_R B$ is denoted by $a \otimes b$. These are called **pure tensors**. An element of $A \otimes_R B$ can be represented as a sum

$$\sum_{i=1}^{n} r_i(a_i \otimes b_i) = \sum_{i=1}^{n} (r_i a_i) \otimes b_i = \sum_{i=1}^{n} a_i \otimes (r_i b_i).$$

Now define a map

$$i : A \times B \to A \otimes_R B, \qquad i(a, b) = a \otimes b.$$

This map is bilinear by the definition of $\mathscr{R}$.

Theorem 4.12.1 (Universal Property of Tensor Product)**.** Let R be a commutative ring and A, B, C be R-modules. If $f : A \times B \to C$ is bilinear, then there exists a unique map $\tilde{f} : A \otimes_R B \to C$ such that $f = \tilde{f} \circ i$, i.e. the following diagram commutes:

$$\begin{array}{ccc} A \times B & \xrightarrow{\quad f \quad} & C \\ {\scriptstyle i}\big\downarrow & \nearrow_{\exists! \tilde{f}} & \\ A \otimes_R B & & \end{array}$$

Proof. We define the map $F : R^{A \times B} \to C$ with $F(a, b) = f(a, b)$ and extend R-linearly. We notice f is bilinear if and only if $\mathscr{R} \subseteq \ker F$. So F induces a map $\tilde{f} : A \otimes_R B \to C$ such that $\tilde{f} \circ i = f$. Moreover, suppose $h : A \otimes_R B \to C$ satisfies $h \circ i = f$. To prove $h = \tilde{f}$, it is enough to check on pure tensors:

$$h(a \otimes b) = h \circ i(a, b) = f(a, b) = \tilde{f} \circ i(a, b) = \tilde{f}(a \otimes b).$$

□

Example 4.12.2. We can show that

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z},$$

by showing that the map $\mathbb{Z} \otimes \mathbb{Z} \to \mathbb{Z}$, with $a \otimes b \mapsto ab$ is an isomorphism.

Example 4.12.3. We consider the tensor product $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3$ which is generated by

$$\left\{ \overline{0} \otimes \overline{0},\ \overline{0} \otimes \overline{1},\ \overline{0} \otimes \overline{2},\ \overline{1} \otimes \overline{0},\ \overline{1} \otimes \overline{1},\ \overline{0} \otimes \overline{2} \right\}.$$

One can checks that $a \otimes b = 0$, for all $a \in \mathbb{Z}_2$ and $b \in Z_3$. So $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3$ is zero.

Properties of Tensor Products

Example 4.12.4 (Tensor Production of Vector Spaces)**.** We consider two vector spaces V and W over a field k with basis $\{e_i\}_{i \in I}$ and $\{f_j\}_{j \in J}$ for V and W respectively. Then $\mathscr{B} = \{e_i \otimes f_j\}_{i,j}$ is a basis for $V \otimes_k W$.

Proof. We can easily show that $\{e_i \otimes f_j\}$ spans by using bilinearity. Later we shall show that $\dim_k (V \otimes_k W) = n \cdot m$, from which we conclude that $\mathscr{B}$ is actually a basis of $V \otimes_k W$. Now we need to show $\{e_i \otimes f_j\}_{i,j}$ are linearly independent. For each (k, ℓ) consider the map which is bilinear:

$$V \times W \to K, \qquad \left(\sum a_i e_i,\ \sum b_j f_j \right) \mapsto a_k b_\ell.$$

This induces a map $\Phi_{(k,\ell)} \colon V \otimes_k W \to k$, denoted $(e_k \otimes f_\ell)^* \in (V \otimes W)^*$, and act in the basis elements as following :

$$(e_k \otimes f_\ell)^*(e_i \otimes f_j) = \begin{cases} 1 & (k,\ell) = (i,j), \\ \\ 0 & \text{otherwise.} \end{cases}$$

Suppose $\sum c_{ij} e_i \otimes f_j = 0$. We show $c_{ij} = 0$, for all $i \in I$ and $j \in J$. If we apply $(e_k \otimes f_\ell)^*$ to

$$\sum c_{ij} e_i \otimes f_j = 0$$

then $c_{k\ell} = 0$. □

Theorem 4.12.2. A is an R-module. The bilinear map defined as

$$R \times A \to A, \quad (r,a) \mapsto ra$$

gives an isomorphism $R \otimes_R A \cong A$. Likewise, if A is a right R-module, this induces an isomorphism $A \otimes_R R \cong A$.

Proof. Take the pair of linear maps :

$$\varphi : R \otimes A \to A, \quad \varphi(r \otimes a) = ra,$$

and

$$\psi : A \to R \otimes A, \quad \psi(a) = 1 \otimes a.$$

□

Example 4.12.5. G is an abelian group. Then the map $\mathbb{Z} \otimes G \to G$ defined as $n \otimes g \mapsto ng$ is an isomorphism of abelian groups and $\mathbb{Z} \otimes G \cong G$.

Theorem 4.12.3. The tensor product commutes with direct limits, i.e. there is a canonical isomorphism

$$\left(\bigoplus_{i \in I} A_i \right) \otimes B \cong \bigoplus_{i \in I} (A_i \otimes B).$$

Likewise, there is a canonica isomorphism :

$$A \otimes \left(\bigoplus_{j \in J} B_j \right) \cong \bigoplus_{j \in J} (A \otimes B_j).$$

Theorem 4.12.4. R is a ring, A is an R-module, F is a free module. Then every element of $A \otimes_R F$ can be written uniquely as

$$u = \sum a_i \otimes y_i, \quad a_i \in A,\ y_i \in F.$$

In particular, this implies $A \otimes_R F \cong A^{\text{rank}(F)}$.

Proof. We choose a basis $Y = \{y_i\}_{i \in I}$ for F. This gives an a natural isomorphism

$$F \cong \bigoplus_{i \in I} R, \quad y_i \mapsto e_i.$$

But by the Theorem 4.12.3 and 4.12.2 we get :

$$A \otimes_R F \cong \bigoplus_{i \in I} A \otimes_R R \cong \bigoplus_{i \in I} A.$$

Now each element of $A \otimes F$ can be written as

$$\sum_{j=1}^{n} a_j \otimes \left(\sum_{i \in I} r_i y_i \right) = \sum_{j=1}^{n} \sum_{i \in I} (a_j r_i) \otimes y_i = \sum_{i \in I} \sum_{j=1}^{n} (a_j r_i) \otimes y_i = \sum_{i \in I} \left(\sum_{j} a_j r_j \right) \otimes y_i$$

Finally, the last calculation gives that each element of $A \otimes_R F$ can be written as

$$\sum_{j=1}^{n} a_j \otimes \left(\sum_{i \in I} r_i y_i \right) = \sum_{i \in I} a_i \otimes y_i$$

The uniqueness comes from the fact that the linear map

$$A \otimes_R F \to \oplus_{i \in I} A, \quad \sum_{i \in I} a_i \otimes y_i \mapsto \{a_i\}_{i \in I}$$

is an isomorphism. □

Corollary 4.12.1. If F_1 and F_2 are two free R-modules with basis X and Y respectively, then $F_1 \otimes F_2$ is a free R-module with basis

$$\mathscr{B} = \{x \otimes y \mid x \in X,\ y \in Y\}.$$

Exactness properties of tensor product

If $f : A \to B$ is an R-module homomorphism and D is any R-module, there is an induced homomorphism

$$D \otimes_R A \xrightarrow{1\otimes f} D \otimes_R B, \quad d \otimes a \mapsto d \otimes f(a).$$

Definition is simple but has surprising properties.

Example 4.12.6. We take the $\mathbb{Z}$ - linear map $f\colon \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$ and $D = \mathbb{Z}_3$. Then $1 \otimes f$ is a bijection :

$$\begin{array}{ccc} \mathbb{Z}_3 \otimes \mathbb{Z} & \xrightarrow{1\otimes(\cdot 2)} & \mathbb{Z}_3 \otimes \mathbb{Z} \\ \downarrow\cong & & \downarrow\cong \\ \mathbb{Z}_3 & \xrightarrow{\cdot 2} & \mathbb{Z}_3 \end{array}$$

If $D = \mathbb{Z}_4$, then $1 \otimes f$ is neither an injection and surjection :

$$\begin{array}{ccc} \mathbb{Z}_4 \otimes \mathbb{Z} & \xrightarrow{1\otimes(\cdot 2)} & \mathbb{Z}_4 \otimes \mathbb{Z} \\ \downarrow\cong & & \downarrow\cong \\ \mathbb{Z}_4 & \xrightarrow{\cdot 2} & \mathbb{Z}_4 \end{array}$$

If $D = \mathbb{Z}_2$, then $1 \otimes f$ is the zero map.

Proposition 4.12.1. If R is a ring, and the sequence $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact for any module D the induced sequence of modules

$$D \otimes_R A \xrightarrow{1\otimes f} D \otimes_R B \xrightarrow{1\otimes g} D \otimes_R C \to 0$$

is exact.

Proof. Looking at the pure tensor we conclude that $1 \otimes g$ is onto. Now is straightforward to show that $(1 \otimes g) \circ (1 \otimes f) = 0$ at the level of pure tensors, since $g \circ f = 0$, hence

$$\text{Im}(1 \otimes f) \subseteq \ker(1 \otimes g).$$

Thus, we know that there is a map $\varphi\colon D \otimes_R B/\operatorname{Im}(1 \otimes f) \to D \otimes_R C$. Want to show that this has an inverse. We need a bilinear map

$$D \times C \to D \otimes_R B/\operatorname{Im}(1 \otimes f), \quad (d, c) \mapsto d \otimes b_c$$

where $c = g(b_c)$. This map is bilinear since $\ker g = \operatorname{Im} f$, therefore there exists a map $\psi\colon D \otimes_R C \to D \otimes_R B/\operatorname{Im}(1 \otimes f)$ which is the inverse of the map $D \otimes_R B/\operatorname{Im}(1 \otimes f) \to D \otimes_R C$. Therefore, φ is injective. Hence, for all $b \in \ker g$, we have that

$$\varphi\left(\overline{d \otimes b}\right) = d \otimes g(b) = 0$$

and since φ is injective we get $\overline{d \otimes b} = 0$, i.e. $d \otimes b \in \operatorname{Im}(1 \otimes f)$ and we are done. □

Definition 4.12.2. An R-module D is **flat** if for every injection $f : A \to B$, then induced map $1 \otimes f \colon D \otimes_R A \to D \otimes_R B$ is injective.

