MAT1100

Algebra I

Course Notes

Contents

Chapter 1

Group Theory

1.1 Introduction

There are many different algebraic structures one may consider, of which the simplest most natural one is a group, defined below.

Definition 1.1.1. A *binary operator* $*$ on a set S is a map $* : S \times S \to S$ denoted by $(a, b) \mapsto a * b$. A *group* is a set G with a binary operator $(g, h) \mapsto gh$ and a distinguished element $e \in G$ called the *identity* such that the binary operator satisfies

1. Associativity: For every $g, h, k \in G$ it follows that $(gh)k = g(hk)$. This is the associativity property.
2. Identity: For every $g \in G, ge = eg = g$. This simply states that e acts as identity under the binary operator.
3. Inverse: For every $g \in G$ there exists a unique $h \in G$ such that $gh = hg = e$. We often denote $g^{-1} = h$.

By removing some of the above properties, we may derive different algebraic structures, although none of these are as useful as groups. The chart below describes which properties are associated to which algebraic structures:

	Associativity	Identity	Inverse
Group	Yes	Yes	Yes
Monoid	Yes	Yes	No
Semigroup	Yes	No	No
Loop	No	Yes	No
Magma	No	No	No

With these fundamental axioms, we can immediately recognize a few simple results concerning the uniqueness of the identity and inverse elements.

Proposition 1.1.2. *Let $(G, *, e)$ be a group, $a, b, c \in G$. Then*

1. *The identity element e is unique.*
2. *The inverse of an element is uniquely determined.*
3. *$(ab)^{-1} = b^{-1}a^{-1}$*
4. *If $ac = bc$ then $a = b$. This is known as the cancellation property.*

Proof. 1. Assume that e, f are both identity elements, so that

$$e = e \cdot f = f \tag{1.1}$$

and so the identity element is unique.

2. Fix $g \in G$ and let $h, h' \in G$ be such that $hg = h'g = e$. Then

$$h' = h'(gh) = (h'g)h = h \tag{1.2}$$

so the inverse is unique.

3. Let $a, b \in G$. By definition, we have that $(ab)^{-1}(ab) = e$. We proceed by multiplying on the right by b^{-1} then a^{-1} to find that

$$\begin{aligned}(ab)^{-1}(ab)b^{-1}a^{-1} &= eb^{-1}a^{-1}\\ (ab)^{-1} &= b^{-1}a^{-1}\end{aligned}$$

which was the desired result.

4. Let $a, b, c \in G$ be such that $ac = bc$. We can simply apply c^{-1} to both sides to find that $acc^{-1} = bcc^{-1}$ which yields $a = b$.

□

Definition 1.1.3. Let G be a group. If for every $a, b \in G$ we have that $ab = ba$ we say that G is *abelian*.

Examples:

1. It is easy to see that $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \times)$, and $(\mathbb{Z}, +)$ are abelian groups.

2. Consider $(\mathbb{Z}/n, +)$ and $((\mathbb{Z}/p) \setminus \{0\}, \times)$ for a prime p. Again, these are both abelian groups.

3. Let X be a topological space. Then the fundamental group $\pi_1(X)$ is a group.

4. Let $GL(n, F)$ denote the set of $n \times n$ invertible matrices with elements in F. This is a group, and is isomorphic to the automorphism group of the vector space F^n.

5. Denote by S_n the *symmetric group on n letters*. This is the set of automorphisms on the set $\{1, \ldots, n\}$. More specifically,

$$S_n = \left(\left\{ \sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \;\middle|\; \sigma \text{ is invertible} \right\}, \circ \right) \tag{1.3}$$

   For a more concrete example, let us consider S_3, and consider $\sigma \in S_3$ as the permutation acting as

$$\sigma(1) = 2, \quad \sigma(2) = 3, \quad \sigma(3) = 1 \tag{1.4}$$

   Using cycle notation, we can denote this as (123). Let $\tau \in S_3$ be similarly given by (23). Then

$$\sigma\tau = (123)(23) = (12) \tag{1.5}$$

   and $|S_3| = 6$. Indeed for general S_n we have that $|S_n| = n!$.

1.1.1 Subgroups

Definition 1.1.4. Let G be a group. Then $H \subset G$ is a *subgroup* of G if it is a group under the restriction of the binary operator with the same identity element. We denote this by $H \leq G$.

Proposition 1.1.5 (One Step Subgroup Test)**.** *Let G be a group. Then $H \subseteq G$ is a subgroup if and only $\forall a, b \in G$ we have that $ab^{-1} \in H$.*

Proof. Assume that $H \leq G$. Then by definition both a and $b^{-1} \in H$ and so by closure, $ab^{-1} \in H$. Conversely, assume that $\forall a, b \in H$ we have that $ab^{-1} \in H$. Let $g, h \in H$. Then since $e \in H$ we know that $eh^{-1} \in H$ so $h^{-1} \in H$, thus H is a subgroup. □

Definition 1.1.6. Let G be a group, and $S \subset G$. Then $\langle S \rangle$ denotes the smallest subgroup of G containing S.

Proposition 1.1.7. *Let G be a group and $S \subset G$. Then*

$$\langle S \rangle = \bigcap_{S \subset H \leq G} H \tag{1.6}$$

Proof. Clearly S is a subset for each group containing it, and so $\langle S \rangle \subseteq H$ for every H by closure of the binary operator. This gives us the inclusion

$$\langle S \rangle \subseteq \bigcap_{S \subseteq H \leq G} H. \tag{1.7}$$

This is also clearly the smallest subgroup containing S, since any smaller subgroup would be be a member of this intersection. □

1.1.2 Order

Definition 1.1.8. Let G be a group and $g \in G$ be an arbitrary element. We define the *order* of g as

$$|g| = \min \{n \in \mathbb{N} : g^n = e_G\}. \tag{1.8}$$

In the event that no such n exists, we say that g has infinite order and denote this as $|g| = \infty$.

Lemma 1.1.9. *The following are some important and easily verifiable facts that we will use in our proof.*

1. *If $g \in G$ not identity and $g^n = e$ then $|g| \,\Big|\, n$.*
2. *If $g \in G$ is an element of finite order and $m \in \mathbb{N}$ then*
$$|g^m| = \frac{|g|}{\gcd(m, |g|)} = \frac{\operatorname{lcm}(m, |g|)}{m}. \tag{1.9}$$
3. *For every $g, h \in G$ we have that $(h^{-1}gh)^n = h^{-1}g^n h$.*
4. *For every $g, h \in G$ we have that $|g| = |h^{-1}gh|$. That is, conjugation preserves order.*

Proof. 1. Assume that $g \in G$ and that $g^n = e$. Since g is not identity, we know that $n > 1$. Since n is an integer, we know $\exists q, r \in \mathbb{Z}$ such that $n = q|g| + r$ where $0 \leq r < |g|$. But then
$$g^n = g^{|g|q+r} = (g^{|g|})^q g^r = g^r = e. \tag{1.10}$$
This implies that $g^r = e$. However, since $|g|$ is the minimal such integer and $r < |g|$ we conclude that $r = 0$. Thus $n = |g|q$, so $|g| \,\Big|\, n$ as required.

2. Note that $g^{m|g^m|} = e$ and so it follows that $|g| \,\Big|\, m|g^m|$. By since $|g^m|$ is the minimal amongst powers that send g^m to e it must follow that $|g^m|$ is the least multiple of m which is almost a mulitple of $|g|$. This implies that
$$m|g^m| = \operatorname{lcm}(m, |g|). \tag{1.11}$$
and the result now follows by dividing by m and realizing that
$$\gcd(m, |g|) \operatorname{lcm}(m, |g|) = m|g|. \tag{1.12}$$

3. Let $g, h \in G$. We will proceed by induction. Clearly $(h^{-1}gh)^1 = h^{-1}g^1h$ so the base case is satisfied. Assume then that $(h^{-1}gh)^k = h^{-1}g^k h$. Now
$$\begin{aligned}(h^{-1}gh)^{k+1} &= (h^{-1}gh)^k(h^{-1}gh) \\ &= (h^{-1}g^k h)(h^{-1}gh) && \text{by induction hypothesis} \\ &= h^{-1}g^k gh = h^{-1}g^{k+1}h\end{aligned}$$
and so $(h^{-1}gh)^{k+1} = h^{-1}g^{k+1}h$ as we required and the result follows.

4. To show that $|g| = |h^{-1}gh|$ we will show that the numbers divide one another. Indeed, note that
$$(h^{-1}gh)^{|g|} = h^{-1}g^{|g|}h = h^{-1}h = e$$
and so by Property 1 we know that $|h^{-1}gh| \,\Big|\, |g|$. Conversely, we know that
$$(h^{-1}gh)^{|h^{-1}gh|} = e \tag{1.13}$$
so
$$\begin{aligned} (h^{-1}gh)^{|h^{-1}gh|} &= e \\ h^{-1}g^{|h^{-1}gh|}h &= e && \text{by Property 2} \\ g^{|h^{-1}gh|} &= hh^{-1} && \text{by multiplying by } h \text{ and } h^{-1} \\ g^{|h^{-1}gh|} &= e \end{aligned}$$
and so we conclude that $|g| \,\Big|\, |h^{-1}gh|$. Both divisibility criteria imply that $|g| = |h^{-1}gh|$ as required.