Example 4.12.7.

a. From the Theorem 4.12.2 we have that the ring R is a flat module. Using the Theorem 4.12.3 we obtain that any free R - module is flat.

b. Since each projective module is a direct summand of a free module we obtain that every projective module is flat.

c. An abelian group is a flat $\mathbb{Z}$ module if and only if is torsion free.

Adjoint property of Hom and $\otimes$

Let R be a commutative ring, A, B, C three R-modules. The abelian group $\mathrm{Hom}_R(A \otimes_R B, C)$ is an R-module homomorphism $A \otimes_R B \to C$, which is equivalent to a bilinear map $\Phi : A \times B \to C$. Given such Φ, we can define

$$\Psi : A \to \mathrm{Hom}_R(B, C), \quad a \mapsto \Psi(a), \quad \Psi(a)(b) = \Phi(a, b).$$

By the bilinearity of Φ, we get that $\Psi \in \mathrm{Hom}_R\big(A, \mathrm{Hom}_R(B, C)\big)$. This produces an R-linear map

$$\mathrm{Hom}_R(A \otimes_R B, C) \longrightarrow \mathrm{Hom}_R\big(A, \mathrm{Hom}_R(B, C)\big).$$

Theorem 4.12.5. This natural map $\mathrm{Hom}_R(A \otimes_R B, C) \longrightarrow \mathrm{Hom}_R\big(A, \mathrm{Hom}_R(B, C)\big)$ is an isomorphism of R-modules

$$\mathrm{Hom}_R(A \otimes_R B, C) \cong \mathrm{Hom}_R\big(A, \mathrm{Hom}_R(B, C)\big).$$

Sketch. To define the inverse map $\mathrm{Hom}_R\big(A, \mathrm{Hom}_R(B, C)\big) \longrightarrow \mathrm{Hom}_R(A \otimes_R B, C)$, given $\Psi : A \to \mathrm{Hom}_R(B, C)$, define

$$\Phi : A \times B \to C, \quad \Phi(a, b) = \Psi(a)(b).$$

Then Φ is bilinear, and by considering the induced R - linear map $A \otimes_R B \to C$ gives the desired inverse. □

4.13 Finitely generated modules over a PID

This theory is developed for two important example.

a. $R = \mathbb{Z}$ and A be a finitely generated abelian group. Then

$$A \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_t},$$

where $1 < a_1 \mid \cdots \mid a_t$.

b. $R = k[x]$, k a field, A is a finitely generated module over R. Thus,

$$A \simeq R^r \oplus \frac{k[x]}{\langle a_1(x)\rangle} \oplus \cdots \oplus \frac{k[x]}{\langle a_t(x)\rangle},$$

where $a_i \neq 0$, $a_1 \mid \cdots \mid a_t$ which are called the **invariant factors** of A. This is important for the theory of the canonical forms.

Recall that for $T \in \text{End}(V)$, the pair (V, T) has a $k[x]$-module structure via $x \cdot v := T(v)$. (V, T) is a torsion $k[x]$ - module because there is $p(x) \in k[x]$ such that $p(T) = 0$.

Definition 4.13.1 (rank of a module)**.** Let A be an R-module. The **rank** of A denoted by $\text{rank}(A)$ is the maximum number of linearly independent elements in A. This is well-defined because if $S = \{a_1, \ldots, a_t\}$ is a maximal linearly independent set, then any other maximal independent set has the same cardinality.

Then $a_1, \ldots, a_t$ are maximal linearly independent in $A \otimes_R \text{Frac}(R)$, which is a $\text{Frac}(R)$-vector space. For example, If $I \subset R$ is an ideal, then $\text{rank}(I) = 1$. In general, for $B \subseteq A$ is true that $\text{rank}(B) \leq \text{rank}(A)$.

Theorem 4.13.1. Let R be a PID, F is a free module of rank n, $G \subset F$ any submodule. Then

a. G is free, of rank, $\text{rank}(G) \leq \text{rank}(F)$,

b. there is a basis $y_1, \ldots, y_n$ of F and elements $a_1 | \ldots | a_t$ in R such that $a_1 y_1, \ldots, a_t y_t$ is a basis for G.

Proof. F is free, $F^* = \text{Hom}_R(F, R)$, $G \subseteq F$ submodule. If $\varphi \in F^*$, then $\varphi(G) \subset R$ is a submodule, i.e. an ideal. Since R is a PID, $\varphi(G) = \langle a_\varphi \rangle$, for $a_\varphi \in R$. We consider the family of ideals :

$$\Sigma_G = \{\langle a_\varphi \rangle \mid \varphi \in F^*\}.$$

Since R is a PID, any ascending chain of ideals stabilizes. By Zorn's Lemma, Σ_G has a maximal element $\langle a_1 \rangle$ corresponding to a map $\nu \colon F \to R$ such that $a_1 = \nu(y)$, for some $y \in G$. If $G \neq 0$ we show that $a_1 \neq 0$. Let $x_1, \ldots, x_m$ be any basis for F. Then elements of F have unique expansions

$$z = \sum a_i x_i.$$

Define $\pi_i : F \to R$ by $\pi_i(z) = a_i$. If $G \neq 0$, then $\pi_i(G) \neq 0$ for some i, so the ideal associated to π_i is nonzero, hence $\langle a_1 \rangle \neq 0$. For all $\varphi \in F^*$, we have that $a_1 \mid \varphi(y)$, i.e. $\varphi(G) \subseteq \langle a_1 \rangle$. Let $d = \text{gcd}(\nu(y), \varphi(y))$. So

$$d = r_1 \nu(y) + r_2 \varphi(y)$$

for some $r_1, r_2 \in R$. Let $\psi \in F^*$, $\psi = r_1 \nu + r_2 \varphi$, so we obtain that $\psi(y) = d$. Thus

$$\psi(G) \supseteq \langle d \rangle \supseteq \langle \nu(y) \rangle = \langle a_1 \rangle.$$

By maximality of $\langle a_1 \rangle$, we get $\psi(G) = \langle a_1 \rangle$, so $a_1 \mid \varphi(y)$. Hence, since $y = \sum_{i=1}^{m} b_i x_i$, and $b_i = \pi_i(y)$, where $\pi_i \colon F \to R$ is the projection. We know $a_1 \mid b_i$ for all $i = 1, \ldots, m$, hence $y = a_1 y_1$,

$$y_1 = \sum_{i=1}^{m} \alpha_i x_i,$$

and $\nu(y_1) = 1$. Consider the s.e.s. :

$$0 \longrightarrow \ker v \longrightarrow F \xrightarrow{\nu} R.$$

Since R is free, the sequence splits, so

$$F \simeq R \oplus \ker \nu.$$

Since $\operatorname{Im} \nu = Ry_1$, we get

$$Ry_1 \oplus \ker v = F \quad \text{(internal sum)}.$$

Thus $G \simeq (\ker v \cap G) \oplus Ry$. However, we do not know if $\ker v$ is free, and we do not know if $\ker(v) \cap G$ is free. We use induction on the rank of the submodule. To show G is free, it suffices to show that $\ker(\nu) \cap G$ is free. To apply induction, we need

$$\operatorname{rank}(\ker(\nu) \cap G) < \operatorname{rank}(G).$$

Let $r_1, \ldots, r_s \in \ker(v) \cap G$ be a maximal set of linearly independent elements. Then $r_1, \ldots, r_s, y$ are linearly independent in G. Thus we have shown that a submodule G of F is free. We know

$$F \simeq Ry_1 \oplus \ker \nu.$$

So now $\ker(\nu) \subseteq F$ is free (by (1)) and

$$\operatorname{rank}(\ker \nu) = \operatorname{rank}(F) - 1.$$

By induction, there exists a basis $y_2, \ldots, y_m$ of $\ker(\nu)$, and $0 \neq a_2 \mid \cdots \mid a_t$ such that $a_2 y_2, \ldots, a_t y_t$ is a basis for $\ker(v) \cap G$. Since

$$G \simeq Ry \oplus (\ker(\nu) \cap G),$$

it follows that

$$y = a_1 y_1,\ a_2 y_2, \ldots, a_t y_t$$

is a basis of G. Moreover, $y_1, y_2, \ldots, y_m$ is a basis of F. To finish the proof, we need to show that $a_1 \mid a_2$. Let $\varphi \in F^*$ be the functional $\varphi = \pi_1(y_1) + \pi_1(y_2)$, so that

$$\varphi(y_1) = \varphi(y_2) = 1, \qquad \varphi(y_i) = 0 \ \text{ for } i > 2.$$

Then, $\varphi(a_2 y_2) = a_2 \in \varphi(G)$. Hence $(a_2) \subseteq \varphi(G) \subseteq \nu(G)$, so $a_1 \mid a_2$. $\square$

Theorem 4.13.2. Let R be a PID, A a finitely generated R-module. Then we have the following decomposition :

$$A = F \oplus T_1 \oplus \cdots \oplus T_t,$$

F is free, T_i is a cyclic torsion module, i.e. $T_i = R/(a_i)$, where $a_i \neq 0$ and

$$(a_1) \supseteq (a_2) \supseteq \cdots \supseteq (a_t).$$

Proof. Let R be a PID and A a finitely generated R-module, generated by $a_1, \ldots, a_m$. Then we can define a surjection $\pi : F = R^m \longrightarrow A$. Now $\ker \pi$ is free and $A = R^m / \ker(\pi)$. Moreover, there exists a basis $y_1, \ldots, y_m$ of F and elements $a_1 \mid \cdots \mid a_t$ such that $a_1 y_1, \ldots, a_t y_t$ is a basis for $\ker \pi$. Thus,

$$A \simeq \bigoplus_{i=1}^{m} \langle y_i \rangle \Big/ \bigoplus_{i=1}^{t} \langle a_i y_i \rangle \cong \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_t)} \oplus R^{m-t}$$

□

4.14 Problems

Problem 4.2. If R has an identity, then every unitary cyclic R-module is isomorphic to an R-module of the form R/J, where J is a left ideal of R.