□

Definition 1.1.10. Let G be a group. The *order* of G, denoted $|G|$, is the cardinality of the underlying set. If G is an infinite group we write $|G| = \infty$.

The choice of notation for denoting the order of a group and the order of an element should be clear in the context of the discussion. Moreover, they are related in that if $g \in G$ then $|\langle g \rangle| = |g|$. If $|g| = \infty$ this is obvious, so consider the case when g has finite order. Enumerate the elements of $\langle g \rangle$ as
$$\langle g \rangle = \left\{ e_G, g, g^2, \ldots, g^{|g|-1} \right\}. \tag{1.14}$$
Clearly after the $|g|^{th}$ power this cycle will repeat, and so $|\langle g \rangle| \leq |g|$. On the other hand, if there are two elements g^k and g^ℓ such that $k < \ell < |g|$ but $g^k = g^\ell$ then we can multiply by $g^{k^{-1}}$ to get that $g^{\ell-k} = e_G$. However, this is a contradiction to the minimality of $|g|$ and so all the elements enumerated above are distinct. This tells us that $|\langle g \rangle| = |g|$ as expected.

1.1.3 Group Homomorphisms

Definition 1.1.11. If G, H are groups, a mapping $\phi : G \to H$ is a *group homomorphism* if $\phi(gg') = \phi(g)\phi(g')$ for all $g, g' \in G$.

Proposition 1.1.12. *If $\phi : G \to H$ is a group homomorphism then*

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = \phi(g)^{-1}$ *for all* $g \in G$.

Proof. Let ϕ be the given homomorphism.

1. Notice that
$$\phi(e_G)\phi(e_G) = \phi(e_G^2) = \phi(e_G). \tag{1.15}$$
By applying the cancellation property in H we get that $\phi(e_G) = e_H$ as required.
2. Fix $g \in G$ and notice that
$$e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \tag{1.16}$$
and so $\phi(g^{-1}) = \phi(g)^{-1}$ as required.

□

Definition 1.1.13. Let $\phi : G \to H$ be a group homomorphism. We define
$$\ker \phi = \left\{ g \in G \;\middle|\; \phi(g) = e_G \right\} = \phi^{-1}(e). \tag{1.17}$$
Similarly, the image of ϕ is
$$\operatorname{im} \phi = \{\phi(g) : g \in G\}. \tag{1.18}$$

As bijections between set mappings give us a way of identifying when two sets are the same, we have the concept of a group isomorphism defined below. As the etymology of isomorphism might suggest, these maps give us a way of determining when two groups which otherwise look disimilar, are actually the same.

Definition 1.1.14. Let G and H be groups and $\phi : G \to H$ a map. We say that ϕ is a *group isomorphism* if ϕ is a bijective group homomorphism. We say that G and H are *isomorphic* and write $G \cong H$ if there is an isomorphism between them.

Proposition 1.1.15. *If $\phi : G \to H$ and $\psi : H \to K$ are group isomorphisms then $\phi^{-1} : H \to G$ and $\psi \circ \phi : G \to K$ are both group isomorphisms.*

Proof. Since ϕ is bijective, ϕ^{-1} is also bijective, so all we need to show is that ϕ^{-1} is a group homomorphism. Indeed, let $h, h' \in H$ and choose $g, g' \in G$ such that $\phi(g) = h$ and $\phi(h) = h'$ which can be done since ϕ is injective. Now $\phi(gg') = \phi(g)\phi(g') = hh'$ and so

$$\phi^{-1}(hh') = gg' = \phi^{-1}(h)\phi^{-1}(h'). \tag{1.19}$$

□

Proposition 1.1.16. *If $\phi : G \to H$ and $g \in G$ is an element of finite order then $|\phi(g)| \,\Big|\, |g|$ with equality if ϕ is an isomorphism.*

Proof. Notice that

$$e_H = \phi(e_G) = \phi\left(g^{|g|}\right) = \phi(g)^{|g|} \tag{1.20}$$

and so by Lemma 1.1.9 it must follow that $|\phi(g)| \,\Big|\, |g|$. For equality assume that ϕ is an isomorphism and note that by Proposition 1.1.15 that ϕ^{-1} is also an isomorphism. It must follow that $|g| \,\Big|\, |\phi(g)|$ and both divisibility propeties give equality. □

Application: Non-Commutative Gaussian Elimination

Let $G = \langle g_1, \ldots, g_\alpha \rangle$. Define the pivot of $\sigma \in S_n$ to be the minimal $k \in \mathbb{N}$ such that $\sigma(k) \neq k$. Prepare a mostly empty table:

$(1,1)$ I				
$(1,2)$	$(2,2)$ I			
$(1,3)$	$(2,3)$	$(3,3)$ I		
$\vdots$	$\vdots$	$\vdots$	$\ddots$	
$(1,n)$	$(2,n)$	$(3,n)$	$\cdots$	(n,n) I

Feed $g_1, \ldots, g_n$ in order. To feed a non-identity σ, find its pivotal position i and let $j = \sigma(i)$.

1. If box (i, j) is empty, put σ in this box.
2. If box (i, j) is not-empty, feed $\sigma' = \sigma_{i,j}^{-1}\sigma$ into the table.

After this procedure is completed, for each occupied box (i, j) and (k, ℓ) feed the product $\sigma_{i,j}\sigma_{k,\ell}$ into the table. Repeat this until the table stops changing. Notice that in the refeed process, the element $\sigma' = \sigma_{i,j}^{-1}\sigma$ has pivot strictly greater than σ. Indeed, notice that

$$\sigma'(i) = \sigma_{i,j}^{-1}\sigma(i) = \sigma_{i,j}^{-1}(j) = i \tag{1.21}$$

and so the pivot has increased.

Claim: The process stops in a finite time, after at most $O(n^6)$ operations. Call the resulting table T.

We first realize that the operation must stabilize. Indeed, after an element is put into the table, it is never altered. Since the number of positions is finite, the table must eventually stop changing. Let us try to analyze the complexity of this algorithm. Feeding σ takes at most n attempts, each one takes n operations resulting in n^2 operations. Now on further iterations, we only need to feed results for pairs of boxes. This corresponds to n^4 elements, for which it again takes $O(n^2)$ operations. Hence the total amount of work done is $O(n^2+n^4n^2) = O(n^6)$.

Claim: Every $\sigma_{i,j}$ in T is in G.

Since every element in the table is derived from closed operations on the operators, it must follow that every element in the table is also in the group.

Claim: Anything fed into T is a monotone product of elements in T. By monotone, we mean of the form $\sigma_{1,j_1}\sigma_{2,j_2}\cdots\sigma_{n,j_n}$ for $j_i \geq i$.

Let σ be an non-identity element with pivot i and let $j = \sigma(i)$. We have two cases: In the first, assume that (i, j) is empty. Then $\sigma = \sigma_{i,j}$. In the second case, assume (i, j) is not empty. Feed $\sigma' = \sigma_{i,j}^{-1}\sigma$, and so $\sigma = \sigma_{i,j}\sigma'$. By induction, it follows that σ' is already a monotone product with elements of index less than i. With the first case as the base example, we are done.

Claim: If $\sigma_{1,j_1}\sigma_{2,j_2}\cdots\sigma_{n,j_n} = \sigma_{1,j_1'}\sigma_{2,j_2'}\cdots\sigma_{n,j_m'}$ then $m = n$ and $j_k = j_k'$ for all k.

Consider the action of each side on the element 1. Then

$$j_1 = (lhs)(1) = (rhs)(1) = j_1' \tag{1.22}$$

so $\sigma_{1,j_1} = \sigma_{1,j_1'}$ and we can cancel these elements on each side. Inductively, we can do the same thing by considering the action of the reduced element on the element $2, \cdots, n$. Hence $\forall i, j_i = j_i'$.

Claim: Let $M_k = \left\{\sigma_{k,j_k}\sigma_{k+1,j_{k+1}}\cdots\sigma_{n,j_n}\right\}$. Then $\forall k, M_k \cdot M_k \subset M_k$. Hence $M_k \leq G$.

Let us proceed by using backwards induction. We first note that $M_n \cdot M_n \subset M_n$ since the only element in M_n is $\sigma_{n,n} = \mathrm{id}$ and $\mathrm{id}\cdot\mathrm{id} = \mathrm{id}$. Now assume that we know $M_{k+1}\cdot M_{k+1} \subset M_{k+1}$, and we proceed on M_k. Let us start with a single non-trivial element in M_k, say $\sigma_{\ell,j}$ with $k < \ell < j$, then we want to show that $\sigma_{\ell,j}M_k \subset M_k$. Indeed, any element of M_k is of the form $\sigma_{k,j_k}M_{k+1}$ and so $\sigma_{\ell,j}\sigma_{k,j_k} = (\sigma_{\ell,j}\sigma_{k,j_k})M_{k+1}$. We notice that this product is then fed into the table, and by previous claim, anything fed into the table is a monotone product. Furthermore, it must be a monotone product with pivot k and so we can rewrite this as

$$(\sigma_{\ell,j}\sigma_{k,j_k})M_{k+1} = (\sigma_{k,j'_k}\underbrace{\sigma_{k+1,j'_{k+1}}\cdots}_{\in M_{k+1}})M_{k+1} \subseteq \sigma_{k,j_k}M_{k+1}M_{k+1} \subseteq \sigma_{k,j'_k}M_{k+1} \subseteq M_k. \tag{1.23}$$

This is what we wanted to show.

More generally, consider the element $(\sigma_{k,j_k}\sigma_{k+1,j'_{k+1}}\cdots) \in M_k$ and multiply it by M_k. We again use backwards induction in a similar manner to before to prove the desired result.

Claim: $M_1 = G$.

Clearly, $M_1 \subseteq G$. Since every element we feed into the table is a monotone product, every element in table is in M_1. More precisely, $g_1, \ldots, g_n \in M_1$. Since G is the minimal group containing all generators, we get that $G \subseteq M_1$. Both inclusions imply that $M_1 = G$ as required.

Example: Consider the permutations $\sigma_1 = (123)$ and $\sigma_2 = (12)(34)$ in S_4. We want to calclulate the size of the subgroup generated by these two elements. We start with a nearly empty table

I			
$(1,2)$	I		
$(1,1)$	$(2,3)$	I	
$(1,4)$	$(2,4)$	$(3,4)$	I

and feed σ_1.

1. σ_1 has pivot in the 1st position, and maps $1 \mapsto 2$. Hence we place σ_1 into $(1,2)$, and we write $\sigma_{1,2} = \sigma_1$.

2. To be efficient, we shall now compute all the products of $\sigma_{1,2}$ and feed them into the table. In most cases, this is simply the identity. However, we also have the element $\sigma_{1,2}\sigma_{1,2} = [3124] = (132)$. Here the pivot is 1 and $1 \mapsto 3$, so $\sigma_{1,3} = \sigma_{1,2}^2$.

3. Since again we have fed a new element, we feed in its product. This is beginning to get messy, so we may use code.

```
Unprotect[And];
 p1_Integer && p2_Integer := Module[
 [s1,s2]
 s1 =IntegerDigits[Abs[p1]];
 If[p1<0,s1=Ordering[s1]];
 s2 = IntegerDigits[Abs[p2]];
 If[p2<0, s2 = Ordering[s2]];
 FromDigits[s1[[s2]]];
 ];
 Protect[And];
```

We can compute $\sigma_{1,3}\sigma_{1,2} = (1)$ so we drop it. Similarily $\sigma_{1,3}\sigma_{1,3} = (123) = \sigma$. However, the corresponding position $(1, 2)$ is occupied, hence we feed in $\sigma_{1,2}^{-1}\sigma = (1)$ so we drop it.

4. Now we feed the second generator, σ_2. It has pivot 1 and $1 \mapsto 2$ so we need to feed $\sigma_{1,2}^{-1}\sigma_2 = [1342] = (234)$ which has pivot 2 and $2 \mapsto 3$. Hence we set $\sigma_{2,3} = (234)$.

We can continue in this fashion to get

I			
2314 σ_1	I		
3124 $\sigma_{1,2}^2$	1324 $\sigma_{1,2}^{-1}\sigma_2$	I	
4132	1423 $\sigma_{1,3}^{-1}\sigma_{2,3}\sigma_{1,2}$	$\emptyset$	I

Thus $|G| = 12$. Is $[4123] \in G$? We feed $\sigma_{1,4}^{-1}[4123] = [1243]$ which has pivot 3 and maps $3 \mapsto 4$. Since we would be adding it to the group, it would make the group larger, so [4123] is not in the group.

Exercise: Write [2431] in terms of σ_1, σ_2.

1.1.4 Normal Groups

If A and B are subsets of G, denote by their product as

$$AB = \left\{ ab \;\middle|\; a \in A, b \in B \right\} \subseteq G \tag{1.24}$$

In the special case when H is a subset of G, and $g \in G$ is a singleton, we define the *left-coset of H in g* as the set gH and the *right-coset of H in g* as Hg.

Definition 1.1.17. A subgroup $N \leq G$ is called normal if $\forall g \in G, gN = Ng$.

Definition 1.1.18. Let G be a group and $X \subseteq G$. Define

$$C_G(X) = \left\{ g \in G \,\middle|\, gxg^{-1} = x, \forall x \in X \right\} \tag{1.25}$$

called the *centralizer* of X in G. As a special case, we have the centre of G denoted $Z(G) = C_G(G)$. Define

$$N_G(X) = \left\{ g \in G \,\middle|\, gXg^{-1} = X \right\} \tag{1.26}$$

called the *normalizer*.

Theorem 1.1.19. *Let N be a subgroup of G. Then the following are equivalent*

1. $N \triangleleft G$
2. $N_g(N) = G$.
3. $gN = Ng$ *for all* $g \in G$.
4. *The set of cosets* $\{gN : g \in G\}$ *is a group.*
5. $gNg^{-1} \subseteq N$ *for all* $g \in G$.

Proof. **Need to fill this in.** Assume that $N \triangleleft G$ is normal. Let $x \in N$ and fix $g \in G$. Now $gN = Ng$ by assumption, so $\exists y \in N$ such that $gx = yg$. Multiplying both sides by g^{-1} to get $y = gxg^{-1} \in N$. The converse follows similarly. □

For $x, g \in G$ denote by x^g the conjugation of x by g. It is important to note that there are two interpretations to what this could be. Either $x^g = gxg^{-1}$ or $x^g = g^{-1}xg$, and one must be careful to check which definition is being used at any given time.

Definition 1.1.20. If G is a group and $g \in G$, we can ascertain a derived automorphism of G called an *inner-automorphism* by defining the map

$$\gamma_g : G \to G, x \mapsto gxg^{-1}. \tag{1.27}$$

It is easy to see that inner automorphisms are indeed isomorphisms from G to itself. For a fixed $g \in G$ we have

$$\gamma_g(x)\gamma_g(y) = (gxg^{-1})(gyg^{-1}) = gxyg^{-1} = \gamma_g(xy). \tag{1.28}$$

If G is a group, consider the set $\operatorname{Aut} G$ of automorphisms of G, and this forms a group under composition. By defining the map $f : G \to \operatorname{Aut} G, g \mapsto \phi^g$ then this is either a group homomorphism (under gxg^{-1}) or a group anti-homomorphism (under $g^{-1}xg$) depending on the choice of conjugation convention.

Theorem 1.1.21. *Let G be a group and denote the set of inner automorphisms of G as $\operatorname{Inn}(G)$. Then $\operatorname{Inn}(G) \triangleleft \operatorname{Aut}(G)$.*

Proof. Let $\phi \in \operatorname{Aut}(G)$ and $\varphi_g \in \operatorname{Inn}(G)$ given by $\varphi_g : x \to gxg^{-1}$. Now we want to consider the automorphism given by $\phi \circ \varphi_g \circ \phi^{-1}$ and show that this is an element of $\operatorname{Inn}(G)$. Indeed, we claim that $\phi \circ \varphi_g \circ \phi^{-1} = \varphi_{\phi(g)}$ where $\varphi_{\phi(g)}(x) = x^{\phi(g)}$. To see this, we note that an automorphism of G is determined entirely by its action on elements of G. Let $h \in G$ be arbitrary, and notice that

$$\begin{aligned}
\phi \circ \varphi_g \circ \phi^{-1}(g) &= \phi\left(\varphi_g\left(\phi^{-1}(h)\right)\right) \\
&= \phi\left(g\phi^{-1}(h)g^{-1}\right) && \text{by definition of inner automorphism} \\
&= \phi(g)\phi\left(\phi^{-1}(h)\right)\phi(g^{-1}) && \text{since } \phi \text{ is a homomorphism} \\
&= [\phi(g)]h[\phi(g)]^{-1} \\
&= \varphi_{\phi(g)}(h).
\end{aligned}$$

Hence as claimed, $\phi \circ \varphi_g \circ \phi^{-1} = \varphi_{\phi(g)} \in \operatorname{Inn}(G)$ so $\operatorname{Inn}(G) \triangleleft \operatorname{Aut}(G)$ as required. □

Proposition 1.1.22. *For any group homomorphism $\phi : G \to H$, $\ker \phi \triangleleft G$.*

Proof. Suppose $x \in \ker\phi, g \in G$. Then

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi^{-1}(g) = \phi(g)\phi^{-1}(g) = e_H \tag{1.29}$$

□

Question: Given $N \lhd G$ does there exist a group homomorphism $\phi : G \to H$ such that $N = \ker\phi$? That answer is that indeed there is as the following theorem shows. This, combined with the First Isomorphism Theorem will tell us that normal subgroups always occur as the kernel of some homomorphism.