Problem 4.3. If R has an identity, then a nonzero unitary R-module A is *simple* if its only submodules are 0 and A.

a. Every simple R-module is cyclic.

b. If A is simple, every R-module endomorphism of A is either the zero map or an isomorphism.

Problem 4.4. a. If A is a module over a commutative ring R and $a \in A$, then

$$\mathscr{O}_a = \{\, r \in R \mid ra = 0 \,\}$$

is an ideal of R. If $\mathscr{O}_a \neq 0$, a is said to be a **torsion element** of A.

b. If R is an integral domain, then the set $T(A)$ of all torsion elements of A is a submodule of A. ($T(A)$ is called the **torsion submodule**.)

c. Show that (b) may be false for a commutative ring R which is not an integral domain.

In (d)–(f) R is an integral domain.

d. If $f : A \to B$ is an R-module homomorphism, then $f(T(A)) \subseteq T(B)$; hence the restriction f_T of f to $T(A)$ is an R-module homomorphism

$$f_T : T(A) \to T(B).$$

e. If $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence of R-modules, then so is

$$0 \to T(A) \xrightarrow{f_T} T(B) \xrightarrow{g_T} T(C).$$

f. If $g : B \to C$ is an R-module epimorphism, then $g_T : T(B) \to T(C)$ need not be an epimorphism.

Problem 4.5. a. If

$$0 \to A \to B \xrightarrow{f} C \to 0 \quad \text{and} \quad 0 \to C \xrightarrow{g} D \to E \to 0$$

are short exact sequences of modules, then the sequence

$$0 \to A \to B \xrightarrow{gf} D \to E \to 0$$

is exact.

b. Show that every exact sequence may be obtained by splicing together suitable short exact sequences as in (a).

Problem 4.6. Let $f : A \to B$ and $g : B \to A$ be R-module homomorphisms such that $g \circ f = 1_A$. Show that

$$B = \text{Im } f \oplus \ker g.$$

Problem 4.7. Let $f : A \to B$ be an R-module homomorphism.

a. f is a monomorphism if and only if for every pair of R-module homomorphisms $g, h : D \to A$ such that $fg = fh$, we have $g = h$.

b. f is an epimorphism if and only if for every pair of R-module homomorphisms $k, \ell : B \to C$ such that $kf = \ell f$, we have $k = \ell$.

Problem 4.8. a. If A and B are R-modules, then the set $\text{Hom}_R(A, B)$ of all R-module homomorphisms $A \to B$ is an abelian group with $f + g$ given on $a \in A$ by

$$(f + g)(a) = f(a) + g(a) \in B.$$

The identity element is the zero map.

b. $\mathrm{Hom}_R(A, A)$ is a ring with identity, where multiplication is composition of functions. $\mathrm{Hom}_R(A, A)$ is called the **endomorphism ring** of A.

c. A is a left $\mathrm{Hom}_R(A, A)$-module with fa defined to be

$$fa = f(a) \qquad (a \in A,\ f \in \mathrm{Hom}_R(A, A)).$$

Problem 4.9. Describe the set of simple $\mathbb{Z}$-modules.

Problem 4.10. Let $f : A \to B$ be a homomorphism of R-modules.

- Show that if C is any R-module, then there are natural maps of abelian groups

$$\mathrm{Hom}_R(C, A) \to \mathrm{Hom}_R(C, B) \quad \text{and} \quad \mathrm{Hom}_R(B, C) \to \mathrm{Hom}_R(A, C).$$

- Show that f is a monomorphism if and only if the natural map of groups

$$\mathrm{Hom}_R(C, A) \to \mathrm{Hom}_R(C, B)$$

  is injective for every R-module C.

- Show that f is an epimorphism if and only if the natural map of groups

$$\mathrm{Hom}_R(B, C) \to \mathrm{Hom}_R(A, C)$$

  is injective for every R-module C.

Problem 4.11. We give three example of different $\mathbb{R}[x]$-module structures on the vector space $V = \mathbb{R}^2$ corresponding to three different linear transformations $T : \mathbb{R}^2 \to \mathbb{R}^2$.

a. Show that if T is the linear transformation that rotates a vector by $\pi/2$, then (V, T) is a simple $\mathbb{R}[x]$-module.

b. Show that if T is the linear transformation $(x, y) \mapsto (0, y)$, then the x-axis and y-axis are the only proper $\mathbb{R}[x]$-submodules of V.

c. Show that if T is the linear transformation that rotates a vector by π, then every one-dimensional subspace of V is a proper submodule.

Problem 4.12. If F is a free module over a ring with identity such that F has a basis of finite cardinality $n \geq 1$ and another basis of cardinality $n + 1$, then F has a basis of cardinality m for every $m \geq n$ ($m \in \mathbb{N}^*$).

Problem 4.13. Let $f : V \to V'$ be a linear transformation of finite-dimensional vector spaces V and V' such that $\dim V = \dim V'$. Then the following conditions are equivalent:

i. f is an isomorphism;

ii. f is an epimorphism;

iii. f is a monomorphism.

Problem 4.14. a. For each prime p, $\mathbb{Z}(p^\infty)$ (see Exercise I.1.10) is a divisible group.

b. No nonzero finite abelian group is divisible.

c. No nonzero free abelian group is divisible.

d. $\mathbb{Q}$ is a divisible abelian group.

Problem 4.15. Prove that $\mathbb{Q}$ is not a projective $\mathbb{Z}$ - module.

Problem 4.16. a. If D is an abelian group with torsion subgroup D_t, then D/D_t is torsion free.

b. If D is divisible, then so is D_t, whence

$$D = D_t \oplus E,$$

with E torsion free.

Problem 4.17. If F_1 and F_2 are free modules over a ring with the invariant dimension property, then

$$\text{rank}(F_1 \oplus F_2) = \text{rank}(F_1) + \text{rank}(F_2).$$

Problem 4.18. Every torsion-free divisible abelian group D is a direct sum of copies of the rationals $\mathbb{Q}$.

Problem 4.19. Prove that :

a. Every homomorphic image of a divisible abelian group is divisible.

b. Every direct summand (Exercise I.8.12) of a divisible abelian group is divisible.

c. A direct sum of divisible abelian groups is divisible.

Problem 4.20. Let p be a prime and D a divisible abelian p-group. Then D is a direct sum of copies of $\mathbb{Z}(p^\infty)$.

Problem 4.21. Every divisible abelian group is a direct sum of copies of the rationals $\mathbb{Q}$ and copies of $\mathbb{Z}(p^\infty)$ for various primes p.

Problem 4.22. Let G be a finite group and let $R = k[G]$ be the group ring of G. (Recall that an element of R is a k-linear combination $\sum_{i=1}^m \lambda_i[g_i]$ and multiplication is given by $[g_i][g_j] = [g_i g_j]$.) An R-module is a k-vector space together with a linear action of G meaning

$$g(v_1 + v_2) = gv_1 + gv_2, \qquad g(\lambda v) = \lambda gv.$$

An R-module homomorphism $f : V \to W$ is a k-linear map which satisfies the additional property that

$$f(gv) = g\, f(v) \qquad \text{for all } g \in G.$$

a. Show that if the characteristic of k does not divide $|G|$ then every short exact sequence of R-modules splits. Conclude that every R-module is projective.

   Hint: Any short exact sequence of R-modules splits as an exact sequence of vector spaces. If $f : V \to W$ is an epimorphism of R-modules and $h : W \to V$ is any k-linear map such that $f \circ h = 1_W$, replace h by the average

$$\frac{1}{|G|} \sum_{g \in G} gh$$

   where $(gh) : W \to V$ is defined by

$$(gh)(w) = gh(g^{-1}w).$$

   The fact that $1/|G| \in k$ requires us to assume that the characteristic of k does not divide $|G|$.

b. Show that every finitely generated R-module is finitely generated as a k-vector space.

   Hint: R is a k-vector space of rank equal to $|G|$.

c. Show that every finitely generated R-module is the direct sum of a finite number of simple R-modules. This result is called *Maschke's theorem*.

d. Show that every simple R-module is isomorphic to a summand in the free R-module R. Conclude that, up to isomorphism, there are only a finite number of simple R-modules.

   Hint: Use the fact that $\mathrm{Hom}_R(R, V)$ is isomorphic to V and is therefore non-zero if V is non-zero.

e. (Challenge) Decompose $\mathbb{C}[S_3]$ into a sum of simple R-modules; i.e. give explicit bases for the various simple S_3-invariant subspaces of the 6-dimensional vector space $\mathbb{C}[S_3]$. How many non-isomorphic simple R-modules are there?

Problem 4.23. a. For any abelian group A and positive integer m,

$$\text{Hom}(\mathbb{Z}_m, A) \cong A[m] = \{a \in A \mid ma = 0\}.$$

b. $\text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_{(m,n)}$.

Problem 4.24. Let S be a nonempty subset of a vector space V over a division ring. The annihilator of S is the subset S^0 of V^* given by

$$S^0 = \{f \in V^* \mid \langle s, f\rangle = 0 \text{ for all } s \in S\}.$$

a. $\emptyset^0 = V^*$; $\quad V^0 = 0$; $\quad S \neq \emptyset$ and $\quad S \neq \{0\} \Rightarrow S^0 \neq V^*$.

b. If W is a subspace of V, then W^0 is a subspace of V^*.

Problem 4.25. If V is a vector space over a division ring and $f \in V^*$, let $W = \{a \in V \mid \langle a, f\rangle = 0\}$. Then W is a subspace of V. If $\dim V$ is finite, determine $\dim W$.

Problem 4.26. If R has an identity and P is a finitely generated projective unitary left R-module, then

a. P^* is a finitely generated projective right R-module.

b. P is reflexive.

Problem 4.27. If A is a torsion abelian group and $\mathbb{Q}$ the (additive) group of rationals, then

a. $A \otimes \mathbb{Q} = 0$,

b. $\mathbb{Q} \otimes \mathbb{Q} \cong \mathbb{Q}$.