Theorem 1.1.23. *Suppose $N \lhd G$, then $\exists H$ a group and a homomorphism $\phi : G \to H$ such that $N = \ker\phi$.*

Proof. Our first step will be to calculate H. For $g, g' \in G$ define a relation on G by $g \sim g'$ if and only if $g'g^{-1} \in N$. This is equivalent to saying that $g'N = gN$. Note that $g \sim g$ since $gg^{-1} = e \in N$ so $\sim$ is reflexive. Further, if $g \sim h$ then there exists $n \in N$ such that $gh^{-1} = n$ which implies that $n^{-1} = hg^{-1} \in N$ so $h \sim g$ and the relation is symmetric. Finally, assume that $g \sim h$ and $h \sim k$ so that $gh^{-1} \in N$ and $hk^{-1} \in N$. This means $\exists n, n' \in N$ such that $gh^{-1} = n$ and $hk^{-1} = n'$. Then the product $nn' \in N$ and so

$$nn' = (gh^{-1})(hk^{-1}) = gk^{-1} \tag{1.30}$$

so $g \sim k$ and we get that the relation is transitive. All of this together means that $\sim$ is an equivalence relation.

Define the set $H = G/N = \{[g]\}$ where $[g]$ denotes an equivalence class of g and define the binary operation $*$ on G/N by $[x] \cdot [y] = [xy]$. To check that $*$ is well defined, suppose that $x \sim x'$ and $y \sim y'$ so that $\exists n_1, n_2 \in N$ such that $x' = n_1 x$ and $y' = n_2 y$. We want to know if $xy \sim x'y'$, and can compute

$$\begin{aligned} x'y' &= n_1 x n_2 y \\ &= n_1(x n_2 x^{-1})xy \\ &= n_1 n' xy && \text{where } x n_2 x^{-1} = n' \text{ follows from normality} \end{aligned}$$

so that $xy \sim x'y'$.

Now $(G/N, *)$ forms a group. Since $e \in N$ we know that $[e] \in G/N$, and associativity is inherited from G. Furthermore this element acts as an identity since $[e][x] = [ex] = [x]$. Finally, we see that $[x]^{-1}[x] = [e] = [xx^{-1}] = [x][x^{-1}]$ so $[x]^{-1} = [^{-1}x]$

Define $\phi : G \to G/N$ by $g \mapsto [g]$, which we claim is a homomorphism. Indeed, note that

$$\phi(xy) = [xy] = [x][y] = \phi(x)\phi(y) \tag{1.31}$$

as required. It now follows that $N = \ker \phi$ since

$$\begin{aligned}\ker \phi &= \{g \in G : \phi(g) = [e]\} = \{g \in G : [g] = [e]\} \\ &= \{g \in G : g \sim e\} = \left\{g \in G : ge^{-1} \in N\right\} \\ &= \{g \in G : g \in N\} \\ &= N\end{aligned}$$

and hence N is the kernel of a group homomorphism as required. □

Definition 1.1.24. If N is a normal subgroup, we define the *quotient group* of G by N as G/N with the structure described above.

Proposition 1.1.25. *Let $X \subseteq G$ be an subset of G. Then*

$$C_G(X) = C_G(\langle X \rangle), \qquad N_G(X) = N_G(\langle X \rangle). \tag{1.32}$$

Proof. Let X be a subset of G. We will show that $N_G(X) = N_G(\langle X \rangle)$ from which the proof for $C_G(X)$ will follow similarly. First, we see that if $g \in N_G(\langle X \rangle)$ the certainly g normalizes each element of X so $g \in N_G(X)$ implying that

$$N_G(\langle X \rangle) \subseteq N_G(X). \tag{1.33}$$

On the other hand, let $g \in N_G(X)$ and consider an arbitrary element $z \in \langle X \rangle$. Consider the simple case where $z = x_1 x_2 \cdots x_n$ for $x_1, \ldots, x_n \in X$. Then

$$\begin{aligned}gzg^{-1} &= gx_1 \cdots x_n g^{-1} \\ &= (gx_1g^{-1})(gx_2g^{-1}) \cdots (gx_n)g^{-1}.\end{aligned}$$

Since $g \in N_G(X)$ we know that each of the gx_ig^{-1} above are contained in X and so we get that

$$gzg^{-1} = \hat{x}_1 \cdots \hat{x}_n \tag{1.34}$$

for some collection of elements $\hat{x}_1, \ldots, \hat{x}_n \in X$. Hence $N_G(X) \subseteq N_G(\langle X \rangle)$ and both inclusions give us the desired equality. □

1.1.5 The Isomorphism Theorems

The following are a class of theorems that are fairly ubiquitous throughout algebra and will allow us to make immediate conclusions given fairly rudimentary results. Before we state this however, we notice the following:

Lemma 1.1.26. *If $\phi : G \to H$ is a group homomorphism then $\operatorname{im}\phi$ is a subgroup of H.*

Proof. By 1.1.12 we know that $\phi(e_G) = e_H$ and so $e_H \in \operatorname{im}\phi$. If $h_1, h_2 \in \operatorname{im}\phi$ we know there exists $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$ so $h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2)$ so $h_1h_2 \in \operatorname{im}\phi$. Next, if $h \in \operatorname{im}\phi$ and $g \in G$ such that $\phi(g) = h$ then $\phi(g^{-1}) = \phi(g)^{-1} = h^{-1}$ so $h^{-1} \in \operatorname{im}\phi$. Finally, associativity is inherited from G and so we are done. □

Theorem 1.1.27 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a group homomorphism. Then*

$$G/\ker\phi \cong \operatorname{im}\phi. \tag{1.35}$$

Before we prove this, note that if $N \lhd G$ we can construct $G \to G/N$ which has kernel N, and that this map is surjective. We can injectively map this into any other subgroup.

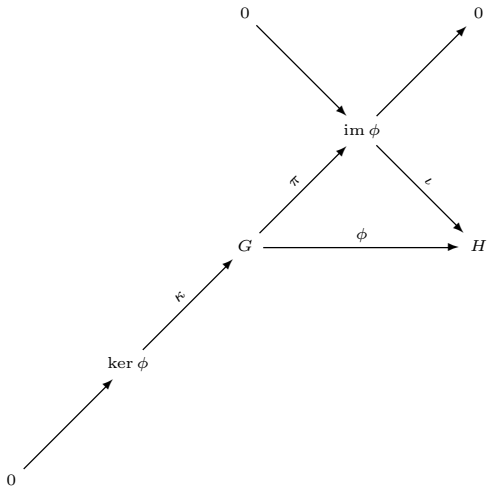
Proof. By 1.1.26 it is clear that $\operatorname{im}\phi$ is a subgroup and so our problem statement makes sense. Let $N = \ker\phi$ and define a map $\psi : G/N \to \operatorname{im}\phi$ by $\psi(Ng) = \phi(g)$. To see that this map is well defined suppose that $Ng = Ng'$ so that $g = ng'$ for some $n \in G$. Then $\phi(g) = \phi(n)\phi(g') = \phi(g')$ since $\phi(n) = e$. The map is a homomorphism since

$$\begin{aligned}\phi\Big((gH)(g'H)\Big) &= \phi(gg'H) = \phi(gg') \\ &= \phi(g)\phi(g') \\ &= \phi(gH)\phi(g'H).\end{aligned}$$

To see that ψ is surjective, note that if $y \in \operatorname{im}\phi$ then $y = \phi(g)$ for some $g \in G$ and so $y = \psi(Ng)$. To show that ψ is injective, let $\psi(Ng_1) = \psi(Ng_2)$. Then $\phi(g_1) = \phi(g_2)$ so that $g_1g_2^{-1} \in N$ which implies $Ng_1 = Ng_2$ as required. Hence ψ is a bijective group homomorphism and we can conclude that it is in fact a group isomorphism concluding the proof. □

The first isomorphism theorem is a powerful too that we will use a great deal in the following pages. Indeed, we will see that is it a fundamental (and almost trivial) result

that follows from category theory. We can visualize the first isomorphism theorem as the following commutative diagram.



Where π is the projectiion mapping and κ, ι are the inclusion mappings.

We wish to state a few other isomorphism theorems that are useful. The second isomorphism considers what happens when we take quotients of the sum and intersection of groups, and so the following proposition and its corollaries will make the final result easier to understand.

Proposition 1.1.28. *Suppose that $H, K \leq G$ then $HK \leq G$ if and only if $HK = KH$.*

Proof. ($\Rightarrow$) Suppose that $HK \leq G$. Let $x \in HK$ so that $x^{-1} \in HK$. Write $x^{-1} = hk$ so that $x = k^{-1}h^{-1} \in KH$ and we conclude that $HK \subseteq KH$. The reverse inclusion follows similarly.

($\Leftarrow$) Suppose that $HK = KH$. Let $x, x' \in HK$. Write $x = kh, x' = h'k'$ then $x'x^{-1} = h'k'h^{-1}k^{-1}$ but $k'h^{-1} \in KH = HK$ so $k'h^{-1} = h''k''$ so $x'x^{-1} = h'h''k''k' \in HK$ as required. □

Corollary 1.1.29. *Let $H, K \leq G$. If $H \subseteq N_G(K)$ then $HK \leq G$ and $K \lhd HK$.*

Proof. Let $x = hk \in HK$. Then $x = \underbrace{(hkh^{-1})}_{\in K} h$ since $H \subseteq N_G(K)$, so $HK \subseteq KH$. Similarly, if $x = kh \in KH$ then $x = h\underbrace{(h^{-1}kh)}_{\in K} \in HK$ so $KH \subseteq HK$ and we conclude $HK = KH$

which implies $HK \leq G$. Now we want to show that $K \lhd HK$. Certainly $K \subseteq N_G(K)$ and by assumption $H \subseteq N_G(K)$ and so $HK \subseteq N_G(K)$ and $K \lhd HK$. □

Corollary 1.1.30. *If $K \lhd G$ then $HK \leq G$ for any H and $K \lhd HK$.*

Proof. Since $K \lhd G$ we have that $N_G(K) = G$ and hence the previous corollary is immediately satisfied by every $H \leq G$. □

We are now in a position to present the second isomorphism theorem. Note that with these results in hand, the following statement actually makes sense.

Theorem 1.1.31 (Second Isomorphism Theorem)**.** *Let $H, K \leq G$ such that $H \subseteq N_G(K)$ Then $H \cap K \lhd H$ and $K \lhd HK$ with*

$$\frac{HK}{K} \cong \frac{H}{H \cap K} \tag{1.36}$$

Proof. We know via corollary that $K \lhd HK$. Define $\phi : H \to HK/K$ by $\phi(h) = Kh$. Then ϕ is the composition $H \hookrightarrow HK \twoheadrightarrow HK/K$ and

1. ϕ is a homomorphism since it is a composition of homomorphisms,

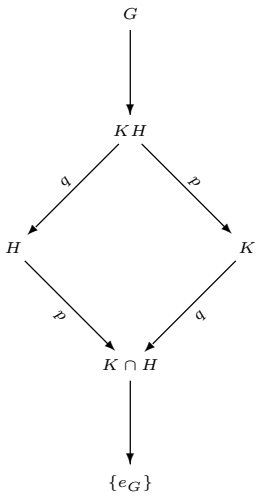
2. ϕ is surjective. Indeed, let $Xk \in HK/K$ for some $x \in HK = KH$. Write $x = kh$ so that $Kx = Kh = \phi(h)$,

3. We can compute that $\ker \phi = H \cap K$ as follows

$$\begin{aligned} \ker \phi &= \left\{ y \in H \;\middle|\; \phi(y) = e \right\} \\ &= \left\{ y \in H \;\middle|\; Ky = e \right\} \\ &= \left\{ y \in H \;\middle|\; y \in K \right\} \\ &= H \cap K. \end{aligned}$$

Combining this information with the first isomorphism theorem gives the desired result. □

The second isomorphism theorem is sometimes referred to as the *diamond isomorphism theorem* because we get the following diagram:



The next isomorphism theorem indicates that quotient groups "behave like fractions" so that common elements cancel.

Theorem 1.1.32 (Third Isomorphism Theorem)**.** *Let $K \lhd G, H \lhd G$ and $K \leq H$. Then $H/K \lhd G/K$ and*

$$\frac{G/K}{H/K} = G/H \tag{1.37}$$

Proof. We can first check that $H/K \lhd G/K$ and $G \twoheadrightarrow G/K \twoheadrightarrow \frac{G/K}{H/K}$ and define $\phi : G \to \frac{G/K}{H/K}$ and show that $G/\ker\phi \cong \operatorname{im}\phi = \frac{G/K}{H/K}$, which is true since ϕ is the composition of surjective functions and hence is surjective. It remains to check that $H = \ker\phi$ to complete the proof. □

Definition 1.1.33. Let G be a group and $H \subseteq G$. Then we define $[G : H]$ to be the number of left cosets gH in G.

The final isomorphism theorem we are going to consider tells us that subgroups of a quotient group pair up nicely with particular subgroups of the original group.

Theorem 1.1.34 (Fourth/Lattice Isomorphism Theorem)**.** *Let $N \triangleleft G$ and $q : G \twoheadrightarrow G/N$ be the quotient map. Then this induces a bijection*

$$\left\{ \begin{array}{c} \textit{Subgroups of } G \\ \textit{containing } N \end{array} \right\} \leftrightarrow \left\{ \textit{ Subgroups of } G/N \right\} \tag{1.38}$$

Furhtermore, this bijection satisfies

1. *$A \leq B$ if and only if $q(A) \leq q(B)$. In this case $[B : A] = [q(B) : q(A)]$.*
2. *$q(A \cap B) = q(A) \cap q(B)$*
3. *$A \triangleleft B$ if and only if $q(A) \triangleleft q(B)$*

Proof. Let $A \leq G$ and define $q(A) \leq G/N$ which gives one direction of the correspondence. Conversely, consider $X \leq G/N$ and define the preimage as $q^{-1}(X) \leq G$. The remainder of the proof is a simple exercise. □

Note that if $\phi : X \to Y$ is a group homomorphism and $H \leq X$ then $\phi(H) \leq Y$. Similarly, if $K \leq Y$ then $q^{-1}(K) \leq X$.

1.2 Simple Groups and Composition Series

When one creates an algebraic construct, there are a few questions that one would like to consider. One of these questions is if there is a way to charactererize every kind of element in your algebraic object. In general this is not possible, however, one can instead strive to understand "building blocks" of the object. In the case of groups, such building blocks are given by simple groups.

Definition 1.2.1. Let G be a group. The G is *simple* if it has no proper, non-trivial normal subgroups.

While simple groups may appear to be anything but simple, the fact is that because they contain no proper non-trivial normal subgroups, they cannot be built out of any smaller subgroups; something that will be corroborated when we consider semi-direct products in section . Our goal will be to do our best to characterize groups via their simple subgroups,

which will be done by considering a group G. If G is simple, we are done. Otherwise, let $A_0 \triangleleft G$ and define $G_1 = G/A_0$. If G_1 is simple we are done; otherwise, let $A_1 \triangleleft G_1$ and let $G_2 = G_1/A_1$. We continue in this manner until we eventually reach a simple group.

Definition 1.2.2. If G is a group, a *composition series* of G is a chain of subgroups

$$G \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq \{e\} \tag{1.39}$$

Such that $A_{i+1} \triangleleft A_i$ and A_i/A_{i+1} is simple. The A_i/A_{i+1} are called *composition factors* and this chain may sometimes be written as

$$G \triangleright A_1 \triangleright A_2 \triangleright \cdots \tag{1.40}$$

Note that the each A_{i+1} need only be normal in A_i and not in all of G. Furthermore, it turns out that given a composition series, it is not possible to reconstruct the group from which it was derived. However, each group has a unique composition series, as we will see in the next section.

1.2.1 The Jordan-Hölder Theorem

Theorem 1.2.3 (Jordan-Hölder Theorem)**.** *Given a finite group G there exists a sequence*

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_n = \{e\} \tag{1.41}$$

such that $H_i = G_i/G_{i+1}$ are simple. Furthermore, the sequence $\{H_0, \ldots, H_{n-1}\}$ called the "composition factors" and these are unique up to a permutation.

Proof. Let us use induction on the order of $|G|$.

Existence: Let G_1 be a proper maximal normal subgroup of G (under inclusion). If $G_1 = \{e\}$ then G is simple and $G \triangleright \{e\}$ is the composition tower. Otherwise, G_1 is a smaller group; that is, $|G_1| < |G|$ and so by induction $G_1 \triangleright G_2 \triangleright G_3 \cdots$ is a tower for G_1. We know that this must terminate in identity since the order of the subgroups descreases strictly at each stage and so the tower must terminate. We conclude that

$$G_1 \triangleright G_2 \triangleright G_3 \cdots$$

is a tower for G.

Uniqueness: Suppose that we are given two towers

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$
$$G = G'_0 \rhd G'_1 \rhd G'_2 \rhd c \cdots \rhd G'_m = \{e\}$$

If $G_1 = G_1$ then the theorem follows by induction. Thus assume that $G_1 \neq G'_1$. Define the composition factors as $H_i = G_i/G_{i+1}$ and $H'_i = G'_i/G'_{i+1}$ which are all simple.

Claim: $G = G_1G'_1$

Indeed, note that $G_1 \subsetneq G_1G'_1$. Similarly $G'_1 \subsetneq G_1G'_1$. And since the product of normal subgroups is normal, then $G_1G'_1 \lhd G$. But this cannot be a strict inclusion, since by the Fourth isomorphism theorem, it would be a normal group between G_1 and G but my maximality of G_1, this is not possible. so $G = G_1G'_1$. Let $K_1 = G_1 \cap G'_1$, and note that using the second isomorphism theorem

$$\frac{G_1}{K_1} = \frac{G_1}{G_1 \cap G_2} \cong \frac{G_1G'_1}{G'_1} = \frac{G}{G'_1} \text{ and } \frac{G'_1}{K} \cong \frac{G}{G_1} \tag{1.42}$$

Let $H''_i = K_i/K_{i+1}$. By uniqueness for G_1 we know that up to a permutation we have

$$(H_2, H_3, \ldots) = (H'_1, H''_2, \ldots)$$
$$(H'_2, H'_3, \ldots) = (H_1, H''_2, \ldots)$$

which implies that

$$(H_1, H_2, \ldots) = (H_1, H'_1, H''_2, \ldots) = (H'_1, H_1, H''_2, \ldots) = (H'_1, H'_2, H'_3, \ldots)$$

□

Example 1.2.4.