Problem 4.28. Let R be a commutative ring. Show that there is a ring isomorphism

$$R[x] \otimes_R R[y] \cong R[x, y].$$

Problem 4.29. Give example to show that each of the following may actually occur for suitable rings R and modules ${}_RA$, ${}_RB$:

a. $A \otimes_R B \ncong A \otimes_{\mathbb{Z}} B$.

b. $u \in A \otimes_R B$, but $u \neq a \otimes b$ for any $a \in A$, $b \in B$.

c. $a \otimes b = a_1 \otimes b_1$ but $a \neq a_1$ and $b \neq b_1$.

Problem 4.30. For any abelian group A and positive integer m:

(a) $\text{Hom}(\mathbb{Z}_m, A) \cong A[m] = \{a \in A \mid ma = 0\}$.

(b) $\text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_{(m,n)}$.

(c) The $\mathbb{Z}$-module $\mathbb{Z}_m$ has $\mathbb{Z}_m^* = 0$.

(d) For each $k \geq 1$, $\mathbb{Z}_m$ is a $\mathbb{Z}_{mk}$-module; as a $\mathbb{Z}_{mk}$-module, $\mathbb{Z}_m^* \cong \mathbb{Z}_m$.

Problem 4.31. If A, B are abelian groups and m, n are integers such that $mA = 0 = nB$, then every element of $\text{Hom}(A, B)$ has order dividing (m, n).

Problem 4.32. Let $\pi : \mathbb{Z} \to \mathbb{Z}_2$ be the canonical epimorphism. The induced map

$$\overline{\pi} : \text{Hom}(\mathbb{Z}_2, \mathbb{Z}) \to \text{Hom}(\mathbb{Z}_2, \mathbb{Z}_2)$$

is the zero map. Since $\text{Hom}(\mathbb{Z}_2, \mathbb{Z}_2) \neq 0$, $\overline{\pi}$ is not an epimorphism.

Problem 4.33. Let S be a nonempty subset of a vector space V over a division ring. The **annihilator** of S is the subset S^0 of V^* given by

$$S^0 = \{f \in V^* \mid \langle s, f \rangle = 0 \text{ for all } s \in S\}.$$

(a) $0^0 = V^*$; $V^0 = 0$; if $S \neq \{0\}$, then $S^0 \neq V^*$.

(b) If W is a subspace of V, then W^0 is a subspace of V^*.

(c) If W is a subspace of V and $\dim V$ is finite, then $\dim W^0 = \dim V - \dim W$.

(d) Let W, V be as in (c). There is an isomorphism $W^* \cong V^*/W^0$.

Problem 4.34. Let A and B be abelian groups.

(a) For each $m > 0$, $A \otimes \mathbb{Z}_m \cong A/mA$.

(b) $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_c$, where $c = (m, n)$.

(c) Describe $A \otimes B$ when A and B are finitely generated.

Problem 4.35. The usual injection $\alpha : \mathbb{Z}_2 \to \mathbb{Z}_4$ is a monomorphism of abelian groups. Show that

$$1 \otimes \alpha : \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes \mathbb{Z}_4$$

is the zero map (but $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \neq 0$ and $\mathbb{Z}_2 \otimes \mathbb{Z}_4 \neq 0$; see Exercise 2).

Problem 4.36. a. Show that a projective module is flat.

b. Show that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module which is not projective.

c. Show that the divisible group $\mathbb{Q}/\mathbb{Z}$ is not a flat $\mathbb{Z}$-module. Is $\mathbb{Z}[p^\infty]$ flat?

d. Prove that if A, B are R-modules, then $A \otimes_R B^*$ is naturally isomorphic to $\mathrm{Hom}_R(A, B^*)$.

Problem 4.37. R is a non-zero commutative ring with identity and every submodule of every free R-module is free. Then R is a principal domain.

Problem 4.38. Let T be the matrix

$$\mathrm{T} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

a. Determine the invariant factors for the $R[x]$-module $(\mathbb{R}^3, \mathrm{T})$.

b. Determine the invariant factors for the $\mathbb{C}[x]$-module $(\mathbb{C}^3, \mathrm{T})$.

c. Determine the invariant factors for the $k[x]$-module (k^3, T), where k is a field of characteristic 3.

Problem 4.39. Let R be a principal ideal domain. For each positive integer r and sequence of nonzero ideals

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_r,$$

choose a sequence $d_1, \ldots, d_r \in R$ such that $(d_i) = I_i$ and $d_1 \mid d_2 \mid \cdots \mid d_r$. For a given pair of positive integers (n, m), let S be the set of all $n \times m$ matrices of the form

$$\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix},$$

where $r = 1, 2, \ldots, \min(n, m)$ and L_r is an $r \times r$ diagonal matrix with main diagonal one of the chosen sequences $d_1, \ldots, d_r$.

Show that S is a set of canonical forms under equivalence for the set of all $n \times m$ matrices over R.

Problem 4.40. Prove of give a counter–example.

a. Every non-zero submodule of a free module is free.

b. If $A \to B \to 0$ is a surjective morphism of R-modules, then $\mathrm{Hom}_R(C, A) \to \mathrm{Hom}_R(C, B)$ is surjective for any R-module C.

c. Every non-zero submodule of a projective module is projective.

d. A $\mathbb{Z}$-module is projective if and only if it is free.

e. Every finite basis of a free module has the same cardinality.

f. Every finite basis of a vector space has the same cardinality.

Chapter 5

Linear Algebra

5.1 Rank - Nullity Theorem

Let R be commutative. Let E and F be free R-modules of ranks n and m, respectively. Each choice of ordered bases

$$(u_1, \ldots, u_n) \quad \text{of } E, \qquad (v_1, \ldots, v_m) \quad \text{of } F$$

defines an isomorphism

$$\text{Hom}_R(E, F) \;\cong\; M_{m\times n}(R).$$

Theorem 5.1.1. Let E, F, G be free R-modules of ranks n, m, p, respectively, and fix bases for E, F, G. If

$$f \in \text{Hom}_R(E, F) \quad \text{has matrix } A, \qquad g \in \text{Hom}_R(F, G) \quad \text{has matrix } B,$$

then the composition $g \circ f \in \text{Hom}_R(E, G)$ has matrix AB.

Remark 5.1.1. Let E be an R-module. Then $\text{End}_R(E)$ is a ring with the composition. $\text{End}_R(E)$ is not typically commutative even if R is commutative.

Corollary 5.1.1. Let R be a commutative ring, and E be an R-free module. Then a choice of basis $\mathscr{U} = \{u_1, \ldots, u_n\}$ defines an isomorphism

$$f : \text{End}_R(E) \longrightarrow M_n(R), \quad \varphi \mapsto A_\varphi,$$

where A_φ is the matrix of φ with respect to the basis $\mathscr{U}$.

Remark 5.1.2. The multiplicative group of invertible matrices is denoted by $GL_n(R)$.

Example 5.1.1. We have that $A \in GL_n(\mathbb{R}) \iff \det(A) \neq 0$. Also $A \in GL_n(\mathbb{Z})$ if and only if $\det A \in \{-1, 1\}$. So $\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$, but not in $GL_2(\mathbb{Z})$, while $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{Z})$.

Definition 5.1.1. Two matrices $A, B \in M_{n\times m}(R)$ are **equivalent** if there exist matrices $P \in GL_n(R)$ and $Q \in GL_m(R)$ such that $B = PAQ$. We also $A \in M_{n\times n}(R)$ is **similar** to B if there exists $P \in GL_n(R)$ such that $B = PAP^{-1}$.

Theorem 5.1.2. a. Let $\varphi : E \to F$ be a map of free R-modules. Let A and B be the matrices of φ with respect to ordered bases $\mathscr{U}$ and $(\mathscr{U}')$ respectively. Then A is equivalent to B.

b. If $A \in M_{n\times m}(R)$ is equivalent to a matrix B, then if A corresponds to an R-linear map $\varphi : R^n \to R^m$, there are bases $\mathscr{U}$ and $\mathscr{V}$ of R^n and R^m respectively such that B is the matrix of φ with respect to these bases.

Proof. a. We consider the following maps:

$$\text{id} : E \to E, \quad P = (\text{id} : \mathscr{U}' \to \mathscr{U}),$$

$$\text{id} : F \to F, \quad Q = (\text{id} : \mathscr{V} \to \mathscr{V}').$$

Then, by considering the composition $\varphi : E \to F = (\text{id}_F \circ \varphi \circ \text{id}_E)$, we get B=PAQ.

b. Part (b) is left as an exercise.

□

Example 5.1.2. Let $R = \mathbb{Z}$, $E = \mathbb{Z}^2$. Consider the ordered bases

$$\mathscr{U} = \left\{ \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}, \quad \mathscr{U}' = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$$

Now we consider the map $\text{id} : \mathbb{Z}^2 \to \mathbb{Z}^2$.

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2e_1 + e_2, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix} = e_1 + e_2.$$

So

$$A = (\text{id} : \mathscr{U} \to \mathscr{U}') = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Now for the inverse:

$$\text{id} : \mathbb{Z}^2 \to \mathbb{Z}^2, \quad \mathscr{U}' \mapsto \mathscr{U},$$

with

$$e_1 \mapsto u_1 - u_2, \qquad e_2 \mapsto -u_1 + 2u_2,$$

so

$$(\text{id} : \mathscr{U}' \to \mathscr{U}) = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}.$$

Corollary 5.1.2. If $\mathscr{U}, \mathscr{U}'$ are two bases for an R-free module E and $\varphi : E \to E$ is a linear transformation, then if

$$A = (\varphi : \mathscr{U} \to \mathscr{U}), \quad B = (\varphi : \mathscr{U}' \to \mathscr{U}'),$$

then A and B are similar.

Definition 5.1.2. Let k be a field and $f : E \to F$ be a k-linear map. We define:

$$\text{rank}(f) := \text{rank}(\text{Im}\, f) = \dim(\text{Im}\, f),$$

$$\text{null}(f) := \text{rank}(\ker f) = \dim(\ker f).$$

Theorem 5.1.3 (null-rank for vector spaces)**.** If k is a field and $f : E \to F$ is k-linear, then:

$$\dim(E) = \text{null}(f) + \text{rank}(f).$$

Proof. We consider the short exact sequence:

$$0 \to \ker f \to E \to \text{Im}\, f \to 0.$$

Since Im f is a free k-module, this sequence splits so: $E \simeq \ker f \oplus \text{Im}\, f$, and we are done. □

Definition 5.1.3. (rank of a linear map of modules) Let $f : E \to F$ be a linear map of modules over an integral domain R. Then we define:

$$\text{rank}(f) = \text{rank}(\text{Im}\, f), \qquad \text{null}(f) = \text{rank}(\ker f).$$

Theorem 5.1.4 (general rank-null theorem)**.** If R is an integral domain and $f : E \to M$ is a linear map, then:

$$\text{rank}(E) = \text{rank}(f) + \text{null}(f).$$

Proof. See Homework VI. □

5.2 Row/Column Rank of a matrix

Definition 5.2.1. Let R be a domain and $A \in M_{n\times m}(R)$. We define colrank(A) to be the rank of the submodule of R^n generated by the columns of A. Similarly, the rowrank(A) is defined as the rank of the submodule of R^m generated by the rows of A.

Remark 5.2.1. A matrix $A \in M_{n\times m}(R)$ defines a map of free R-modules

$$\varphi : R^m \to R^n, \quad e_i \mapsto Ae_i \quad \text{(the } i\text{-th column of } A\text{)}.$$

If $\varphi(A)$ denotes the span of the columns of A, then colrank$(A) =$ rank(φ).

Proposition 5.2.1. With the above assumptions, rowrank$(A) =$ colrank(A).

Proof. Let $v_1, \ldots, v_m$ be the rows of A. Then the row rank is the rank of the span $\langle v_1, \ldots, v_\rangle \subseteq R^m$. Passing to the field of fractions $k =$ Frac(R), we consider then $\langle v_1 \otimes 1, \ldots, v_n \otimes 1\rangle \subseteq R^m \otimes_R k \cong k^m$. which is a k - vector space. Thus, rowrank$(A) =$ rowrank$(A \otimes 1)$. Similarly, colrank$(A) =$ colrank$(A \otimes 1)$, where $A \otimes 1$ is the matrix A with entries in k. Hence it suffices to prove the result over a field. □

Proposition 5.2.2. If k is a field and $A \in M_{n\times m}(k)$, then

$$\text{colrank}(A) = \text{rowrank}(A) = \text{colrank}(A^t).$$

Lemma 5.2.1. If A represents a linear map $\varphi : E \to F$, then A^t represents the dual map

$$\varphi^* : F^* \to E^*, \quad \varphi^*(f) = f \circ \varphi.$$

Proof. Let $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_n\}$ be bases of E and F, with dual bases $\{u_1^*, \ldots, u_m^*\}$ and $\{v_1^*, \ldots, v_n^*\}$. For $i = 1, \ldots, n$ we have that

$$\varphi^*\left(v_i^*\right) = \sum_{j=1}^{m} b_{ij} u_j^*.$$

Now for arbitrary $k \in \{1, \ldots, m\}$ we get $\varphi(u_k) = \sum_{\ell=1}^{n} a_{k\ell} v_\ell$, then $\varphi^*(v_i^*)(u_k) = b_{ik}$. Additionally,

$$\varphi^*(v_i^*)(u_k) = v_j^*(\varphi(u_k)) = v_i^*\left(\sum_{\ell=1}^{n} a_{k\ell} v_\ell,\right) = a_{ki} = b_{ik}.$$

Hence the matrix of φ^* is A^t. □

Proposition 5.2.3. If $\varphi : E \to F$ is linear (over a field), then rank$(\varphi) =$ rank(φ^*).

Proof. From the rank-nullity theorem,

$$\operatorname{rank}(\varphi) = \dim E - \dim \operatorname{null} \varphi \quad \text{and} \quad \operatorname{rank} \varphi^* = \operatorname{rank} F^* - \operatorname{null} \varphi^*$$

For a vector space $W \subseteq E$ we define $\operatorname{Ann}(W) = \{f \in E^* \mid f|_W = 0\}$. Considering the map

$$E^* \to W^*, \quad f \mapsto f|_W$$

from rank - nullity theorem we get :

$$\operatorname{rank}(E^*) = \operatorname{Ann}(W) + \operatorname{rank}(F^*).$$

Applying the last relationship for $W = \operatorname{Im} \varphi$ and notice that $\operatorname{null} \varphi^* = \operatorname{Ann}(\operatorname{Im} \varphi)$. □

Elementary Row and Column Operations

Definition 5.2.2. Elementary row (column) operations on a matrix $A \in M_{m\times n}(R)$ are:

1. Exchange two rows (columns).
2. Multiply a row (column) by a unit.
3. Replace a row (column) by a linear combination with another row (column).

Remark 5.2.2. Row operations correspond to replacing A with EA, where E is an elementary matrix obtained by applying the operation to I_n. Analogously, column operations correspond to replacing A with AE, where E is an elementary matrix. Elementary matrices are invertible over any ring R.

Proposition 5.2.4. If $B \in M_{n\times m}(R)$ has been obtained from A by elementary row and column operations, then B is equivalent to A.

Proposition 5.2.5 (Smith normal form)**.** Let R be a P.I.D., then after a sequence of row/column operations for $A \in M_{n\times m}(R)$, A can be put in Smith Normal Form

$$\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_t & \\ & & & 0 \end{pmatrix} \qquad d_1 \mid \cdots \mid d_t$$

An important case is when $R = k$ field Smith Normal Form:

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

Corollary 5.2.1. $A \in M_{n\times m}(k)$ is equivalent to $B \in M_{n\times m}(k)$ iff rank$(A) =$ rank(B).

Proposition 5.2.6. $A \in M_{n\times n}(k)$, k field. The following are equivalent:

a. rank$(A) = n$

b. A is equivalent to I_n

c. A is invertible

d. A is a product of elementary matrices

e. I_n can be obtained by A using only row (column) operations.

5.3 Eigenvalues and Diagonalization

Definition 5.3.1. Let $T : E \to E$ be a linear transformation. A nonzero vector $v \in E$ is called an **eigenvector** with eigenvalue $\lambda \in K$ if $Tv = \lambda v$.

Given $T : E \to E$ a linear transformation on a finite-dimensional vector space E, we want to find (if possible) a basis of E consisting of eigenvectors of T. This is called the **diagonalization problem**.

Definition 5.3.2. The endomorphism $T\colon E \to E$ is called **diagonalizable** if E has a basis of eigenvectors of T. Equivalently, $A \in M_n(K)$ is diagonalizable if K^n has a basis of eigenvectors of A.

Proposition 5.3.1. $A \in M_n(K)$ is diagonalizable if and only if A is similar to a diagonal matrix.

How to find eigenvalues/eigenvectors

Let dim $E = n$ and $T : E \to E$ be linear. A nonzero vector v is an eigenvector with eigenvalue $\lambda \in K$ if and only if

$$Tv = \lambda v \quad \iff \quad (T - \lambda I)v = 0.$$

Thus,

$$v \in \ker(T - \lambda I) \quad \iff \quad \det(T - \lambda I) = 0.$$

If A is a matrix representing T, then

$$\det(T - \lambda I) = \det(A - \lambda I).$$

If $B = PAP^{-1}$, then

$$B - \lambda I = P(A - \lambda I)P^{-1}.$$

Proposition 5.3.2. The eigenvalues of T are the roots of the polynomial $c_T(x) = \det(T - xI)$.

Definition 5.3.3. The polynomial $c_T(x) = \det(T - xI)$ is called the **characteristic polynomial** of T.

If $\lambda \in K$ is a root of $c_T(x)$, then $\ker(T - \lambda I)$ is the eigenspace corresponding to λ. For $\lambda = 0$, the eigenspace is $\ker(T) = \text{null}(T)$.

Proposition 5.3.3. If K is algebraically closed (e.g. $K = \mathbb{C}$), then every linear transformation has at least one eigenvalue.

Proof. The characteristic polynomial $c_T(x)$ has at least one root by the Fundamental Theorem of Algebra. □

Example 5.3.1. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$. Then

$$\det(A - xI) = \det \begin{pmatrix} -x & 1 \\ -1 & -x \end{pmatrix} = x^2 + 1,$$

which has no real roots. Hence A is not diagonalizable over $\mathbb{R}$. Over $\mathbb{C}$, the eigenvalues are $\lambda = \pm i$, so A is diagonalizable over $\mathbb{C}$. To compute eigenvectors:

$$(A - iI) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -i & 1 \\ -1 & -i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow -ix + y = 0 \Rightarrow y = ix,$$

gives so $(1, i)^T$ is an eigenvector for $\lambda = i$. Similarly, $(1, -i)^T$ is an eigenvector for $\lambda = -i$. Thus A is similar to

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Proposition 5.3.4. If $c_T(x)$ has n distinct roots $\lambda_1, \ldots, \lambda_n$ (where $n = \dim E$), then T is diagonalizable. [1]

Proposition 5.3.5. Let $v_1, \ldots, v_n$ be eigenvectors with distinct eigenvalues $\lambda_1, \ldots, \lambda_n$. Then $v_1, \ldots, v_n$ are linearly independent.

Proof. Suppose

$$a_1 v_1 + \cdots + a_m v_m = 0$$

Apply T:

$$a_1 \lambda_1 v_1 + \cdots + a_m \lambda_m v_m = 0.$$

Subtract λ_1 times the original relation:

$$a_2(\lambda_2 - \lambda_1)v_2 + \cdots + a_m(\lambda_m - \lambda_1)v_m = 0,$$

and use induction. □

[1] The converse is not true. For example $A = I_n$ is diagonalizable, but all its eigenvalues are equal.

Example 5.3.2. (Power of diagonalization) Let

$$A = \begin{pmatrix} 3 & 0 & 0 \\ -2 & 1 & 0 \\ 5 & 1 & -1 \end{pmatrix}.$$

Then, $\det(A - xI) = (3-x)(1-x)(-1-x)$, so the eigenvalues are $3, 1, -1$. Thus A is diagonalizable:

$$A = PDP^{-1}, \quad D = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Hence

$$A^{30} = PD^{30}P^{-1}.$$

5.4 Minimal Polynomial

Theorem 5.4.1. Let $T : E \to E$ be a linear transformation on an n-dimensional vector space over k. There exists a unique monic polynomial $q_T \in k[x]$ such that $q_T(T) = 0$, and if $f(T) = 0$, then $q_T \mid f$. Moreover, $\deg q_T \leq n$.