1. Consider $\mathbb{Z}/p$. This group is simple, and so it yields a composition series $\mathbb{Z}/p \rhd \{e\}$.

2. Consider S_3 which has order 6. Since the subgroup must divide the order of the group, the next element must have order 2 or 3. There is no normal subgroup of order 2, so we must move to order 3. Let $H_3 = \langle(123)\rangle$ which is indeed normal. So we can write

   $$S_3 \lhd H_3 \lhd \{e\}$$

   which as composition factors $S_3/H_3 = \mathbb{Z}/2$ and $H_3/\{e\} = \mathbb{Z}/3$.

3. Consider S_5 whose order is $|S_5| = 120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$. We can write

   $$S_5 \rhd A_5 \rhd \{e\}$$

   which has composition factors $S_5/A_5 = \mathbb{Z}/2$ and $A_5/\{e\} = A_5$.

4. Consider S_4 and write

   $$S_4 \rhd A_4 \rhd V \rhd \mathbb{Z}/2 \rhd \{e\}$$

   where $V = \{e, (12)(34), (13)(24), (14)(23)\} = \mathbb{Z}/2 \oplus \mathbb{Z}/2$ is the Klein four group, and $\mathbb{Z}/2$ is chosen to be the identity and any other non-identity element of V. The composition factors are $S_4/A_4 = \mathbb{Z}/2, A_4/V = \mathbb{Z}_3, V/(\mathbb{Z}/2) = \mathbb{Z}/2$ and $(\mathbb{Z}/2)/\{e\} = \mathbb{Z}/2$

1.2.2 The Simplicity of A_n

Definition 1.2.5. Let X be a set and define S_X to be the set of all self-bijections of X. This is a group under the composition of bijections and is sometimes denoted $\mathrm{Aut}(X)$.

We have already seen a special case of $\mathrm{Aut}(X)$, when the set X is given by $\{1, \ldots, n)\}$. This is then just the symmetric group, and we use the related but subtly different notation S_n.

Note that when considering the product in the automorphism group, there are two possible convenentions. If $f, g \in S_X$ then we define $f * g = g \circ f$; alternatively, one may define $f * g = f \circ g$. Again, one must be consistent and for our purposes, we shall always use the latter definition of the product.

Cycle Notation: Consider the element $(a_1 \cdots a_n)$ called an n-cycle. This notation means that this is the permutation acting as $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_n \mapsto a_1$. Any given permutation may be able to be written as a single cycle, but can always be written in terms of disjoint cycles. As a convention we omit 1-cycles from our expression.

The difference in the two conventions mentioned above becomes evident when we consider the product of two permutations using cycle notation. Using the definition $f * g = g \circ f$ we evaluate products as

$$(123)(134) = (124). \tag{1.43}$$

Alternatively, using the definition $f * g = f \circ g$ we get

$$(123)(134) = (234). \tag{1.44}$$

Definition 1.2.6. Given a permutation $\sigma \in S_n$, the *cycle type* of σ is a multiset of natural numbers describing the unique decomposition of σ into disjoint cycles. That is, if σ is given by

$$\sigma = (a_1^1 \cdots a_{n_1}^1) \cdots (a_1^k \cdots a_{n_k}^k) \tag{1.45}$$

then σ has cycle type $[n_1, \ldots, n_k]$.

Note that if $\sigma \in S_n$ has cycle type $[n_1, \ldots, n_k]$ then $n = \sum_{i=1}^{k} n_i$.

Properties:

1. In cycle notation, we note that $(a_1 \cdots a_n)^{-1} = (a_n \cdots a_1)$.
2. If σ has cycle type $[b_1, \ldots, b_k]$ then the order of σ is $\operatorname{lcm}(b_1, \ldots, b_k)$.
3. Let $\sigma, \tau \in S_m$ with $\sigma = (a_1^{(1)} \cdots a_1^{(r_1)}) \cdots (a_n^{(1)} \cdots a_n^{(r_n)})$. Then
$$\tau\sigma\tau^{-1} = \left(\tau^{-1}(a_1^{(1)}) \cdots \tau^{-1}(a_1^{(r_1)})\right) \cdots \left(\tau^{-1}(a_n^{(1)}) \cdots \tau^{-1}(a_n^{(r_n)})\right) \tag{1.46}$$
4. σ is conjugate to σ' if and only σ and σ' have the same cycle type.
5. Given a cycle type $[b_1, \cdots, b_k]$ in S_n. Let $m \in \mathbb{N}$ and $\ell_m = |\{b_k = m\}|$. Then the number of elements in the conjugacy class
$$\frac{n!}{\prod_{i=1}^{\max\{b_i\}} m^{\ell_m} \ell_m!}. \tag{1.47}$$

Definition 1.2.7. Consider S_n and define the polynomial
$$\Delta = \prod_{\substack{i,j \\ i \neq j}} (x_i - x_j). \tag{1.48}$$
For each $\sigma \in S_n$ we have that $\sigma(\Delta) = \pm\Delta$ and so we define the *sign* of the permutation σ as
$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \sigma\Delta = \Delta \\ -1 & \sigma\Delta = -\Delta \end{cases}. \tag{1.49}$$

Definition 1.2.8. Let $\varepsilon : S_n \to C_2$ by $\sigma \mapsto \operatorname{sgn}(\sigma)$, which is a group homomorphism. We define the *alternating group* to be $A_n = \ker \varepsilon$.

Example 1.2.9. Consider a surjective homomorphism $\phi : S_4 \twoheadrightarrow S_3$. We can view S_4 as acting on the vertices of a tetrahedron. In order to find a homomorphic image, we ask ourselves the question "What is there three of on the tetrahedron?" We notice that there are precisely three pairs of opposite edges, and so this is how we will define our homomorphism.

Label the vertices $\{1, 2, 3, 4\}$ and let S_3 be described by $\{R, G, B\}$ where
$$R = \{[34], [12]\}, B = \{[13], [42]\}, G = \{[14], [23]\} \tag{1.50}$$

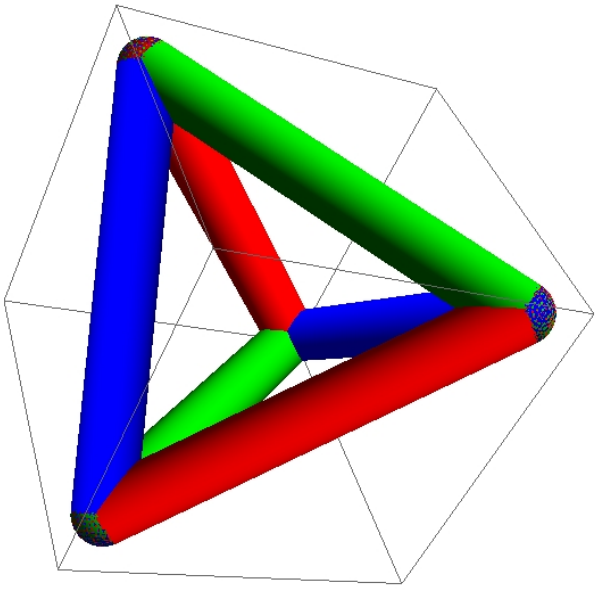


Figure 1.1: Coloured tetrahedron. ©Dror Bar-Natan, 2011.

and consider [2314]. This permutation acts as

$$\phi([2314])(\mathrm{RGB}) = (\mathrm{GBR}). \tag{1.51}$$

Question: Does there exist some homomorphism $\phi : S_4 \to G$ such that $\ker \phi = S_3$? That is, is S_3 a normal subgroup of S_4? If we fix any point, say$[***4]$ in S_4, the corresponding set of permutations is in S_3 but is not preserved under conjugation. Indeed, conjugation by a transposition in the fourth element will not be preserved. However, this is not sufficient to conclude that no such homomorphism could exist. It only shows that this subgroup of S_4 is not isomorphic to S_3. So is there some other?

Proposition 1.2.10. *If $\sigma = (a_1, \ldots, a_k)$ is a k-cycle and $\tau = [\tau_1, \ldots, \tau_n]$ then $\sigma^\tau = \tau^{-1} \circ \sigma \circ \tau$ is again a cycle and*

$$\sigma^\tau = (\tau^{-1}(a_1), \ldots, \tau^{-1}(a_k)). \tag{1.52}$$

The proof of this result is just an exercise in book keeping and is left as an exercise. This being said, we claimed earlier that two cycles were conjugate if and only if they had the same cycle type. To make this more precise, consider the following corollary:

Corollary 1.2.11. *Two permutations $\sigma, \sigma' \in S_n$ are conjugate if and only if they have the same cycle structure. That is, write*

$$\sigma = (a_1^1 \cdots a_{k_1}^1)(a_1^2 \cdots a_{k_2}^2) \cdots$$
$$\tau = (b_1^1 \cdots b_{\ell_1}^1)(b_1^2 \cdots b_{\ell_2}^2) \cdots$$

then σ and τ are conjugate if and only if $(k_1, k_2, \ldots) = (\ell_1, \ell_2, \ldots)$ up to a possible permutation.

Proof. Consider single cycles $\sigma = (a_1, \ldots, a_k)$ and $\sigma = (b_1, \cdots b_k)$. By the previous claim, we know that $\tau^{-1} a_i = b_i$ for every $i = 1, \ldots, k$. This defines τ^{-1} on $a_1, \ldots, a_k$ and we can extend τ^{-1} arbitrarly. □

Corollary 1.2.12. *The number of conjugacy classes in S_n is the number of partitions of n.*

Of the group we have seen so far, it is difficult to positively identify whether any of them have been simple except in very special cases (finite cyclic groups of prime order). In fact, after discussing the Sylow Theorem in section we will be able to show that for all orders up to 60 we can be guaranteed there is a non-simple group of that order. Indeed, it turns out that the first non-simple, non-abelian group is given by the alternating group on five letters, and that alternating groups in general give us an entire class of groups that are simple.

Theorem 1.2.13. *The alternating group A_n is simple for $n \neq 4$.*

Note that for $n = 1, 2$ this is trivial as $A_1 = \emptyset$ and $A_2 = \{0\}$ the trivial group. For $n = 3$ we have that $A_3 = \mathbb{Z}/3$ which is an abelian group of prime-order, and hence simple.

We know that for $n = 4$, A_n is not simple. Indeed, we have seen that there is a non-trivial homomorphism $\phi : S_4 \to S_3$. By restricting ϕ to A_4 we still have a non-trivial homomorphism whose kernel is non-trivial. This kernel is a normal subgroup.

We will need the following Lemmas for our proof.

Lemma 1.2.14. *Every element of A_n is a product of 3-cycles.*

Proof. Every $\sigma \in A_n$ is a product of an even number of 2-cycles. Without loss of generality, we will demonstrate this on the following cycles. Indeed,

$$(12)(23) = (123) \qquad (123)(234) = (12)(34)$$

□

Lemma 1.2.15. *If $N \triangleleft A_n$ contains a 3-cycle, then $N = A_n$.*

Proof. Without loss of generality, we can consider $(123) \in N$. We want to show that for all $\sigma \in S_n$ we must have that $(123)^\sigma \in N$. If $\sigma \in A_n$ then this is clear since N is normal in A_n; otherwise, take $\sigma = (12)\sigma'$ with $\sigma' \in A_n$. Since $(123)^{(12)} = (123)^2$ we have that $(123)^\sigma = \left((123)^2\right)^{\sigma'} \in N$. So N contains all three cycles. □

Proof of Theorem 1.2.2. Let $n \geq 5$ and take $N \triangleleft A_n$. By the previous two lemmas, it is sufficient to show that N always contains a three cycle.

Case 1: N contains an element with cycle length at least 4.

Let $\sigma = (123456)\sigma' \in N$. Now N is normal in A_n so $(123)\sigma(123)^{-1} \in N$. Similarly, multiplying by σ^{-1} will keep the element in N, so $\sigma^{-1}(123)\sigma(123)^{-1} = (136) \in N$ and N contains a three cycle.

Case 2: N contains an element with two cycles of length 3.

Let $\sigma = (123)(456)\sigma' \in N$. Then by the same reasoning as before $\sigma^{-1}(124)\sigma(124)^{-1} \in N$ and can be computed as $\sigma^{-1}(124)\sigma(124)^{-1} = (14263)$. We can now use Case 1 to deduce that N has a three cycle.

Case 3: N contains an element that is a three-cycle and a product of disjoint transpositions. Write $\sigma = (123)\sigma'$ and note that $\sigma'^2 = e$.

Then $\sigma^2 = (123)\sigma'(123)\sigma'$ but the elements of σ' are disjoint with (123), and we conclude that σ' and (123) commute; that is, $(123)\sigma' = \sigma'(123)$. Thus $\sigma^2 = (123)^2\sigma'^2 = (132) \in N$, and N contains a three cycle.

Case 4: Finally, consider the case when the element of N is a product of disjoint 2-cycles.

Write $\sigma = (12)(34)\sigma'$. By previous rationale, we know that $\sigma^{-1}(123)\sigma(123)^{-1} \in N$ and can be computed as $\sigma^{-1}(123)\sigma(123)^{-1} = (13)(24) = \tau \in N$. We can view this as a sort of purification, in that we have simplified a product of disjoint 2-cycles of arbitrary length into the case of two disjoint 2-cycles. Applying this procedure again, we get $\tau^{-1}(125)\tau(125)^{-1} = (13452) \in N$ and we again refer to Case 1 to conclude N contains a three cycle. □

Note that this last case is the only case in which we did not assume "5" was part of the hypothesis, but needed to use it. Hence we need $n \geq 5$ for this case to hold.

If $\{e\} \neq N \triangleleft A_4$ then N must contain τ from case 4 above, which implies that

$$N = \{e, (13)(24), (12)(34), (14)(23)\} \tag{1.53}$$

the Klein four group.

We now return to a problem we considered previously.

Proposition 1.2.16. *S_4 contains no normal subgroup $H \leq S_4$ such that $H \cong S_3$.*

Proof. For the sake of contradiction, assume there is such a normal subgroup. Then S_3 has an element of order 3 and therefore so does H. Such an element must be a three-cycle, and hence it contains all three cycles. There are eight three-cycles in S_4 and so $|H| > 8$. But this cannot be true, so no such normal subgroup exists. □

1.3 Group Actions

Definition 1.3.1. A left group action is a group G acting on a set X is a binary map $G \times X \to X$ denoted by $(g, x) \mapsto gx$ such that $(g_1 g_2)x = g_1(g_2(x))$ and $ex = x$.

If $gx = y$ then $g^{-1}y = x$. We sometimes say that "X is a G-set" or write "$G \circlearrowright X$."

Similarly, we can define a right group action $X \circlearrowleft G$ with a binary map $X \times G \to X$ mapping $(x, g) \mapsto xg$ satisfying $x(g_1 g_2) = (xg_1)g_2$.

Alternatively, assume we have a group action of G on a set X. Note that for any set X we can define the *symmetric group on* X, S_X which is just the set of all bijections on X. Thus given a $g \in G$, the map $x \mapsto gx$ is a mapping $X \to X$ which is an element of $S(X)$. Hence we can define a map $\alpha : G \to S(X)$. If the group acts on the left, then α is an anti-homomorphism. Conversely, if G acts on the right then α is a homomorphism. To be more precise, we have the following theorem:

Proposition 1.3.2. *There is a bijective correspondence between the set of left-group actions of a group G on a set X, and the set of group homomorphisms $\sigma : G \to S_X$.*

Proof. Let ρ be our left group action, and define $\sigma : G \to S_X$ by $\sigma(g)(x) = \rho(g, x)$. Now

$$\begin{aligned}\sigma(gh)(x) &= \rho(gh, x) = \rho(g, \rho(h, x)) = \sigma(g)\rho(h, a) = \sigma(g)(\sigma(h)(x)) \\ &= \sigma(g) \circ \sigma(h)(x)\end{aligned}$$

so σ preserves the product. On the other hand

$$\sigma(g^{-1}) \circ \sigma(g)(x) = \sigma(g^{-1}g)(x) = \sigma(e_G)(x) = \rho(e_G)(x) = x$$

so σ also preserves inverses.

Conversely, if $\sigma : G \to S_X$ is a group homomorphism, define $\rho : G \times X \to X$ as $\rho(g, x) = \sigma(g)(x)$. The exact same argument as above (only done in the opposite direction) tells us that ρ is indeed a group action. □

Note that the differences between group homomorphisms and anti-homomorphisms are very minor. Indeed, every group comes canonically equipped with an anti-homomorphims: the inverse map. Define $\iota_G : G \to G$ by $g \mapsto g^{-1}$. Then $(gh)^{-1} = h^{-1}g^{-1}$. Thus if $\phi : G \to H$ is a morphism, then $\phi \circ \iota_G = \iota_H \circ \phi$ is an anti-homomorphism, and vice-versa.

Example 1.3.3.

1. G may act on itself by conjugation. Depending on the convention used for conjugation, this could be seen as either a left- or a right-group action. For our purposes, we will consider the later. In this situation $X = G$, and $(g, g') \mapsto g^{g'}$. But $x^{(gh)} = (x^g)^h$.

2. Every group G acts on itself by left-multiplication. In otherwords, take $X = G$ so that $(g, x) = gx$ where this notation now denotes the actual product. Notice that this guarantees that a homomorphism $\beta : G \to S(X)$ always exists. It can be shown that this is an injective homomorphism and so $\ker \phi = \{e\}$. Thus every group is isomorphic to a subgroup of $S(G)$.

   What if we apply this to S_n? Then $\beta : S_n \to S(S_n)$ and $S(S_n) = S_{n!}$.

3. Given any group G and $H < G$ not necessarily normal, we define $G \circlearrowleft G/H$ by $g(xH) = (gx)H$.

4. Consider $S_{n-1} < S_n$. Note that $|S_n/S_{n-1}| = \frac{|S_n|}{|S_{n-1}|} = \frac{n!}{(n-1)!} = n$. Now we know that S_n can be seen as acting on a set of cardinality n just by permutation. Hence S_n can act on S_n/S_{n-1} in the same manner.