Theorem 5.4.2. For $A \in M_n(k)$, there exists a polynomial $q_A \in k[x]$ such that $q_A(A) = 0$, and if $f(A) = 0$, then $q_A \mid f$. If A is similar to B, then $q_A = q_B$.

Proof. Define

$$\Phi_T : k[x] \to \mathrm{End}_k(E), \quad x \mapsto T.$$

This is a homomorphism of K-algebras. Since $k[x]$ is infinite-dimensional and $\mathrm{End}_k(E)$ has dimension n^2, $\ker(\Phi_T) \neq 0$. Since $k[x]$ is a PID, $\ker(\Phi_T) = \langle q_T \rangle$ for a unique monic polynomial q_T. □

5.5 Cayley–Hamilton Theorem

Theorem 5.5.1 (Cayley–Hamilton)**.** Let $T : E \to E$ be a linear transformation on a finite-dimensional vector space. Then $q_T \mid c_T$, where q_T denotes the minimal polynomial of T and c_T the characteristic polynomial of T.

Remark 5.5.1. For $A \in M_n(R)$ (with R commutative), $c_A(A) = 0$, where $c_A(x) = \det(A - xI)$.

In fact, we will prove a slightly stronger statement.

Proposition 5.5.1. Let R be a commutative ring and let $A \in M_{n\times n}(R)$. Then $c_A(A) = 0$, where $c_A(x) = \det(A - xI)$.

Proof. Let $B = A - x\mathrm{I} \in M_{n\times n}(R[x])$. Recall that $BB^{\text{adj}} = (\det B)\cdot \mathrm{I}_n$. Since $\det(B) = c_A(x)$, we get $B^{\text{adj}}(A - xI) = c_A(x)I$. We now interpret each entry of this matrix as an operator on R^n, where the $R[x]$-module structure on R^n is given by $x \cdot v = Av$. Let

$$B_{ij} = \delta_{ij}x - A_{ij} \in R[x].$$

Viewed as an operator on R^n, we have $B_{ij}v = (\delta_{ij}A - A_{ij}I)v$. Let $e_1, \ldots, e_n$ be the standard basis of R^n. Then

$$B_{ij}e_i = \delta_{ij}A(e_i) - A_{ij}e_i.$$

Since $A(e_j) = \sum_{i=1}^n A_{ij}e_i$, it follows that

$$\sum_{i=1}^n B_{ij}e_i = A(e_j) - \sum_{i=1}^n A_{ij}e_i = 0.$$

Now apply the operator B_{jk}^{adj} to this equality: $B_{jk}^{\text{adj}}\left(\sum_{i=1}^n B_{ij}e_i\right) = 0$. Summing over i, we obtain

$$0 = \sum_{i=1}^n B_{jk}^{\text{adj}}\left(\sum_{j=1}^n B_{ij}e_i\right) = \sum_{i=1}^n \left(\sum_{j=1}^n B_{jk}^{\text{adj}}B_{ij}\right)e_i.$$

But $B^{\text{adj}}B = (\det B)\mathrm{I}$, hence by looking the entry (k, j) of the previous inequality we get :

$$\sum_{j=1}^n B_{kj}^{\text{adj}}B_{ij} = \delta_{ik}\det(B) \Rightarrow 0 = \sum_{i=1}^n \delta_{ik}\det(B)e_i = \det(B)e_k.$$

Therefore, Since this holds for every k, we conclude that $\det(B)$ acts as the zero operator on R^n. Hence $c_A(A) = 0$. □

5.6 Invariant Factors

Definition 5.6.1. Let $T : E \to E$ be a linear transformation. A subspace $F \subseteq E$ is called T-**invariant** if $T(F) \subseteq F$.

Example 5.6.1. The following subspaces are T-invariant: $\ker(T)$, $\mathrm{im}(T)$, and more generally every eigenspace

$$\ker(T - \lambda I), \quad \lambda \in K.$$

Proposition 5.6.1. The operator T is diagonalizable if and only if E has a basis of eigenvectors. Equivalently, E splits as a direct sum of one-dimensional invariant subspaces.

Proposition 5.6.2. If K is algebraically closed, then every invariant subspace is a sum of eigenspaces.

Example 5.6.2. Let $k = \mathbb{C}$ and $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Then

$$x\mathrm{I} - A = \begin{pmatrix} x & -1 & 0 \\ 0 & x & -1 \\ -1 & 0 & x \end{pmatrix} \Rightarrow c_A(x) = \det(x\mathrm{I} - A) = x^3 - 1.$$

Thus the eigenvalues are $1, \omega, \omega^2$, where $\omega = e^{2\pi i/3}$. Hence the one-dimensional invariant subspaces are

$$V_A(1) = \langle (1,1,1) \rangle, \qquad V_A(\omega) = \langle (1, \omega, \omega^2) \rangle, \qquad V_A\left(\omega^2\right) = \langle (1, \omega^2, \omega) \rangle.$$

Now, if we consider the same matrix over the rational number we have $c_A(x) = (x-1)\left(x^2 + x + 1\right)$. There is only one eigenspace over $\mathbb{Q}$, namely $V_A(1) = \langle (1,1,1) \rangle$. Moreover,

$$\mathbb{Q}^3 = \langle (1,1,1) \rangle \oplus F, \quad \text{where} \quad F = \left\{ (a,b,c) \in \mathbb{Q}^3 \;\middle|\; a+b+c = 0 \right\}.$$

A basis for F is $\{(1,-1,0), (1,0,-1)\}$.

Example 5.6.3. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $c_A(x) = x^2 + 1$. Since this polynomial is irreducible over $\mathbb{Q}$, then $\mathbb{Q}^2$ has no non-trivial A-invariant subspaces.

Definition 5.6.2. Let $T : E \to E$ and let $F \subseteq E$ be a T-invariant subspace. We say that F is **T-cyclic** if there exists $v \in F$ such that $\{v, T(v), T^2(v), \ldots, T^n(v), \ldots, \}$ spans F. Such a vector v is called a **cyclic vector**.

Lemma 5.6.1. View E as a $k[x]$-module via $x \cdot v = T(v)$. Then a subspace $F \subseteq E$ is T-cyclic if and only if F is a cyclic $k[x]$-module.

Proof. Suppose first that F is T-cyclic with cyclic vector v. Then every element of F is of the form

$$(a_r T^r + \cdots + a_1 T + a_0 \mathrm{I})v.$$

Equivalently, each element can be written as $p(T)v$, for some polynomial $p(x) \in k[x]$. Viewing F as a $k[x]$-module, this means that every element of F is of the form $p(x) \cdot v$. Hence v generates F as a $k[x]$-module. The converse is left as an exercise. □

Example 5.6.4. Consider again the matrix $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Then both $\mathbb{Q}^3$ and $\mathbb{C}^3$ are cyclic, since they are generated by $e_1 = (1,0,0)$ as $k[x]$ - modules.

Example 5.6.5. Let $V = \mathbb{Q}^3$ and $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Consider the invariant subspace

$$F = \left\{(a, b, c) \in \mathbb{Q}^3 \;\middle|\; a + b + c = 0\right\}.$$

A basis is $v_1 = (1, -1, 0)$ and $v_2 = (1, 0, -1)$. We compute:

$$Av_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = -v_2,$$

and

$$Av_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} = v_1 - v_2.$$

Hence the matrix of $T_{A|F}$ in the basis (v_1, v_2) is $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Its characteristic polynomial is $x^2 + x + 1$.

Invariant Factor Decomposition

Theorem 5.6.1. Let $\varphi : E \to E$ be a linear transformation on a finite-dimensional vector space over k. Then:

i. There exist monic polynomials $q_1, \ldots, q_t \in k[x]$ satisfying $q_1 \mid q_2 \mid \cdots \mid q_t$, and φ-invariant subspaces $E_1, \ldots, E_t$ such that:

   a. each $E_i \cong k[x]/\langle q_i(q)\rangle$ is cyclic,

   b. the minimal polynomial of $\varphi_{|E_i}$ is q_i,

   c. $E = E_1 \oplus \cdots \oplus E_t$.

   The polynomials $q_1, \ldots, q_t$ are called the **invariant factors** of φ.

ii. There exist irreducible monic polynomials $p_1, \ldots, p_s \in k[x]$, $m_{ij} \geq 1$, and cyclic invariant subspaces

$$E_{11}, \ldots, E_{1k_1}, \ldots, E_{s1}, \ldots, E_{sk_s}$$

such that the minimal polynomial of $\varphi|_{E_{ij}}$ is $p_i^{m_{ij}}$, and $E = \bigoplus_{i,j} E_{ij}$. This decomposition is called the **elementary divisor decomposition**.

Proof. We view E as a $k[x]$-module via

$$f \cdot u := f(\varphi)(u), \quad f \in k[x],\ u \in E.$$

Since $\dim_k E < \infty$ and $k \subseteq k[x]$, it follows that E is finitely generated over $k[x]$. Let q_φ be the minimal polynomial of φ. Then

$$q_\varphi(\varphi) = 0 \quad \Rightarrow \quad q_\varphi \cdot E = 0,$$

so E is a torsion $k[x]$-module. Since $k[x]$ is a principal ideal domain, the structure theorem for finitely generated torsion modules gives:

$$E \cong \bigoplus_{i=1}^{t} k[x]/(q_i),$$

where $q_1 \mid q_2 \mid \cdots \mid q_t$. Each summand corresponds to a cyclic $k[x]$-submodule E_i, so

$$E = E_1 \oplus \cdots \oplus E_t.$$

Each E_i is cyclic, hence of the form $E_i \cong k[x]/(q_i)$. Thus E_i is generated by some $v_i \in E$ and $E_i = k[x] \cdot v_i = E(\varphi, v_i)$, so each E_i is a φ-cyclic subspace. Let $v_i \in E_i$ correspond to $\overline{1} \in k[x]/(q_i)$ under the isomorphism $E_i \cong k[x]/(q_i)$. Then v_i generates E_i as a $k[x]$-module, so $E_i = k[x] \cdot v_i$. Now, if $f \in k[x]$, then under this isomorphism

$$f(x) \cdot v_i = f(\varphi)(v_i) \longleftrightarrow f(x) \cdot \overline{1} = \overline{f(x)}.$$

Therefore,

$$f(x) \cdot v = 0 \iff f(\varphi)(v_i) = 0 \iff \overline{f(x)} = 0 \text{ in } K[x]/(q_i) \iff f \in (q_i) \iff q_i \mid f.$$

Since v_i generates E_i, this means that the polynomials annihilating $\varphi|_{E_i}$ are exactly the multiples of q_i. Hence q_i is the minimal polynomial of $\varphi|_{E_i}$. From the decomposition,

$$q_\varphi(\varphi)E = q(\varphi)E_1 \oplus \cdots \oplus q_\varphi(\varphi)E_t = 0,$$

so q_φ annihilates each E_i, hence $q_1 \mid q_\varphi$, for all $i = 1, \ldots, t$. Conversely, since $q_t(\varphi)$ annihilates all components, then $q_t(x) \cdot E = 0$. Hence $q_\varphi = q_t$. The uniqueness follows from the uniqueness part of the structure theorem for modules over a PID, together with the divisibility condition $q_1 \mid q_2 \mid \cdots \mid q_t$. We obtain a decomposition $E = E_1 \oplus \cdots \oplus E_t$ into φ-cyclic subspaces with invariant factors $q_1 \mid q_2 \mid \cdots \mid q_t$, and $q_t = q_\varphi$. Use the Chinese remainder theorem for part (b). □

Proposition 5.6.3. Let $T : F \to F$ be a linear transformation. Then F is a cyclic T-module if and only if $q_T = c_T$.

Proof. Suppose first that (F, T) is cyclic. By the Cayley–Hamilton theorem, $q_T \mid c_T$. Let $d_1 = \deg(q_T)$ and $d_1 = \deg c_T$. Show that $F = \text{span}\{T^n(v) \mid n \in \mathbb{Z}_{\geq 0}\}$, is generated as a k - v.s. by $v, T(v), \ldots, T^{d_1-1}(v)$, hence

$$d_1 = \dim_k E = \deg c_T(x) = d_2$$

hence considering that C_T is monic, we are done. Conversely, suppose that $q_T = c_T$. Consider the invariant factor decomposition

$$E = E_1 \oplus \cdots \oplus E_t,$$

where each E_i is cyclic with minimal polynomial q_i, and $q_1 \mid q_2 \mid \cdots \mid q_t$. The minimal polynomial of T is $q_t = q_T$. Moreover, $\dim(E_i) = \deg(q_i)$, since each E_i is cyclic and its characteristic polynomial equals its minimal polynomial. Hence

$$\dim(E) = \deg(q_1) + \cdots + \deg(q_t).$$

Since $q_T = c_T$, we get $\deg(q_t) = \deg(c_T) = \dim(E)$. Therefore

$$\deg(q_1) + \cdots + \deg(q_t) = \deg(q_t),$$

which implies $t = 1$, and in particular E itself is cyclic. □

Proposition 5.6.4. Suppose $T : E \to E$ has invariant factors $q_1, \ldots, q_t$. Then $c_T = q_1 \cdots q_t$.

Proof. By the invariant factor decomposition, $E = E_1 \oplus \cdots \oplus E_t$, where each E_i is cyclic with minimal polynomial q_i. Choose a basis $\mathscr{V}_i = (v_{i1}, \ldots, v_{in_i})$ for each E_i, and concatenate them into a basis

$$\mathscr{V} = (v_{11}, \ldots, v_{1n_1}, v_{21}, \ldots, v_{2n_2}, \ldots, v_{t1}, \ldots, v_{tn_t})$$

for E. If A_i is the matrix representing $T_{|E_i}$ with respect to $\mathscr{V}_i$, then the matrix of T with respect to $\mathscr{V}$ is block diagonal:

$$A = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_t \end{pmatrix}.$$

Therefore, $c_T(x) = \det(x\mathrm{I} - A)$. Since $xI - A$ is block diagonal,

$$c_T(x) = \det(xI - A_1) \cdots \det(xI - A_t).$$

But each E_i is cyclic, so $c_{T|_{E_i}}(x) = q_i(x)$. Hence $c_T = q_1 \cdots q_t$. □

Corollary 5.6.1. The roots of the minimal polynomial q_T are precisely the eigenvalues of T.

Proof. The eigenvalues of T are the roots of the characteristic polynomial c_T. From the previous proposition, $c_T = q_1 \cdots q_t$, where $q_1 \mid q_2 \mid \cdots \mid q_t = q_T$. Thus, every root of c_T is a root of q_T. Conversely, since $q_T \mid c_T$, every root of q_T is a root of c_T. Therefore the two sets of roots coincide. □

Theorem 5.6.2. The operator $T : E \to E$ is diagonalizable if and only if the minimal polynomial q_T splits as a product of distinct linear factors.

Proof. Suppose first that T is diagonalizable. Then $E = E_1 \oplus \cdots \oplus E_n$, where each $E_i = \langle v_i \rangle$ is one-dimensional and $Tv_i = \lambda_i v_i$. The minimal polynomial of $T_{|E_i}$ is $x - \lambda_i$. Hence, as a $k[x]$-module,

$$E \cong \frac{k[x]}{(x-\lambda_1)} \oplus \cdots \oplus \frac{k[x]}{(x-\lambda_n)}.$$

The minimal polynomial of T is therefore $q_T = (x-\lambda_1)\cdots(x-\lambda_c)$, where $\lambda_1, \ldots, \lambda_c$ are the distinct eigenvalues of T. Thus q_T splits into distinct linear factors. Conversely, suppose

$$q_T = (x-\lambda_1)\cdots(x-\lambda_c),$$

with distinct λ_i. Every invariant factor divides q_T, hence each invariant factor is also a product of distinct linear factors: $q_i = (x-\lambda_{i_1})\cdots(x-\lambda_{i_{r_i}})$. By the Chinese remainder theorem,

$$\frac{k[x]}{\langle q_i \rangle} \cong \frac{k[x]}{\langle x-\lambda_{i_1} \rangle} \oplus \cdots \oplus \frac{k[x]}{\langle x-\lambda_{i_{r_i}} \rangle}.$$

Therefore E decomposes as a direct sum of one-dimensional invariant subspaces. Hence T is diagonalizable. □

Example 5.6.6. Suppose $T^n = I$. Then the minimal polynomial q_T divides $x^n - 1$. If $k = \mathbb{C}$, then $x^n - 1$ has distinct roots. Hence q_T also has distinct roots, so T is diagonalizable.

Corollary 5.6.2. Let V be a complex representation of a finite group G. Then for every $g \in G$, the matrix representing g in $\mathrm{GL}(V)$ is diagonalizable.

Proof. Problem 5.10. □

5.7 Canonical Forms and Companion Matrices

Theorem 5.7.1. Let $T : E \to E$ be a linear transformation such that (E, T) is cyclic with cyclic vector v. Suppose the minimal polynomial of T is

$$q_T(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Then $\{v, Tv, T^2v, \ldots, T^{n-1}v\}$ is a basis for E. Moreover, with respect to this basis, the matrix of T is

$$A_T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}.$$

This matrix is called the **companion matrix** of q_T.

Proof. Problem 5.7.1. □

Corollary 5.7.1. Suppose (E, T) is cyclic with minimal polynomial $(x-\lambda)^n$. Then there exists a basis of E in which T is represented by the matrix

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \lambda \end{pmatrix}.$$

This matrix is called a **Jordan block**.

Proof. Let $\varphi = \psi - bI_E$. Then $\psi = \varphi + bI_E$. We first observe that $q_\psi(x) = (x-b)^r$ is the minimal polynomial of ψ if and only if $q_\varphi(x) = x^r$ is the minimal polynomial of φ. Notice also that E is φ - cyclic if and only if ψ - cyclic. By Theorem 4.3, E is φ-cyclic with minimal polynomial x^r if and only if $\dim_K E = r$ and there is an ordered basis

$$\mathscr{B} = \{v, \varphi(v), \ldots, \varphi^{r-1}(v)\}$$

relative to which the matrix of φ is the companion matrix of x^r, namely

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Since $\psi = \varphi + bI_E$, the matrix of ψ relative to the same basis is $B = A + bI_r$. Therefore

$$B = \begin{pmatrix} b & 1 & 0 & \cdots & 0 \\ 0 & b & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & b \end{pmatrix}.$$

Conversely, suppose that $\dim_K E = r$ and that the matrix of ψ relative to some ordered basis is

$$B = \begin{pmatrix} b & 1 & 0 & \cdots & 0 \\ 0 & b & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & b \end{pmatrix}.$$

Then the matrix of $\varphi = \psi - bI_E$ relative to the same basis is

$$A = B - bI_r = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

By Theorem 4.3, E is φ-cyclic and the minimal polynomial of φ is x^r. Therefore E is also ψ-cyclic, and the minimal polynomial of ψ is $(x-b)^r$. This proves the corollary. □

Remark 5.7.1. The matrix above is not the companion matrix of $(x-\lambda)^n$, but it is similar to it.

Remark 5.7.2.

i. The **rational canonical form** is obtained by using companion matrices coming from the invariant factor decomposition of T. This construction is independent of the field.

ii. The **primary canonical form** is obtained by using companion matrices coming from the elementary divisor decomposition. This depends on the field.

iii. If the field k is algebraically closed, the elementary divisors are powers of linear factors, and the corresponding companion matrices become Jordan blocks. This gives the **Jordan canonical form**.

5.8 Simultaneous Diagonalization

Remark 5.8.1. The fact that A, B are diagonalizable does not imply that AB is diagonalizable. For example, consider

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1/2 \end{pmatrix}, \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Both A and B are diagonalizable, but $AB = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, which is not diagonalizable.

Proposition 5.8.1. Let $A, B \in M_n(k)$, where $\overline{k} = k$, and assume that $AB = BA$. Then A and B have a common eigenvector.

Proof. Let v be an eigenvector of A with eigenvalue λ, i.e. $Av = \lambda v$. Consider

$$F = \text{span}\{v, Bv, \ldots, B^{n-1}v\}.$$

Clearly F is B-invariant. Moreover, for every $\ell \geq 0$,

$$AB^\ell v = B^\ell Av = B^\ell(\lambda v) = \lambda B^\ell v.$$

Hence each $B^\ell v$ is also an eigenvector of A with eigenvalue λ. Therefore $F \subseteq E_\lambda(A)$, where $E_\lambda(A)$ denotes the λ-eigenspace of A. Since $\overline{k} = k$, the operator $B|_F$ has an eigenvector $w \in F$, so $Bw = \mu w$, for some $\mu \in k$. Because $w \in F \subseteq E_\lambda(A)$, we also have $Aw = \lambda w$. Thus w is a common eigenvector of A and B. □

Theorem 5.8.1. Let $A, B \in M_n(k)$ be diagonalizable matrices such that $AB = BA$. Then there exists a basis of k^n consisting of simultaneous eigenvectors of A and B. Equivalently, there exists an invertible matrix P such that

$$PAP^{-1} \quad \text{and} \quad PBP^{-1} \quad \text{are both diagonal.}$$

Proof. Since A is diagonalizable, if $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of A, then

$$k^n = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k},$$

where E_{λ_i} denotes the eigenspace corresponding to λ_i. Now let $v \in E_{\lambda_i}$. Then $Av = \lambda_i v$. Using the commutativity assumption,

$$A(Bv) = B(Av) = B(\lambda_i v) = \lambda_i Bv.$$

Hence $Bv \in E_{\lambda_i}$. Therefore each eigenspace E_{λ_i} is B-invariant. Since B is diagonalizable, the restriction $B|_{E_{\lambda_i}}$ is also diagonalizable. Hence, for each i we may choose a basis $\mathscr{V}_i = \{v_{i1}, \ldots, v_{in_i}\}$ of E_{λ_i} consisting of eigenvectors of B. But every vector in E_{λ_i} is automatically an eigenvector of A with eigenvalue λ_i. Therefore each v_{ij} is simultaneously an eigenvector of A and B. Collecting all these bases together gives a basis of k^n consisting of simultaneous eigenvectors of A and B. □

Corollary 5.8.1. If $A, B \in M_n(k)$ are diagonalizable and commute, then AB is diagonalizable. Moreover, $A + B$ is also diagonalizable.

Proof. By the theorem, there exists a basis $v_1, \ldots, v_n$ consisting of simultaneous eigenvectors of A and B. Suppose

$$Av_i = \lambda_i v_i, \quad \text{and} \quad Bv_i = \mu_i v_i.$$

Then

$$(AB)v_i = A(Bv_i) = A(\mu_i v_i) = \mu_i Av_i = \lambda_i \mu_i v_i.$$

Hence each v_i is an eigenvector of AB, so AB is diagonalizable. Similarly,

$$(A + B)v_i = Av_i + Bv_i = (\lambda_i + \mu_i)v_i,$$

so $A + B$ is diagonalizable as well. □

Remark 5.8.2. More generally, if A and B are commuting diagonalizable matrices, then every polynomial expression $f(A, B)$ is diagonalizable.

5.9 Problems

Problem 5.1. Let $f, g : E \to E$, $h : E \to F$, $k : F \to G$ be linear transformations of left vector spaces over a division ring D with $\dim_D E = n$, $\dim_D F = m$, $\dim_D G = p$.

a. $\text{rank}(f + g) \leq \text{rank}\, f + \text{rank}\, g$.

b. $\text{rank}(kh) \leq \min\{\text{rank}\, h, \text{rank}\, k\}$.

c. $\text{nullity}(kh) \leq \text{nullity}\, h + \text{nullity}\, k$.

d. $\text{rank}\, f + \text{rank}\, g - n \leq \text{rank}(fg) \leq \min\{\text{rank}\, f, \text{rank}\, g\}$.

e. $\max\{\text{nullity}\, g, \text{nullity}\, h\} \leq \text{nullity}(hg)$.

f. If $m \neq n$, then (e) is false for h and k.

Problem 5.2. Let R be a principal ideal domain. For each positive integer r and sequence of nonzero ideals

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_r,$$

choose a sequence $d_1, \ldots, d_r \in R$ such that $(d_i) = I_i$ and $d_1 \mid d_2 \mid \cdots \mid d_r$. For a given pair of positive integers (n, m), let S be the set of all $n \times m$ matrices of the form

$$\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix},$$

where $r = 1, 2, \ldots, \min(n, m)$ and L_r is an $r \times r$ diagonal matrix with main diagonal one of the chosen sequences $d_1, \ldots, d_r$.

Show that S is a set of canonical forms under equivalence for the set of all $n \times m$ matrices over R.

Problem 5.3. a. Show that if R is a commutative ring, A is and R-module and $R \to S$ is homomorphism of commutative rings then $A \otimes_R S$ is an S-module.

b. Prove that if F is a free R-module then $F \otimes_R S$ is a free S-module

c. Show that if R is an integral domain with fraction field K, then K is a flat R algebra. (Hint. You just need to show that if $A \to B$ is an injective homomorphism of R-modules then $A \otimes_R K \to B \otimes_R K$ is injective.)

d. Show that if $a_1, \ldots, a_t$ are linearly independent elements in A then $a_1 \otimes 1, \ldots, a_t \otimes 1$ are linearly independent elements in the vector space $A \otimes_R K$.

e. Prove that if $a_i i \in I$ is a maximal linearly independent set of elements then $a_i \otimes 1i \in I$ is a basis for the vector space $A \otimes_R K$ by showing that these elements form a maximal linearly independent subset. Conclude that all maximal linearly independent subsets of A have the same cardinality so the linear rank is well defined.

f. State and prove the rank nullity theorem for a map of finitely generated R-modules $A \to B$ when R is an integral domain.

Problem 5.4. (a) If $m > n$, then every alternating R-multilinear form on $(R^n)^m$ is zero.

(b) If $m \leq n$, then there exists a nonzero alternating R-multilinear form on $(R^n)^m$.

Problem 5.5. Let R be an integral domain and let $k = \text{Frac}(R)$. If $A : R^n \to R^m$ is an R-module homomorphism, we know that the rank of A is

$$\text{rank}(A) = \text{rank}(\text{im}(A)) = \dim_k (\text{im}(A) \otimes_R k)$$

a. Prove that tensoring the exact sequence

$$R^n \xrightarrow{A} R^m \to \frac{R^m}{\text{im}(A)} \to 0$$

with k yields an exact sequence

$$R^n \otimes_R k \xrightarrow{A \otimes k} R^m \otimes_R k \to \frac{R^m}{\text{im}(A)} \otimes_R k \to 0.$$

b. Deduce that

$$\text{im}(A \otimes k) \cong (\text{im}\, A) \otimes_R k.$$

c. Show that $\text{rank}(A) = \text{rank}_k(A \otimes k)$, where the right-hand side denotes the ordinary rank of the induced K-linear map

$$A \otimes k : R^n \otimes_R k \to R^m \otimes_R k.$$

d. Suppose that $B = PAQ$, where $P \in GL_m(R)$, and $Q \in GL_n(R)$. Prove that $\text{rank}(A) = \text{rank}(B)$.

Problem 5.6. Find all possible primary rational canonical forms for a matrix $A \in \text{Mat}_n(\mathbb{Q})$ such that:

(i) A is 6×6 with minimal polynomial $(x-2)^2(x+3)$;

(ii) A is 7×7 with minimal polynomial $(x^2+1)(x-7)$.

Find all possible Jordan canonical forms of A considered as a matrix over $\mathbb{C}$.

Problem 5.7. A matrix $A \in \mathrm{Mat}_n(K)$ is called idempotent if $A^2 = A$. Show that two idempotent matrices in $\mathrm{Mat}_n(K)$ are similar if and only if they are equivalent.

Problem 5.8. (a) Exhibit three 3×3 matrices over $\mathbb{Q}$, no two of which are similar, such that -2 is the only eigenvalue of each of the matrices.

(b) Exhibit a 4×4 matrix whose eigenvalues over $\mathbb{R}$ are ± 1 and whose eigenvalues over $\mathbb{C}$ are ± 1 and $\pm i$.

Problem 5.9. Let k be a field and $A \in \mathrm{Mat}_n(k)$.

(a) If A is nilpotent (that is, $A^m = 0$ for some m), then $\mathrm{Tr}(A^r) = 0$ for all $r \geq 1$.

[Hint: the minimal polynomial of A^r has the form x^t and A^r is similar to a matrix in rational Jordan canonical form.]

(b) If $\mathrm{char}\, K = 0$ and $\mathrm{Tr}(A^r) = 0$ for all $r \geq 1$, then A is nilpotent.

Problem 5.10. Prove Corollary 5.6.2.

Problem 5.11. Prove directly that if there is an R-module isomorphism $R^m \cong R^n$, then $m = n$.

Problem 5.12. Prove Theorem 5.7.1.

Problem 5.13. If R is a field and $A, B \in \mathrm{Mat}_n(R)$ are invertible, then the matrix $A + rB$ is invertible for all but finitely many $r \in R$.

Problem 5.14. Let F be an extension field of K. The invariant factors in $K[x]$ of a matrix $A \in \mathrm{Mat}_n(K)$ are the same as the invariant factors in $F[x]$ of A considered as a matrix over F.

Hint: A K-basis of K^n is an F-basis of F^n. Use linear transformations.

Problem 5.15. Let K be a field and $A \in \mathrm{Mat}_n(K)$.

(a) 0 is an eigenvalue of A if and only if A is not invertible.

(b) If $k_1, \ldots, k_r \in K$ are the (not necessarily distinct) eigenvalues of A and $f \in K[x]$, then $f(A) \in \mathrm{Mat}_n(K)$ has eigenvalues $f(k_1), \ldots, f(k_r)$.

Problem 5.16. If φ and ψ are endomorphisms of a finite-dimensional vector space over an algebraically closed field K such that $\varphi\psi = \psi\varphi$, then φ and ψ have a common eigenvector.

Index