5. Consider the special orthogonal group $SO(n)$ which is the set of orientation preserving symmetries of $\mathbb{R}^n$, or alternatively S^{n-1}. We can write

$$SO(n) = \left\{ X \in M_n(\mathbb{R}) \;\middle|\; X^T X = I, \det X = 1 \right\}. \tag{1.54}$$

Note that $SO(3)$ are rotations in $\mathbb{R}^3$ and that $SO(2) \subset SO(3)$ are rotations of $\mathbb{R}^2$, as rotations on S^2 which preserve N the North pole. Let us consider the quotient space,

$$SO(3)/SO(2) = \left\{ g \cdot SO(2) \;\middle|\; g \in SO(3) \right\}. \tag{1.55}$$

We can visualize $SO(3)/SO(2) \to S^2$ and the image of cosets will be $gSO(2) \to gN$. Hence $SO(3)$ acts on $SO(3)/SO(2) = S^2$.

Exercise: Show that $S_n \circlearrowleft \{1, \ldots, n\}$ and $S_n \circlearrowleft S_n/S_{n-1}$ are isomorphic.

Fact: If X_1 and X_2 are G-sets then so is $X_1 \sqcup X_2$, the disjoint union of X_1 and X_2.

Definition 1.3.4. We say that a the action of a group G on a set X is *transitive* if $\forall x, y \in X, \exists g \in G$ such that $gx = y$.

1.3.1 The Orbit-Stabilizer Theorem

Definition 1.3.5. If X is a G-set and $x \in X$ then the *stabilizer* of x is

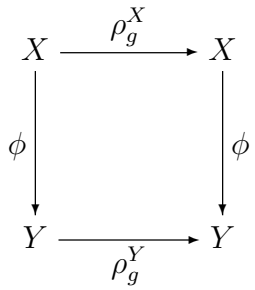
$$\mathrm{Stab}_X(x) = \left\{ g \in G \;\middle|\; gx = x \right\} < G. \tag{1.56}$$

Left G-sets form a category. Indeed, the objects are just the G-sets themselves; that is, a set X and an action $G \circlearrowleft X : G \times X \to X$. The morphisms are given as follows:

Definition 1.3.6. If X, Y are two G-sets then $\phi : X \to Y$ is a *G-set homomorphism* if $\forall g \in G$ we have that $\phi(gx) = g\phi(x)$. In this case, we say that ϕ is *equivariant* and if ϕ is bijective it is a *G-set isomorphism*.

We can visualize this using the following commutative diagram. Let $\phi : X \to Y$ be a G-set homomorphism, $\rho_g^X : X \to X$ be the group action on X by g, and $\rho_g^Y : Y \to Y$ be the

group action on Y induced by g. Then the following diagram commutes:



that is, $\rho_g^Y \circ \phi = \phi \circ \rho_g^X$.

Theorem 1.3.7 (Orbit-Stabilizer Theorem)**.** *Any G-set X is a disjoint union of transitive G-sets. Furthermore, if X is a transitive G-set and $x \in X$, then $X \cong G/H$ as a G-set for some $H < G$. In particular, $H = \mathrm{Stab}_X(x)$.*

Proof. Define an equivalence relation on X by $x \sim y$ if and only if $\exists g$ such that $gx = y$. Equivalently, we can write this as $y \in Gx$. We call Gx the G-orbit of x. By symmetry we can say that $x \in Gy$. It is possible then the show that $Gx = Gy$. Hence this equivalence relation partitions X into disjoint sets, and so X is a disjoint union of orbits of some $x_i \in X$ where each x_i is a class representative.

Claim 1.3.8. *Gx_i is a transtive G-set, and $Gx_i \cong G/\operatorname{Stab}(x_i)$.*

Proof. Let $H = \operatorname{Stab}(x)$, and take $y, z \in Gx_i$. Then there exists $g, h \in G$ such that $y = gx_i, z = hx_i$. Then $(gh^{-1})z = g(h^{-1}z) = gx_i = y$ and so Gx_i is transitive. □

We want to define $\psi : Gx \xrightarrow{G} / \operatorname{Stab}(x)$. If $y \in Gx$ then $y = gx$ for some $g \in G$. Define $\psi(y) = [g]_H = gH$. We must now show that this is well defined. Assume that $y = g'x$ then $g'x = gx$ so that $g^{-1}g'x = x$ so that $g^{-1}g' \in \operatorname{Stab}(x)$. Hence $gH = g'H$ so ψ is well defined.

Conversely, let $gH \in G/H$ then define $\phi : G/\operatorname{Stab}(x) \to Gx$ by $\phi(gH) = gx$. Again, we must check that this is well defined. If Assume then that $g'H = gH$ so that we can write $g' = gh$ for some $h \in H$. Then $g'x = ghx = gx$ so the function is well defined.

All that remains to be shown is that if $y \in Gx$ and $g \in G$ then $g_1\psi(y) = \psi(g_1y)$. Indeed, since Gx is transitive, find g such that $y = gx$. But then

$$g_1\psi(y) = g_1(gH) = (g_1g)H. \tag{1.57}$$

To compute $\psi(g_1y)$ we must find a g' such that $g'x = g_1y$. However, $y = gx$ so $g_1y = g_1gx = (g_1g)x$ so $g' = g_1g$. Thus

$$\psi(g_1y) = g'H = (g_1g)H. \tag{1.58}$$

so $\psi(g_1 y) = g_1 \psi(y)$. □

Corollary 1.3.9. *If X is transitive, then $|X| \Big| |G|$.*

Proof. By the previous theorem, we know that $X \cong G/\operatorname{Stab}_X(x)$. The result follows from Lagrange's theorem. □

If $|x| < \infty$ and x_i are representatives of the orbits then

$$|X| = \sum_i \frac{|G|}{|\operatorname{Stab}_X(x_i)|}. \tag{1.59}$$

1.3.2 Sylow Theorems

Definition 1.3.10. A p-group is a group whose order is a power of a prime p.

For example, consider groups of order 8. Then $(\mathbb{Z}/2)^3, \mathbb{Z}/2 \times \mathbb{Z}4, \mathbb{Z}/8, \mathbb{H}$, and D_8 the dihedral group of the square. The group $\mathbb{H} = \left\{ \pm 1, \pm i, \pm j, \pm k \;\middle|\; ij = k, i^2 = j^2 = k^2 = -1 \right\}$.

Proposition 1.3.11. *If G is a p-group, then G has a non-trivial centre $Z(G)$.*

Proof. G acts on itself by conjugation. Then we can write $|G|$ as the sum of the orbit of singletons, and all other orbits. Now note that if the orbits are singletons, we mjust have that $g^h = h^{-1}gh = g$ so that $gh = hg$. Thus singleton orbits are $\left\{ g \;\middle|\; \forall h, gh = hg \right\}$, this is precisely the centre. Similarly, for all other orbits we can choose a representative x_i in each non-trvial orbit, so that

$$|G| = |Z(G)| + \sum_i \frac{|G|}{\operatorname{Stab}(x_i)} \tag{1.60}$$

Now since $|G|$ is a power of a prime, $\frac{|G|}{\operatorname{Stab}(x_i)}$ is also a power of a prime. It cannot be one, since we have accounted for all singleton orbits, so p must divide it. Thus, $p \Big| |Z(g)|$. In particular $|Z(g)| > 1$ as required. □

Notice that in the previous theorem, the stabilizer $\text{Stab}(x_i) = \left\{ g \;\middle|\; x_i^g = x_i \right\} = \left\{ g \;\middle|\; gx_i = x_i g \right\}$, which is called the centralizer.

Definition 1.3.12. If G is a finite group, write $|G| = p^\alpha m$ where $p \nmid m$. A *Sylow-p subgroup of* G is a subgroup $P < G$ such that $|P| = p^\alpha$. Define $\text{Syl}_p(G)$ be the collection of all Sylow p-subgroups; that is,

$$\text{Syl}_p(G) = \left\{ P < G \;\middle|\; |P| = p^\alpha \right\}. \tag{1.61}$$

Lemma 1.3.13 (Cauchy's Theorem)**.** *If A is an abelian group and p is a prime which divides the order of A, then $\exists x \in A$ such that $|x| = p$.*

Proof. Proceed by induction on the order of $|A|$. Choose an element $x \in A$. If $p \;\middle|\; |x|$ then $x^{pn} = e$ for some n. So then $(x^n)^p = e$ and $|x^n| = p$. Otherwise, consider $A/\langle x \rangle$. Then there is an element of order $p \in A/\langle x \rangle$, say $\bar{y}$, so that $|\bar{y}|_{A/\langle x \rangle} = p$. But then $\bar{y}^p = e = \overline{y^p}$ which implies that $\exists y \in A$ such that $\pi(y) = \bar{y}$ and $y^p \langle x \rangle$. Let α be such that $y^p = x^\alpha$. Suppose that $|y| = pn + r$ where $0 \leq r < p$. Then

$$e = y^{|y|} = y^{pn+r} = (y^p)^n y^r = x^{\alpha n} y^r$$

so then $y^r \in \langle x \rangle$ so $\bar{y}^r = e$. However, $\bar{y}$ was an element of order p and $r < p$ so $r = 0$. Hence $p \;\middle|\; |y|$. Then we can refer to the first case and can find an element of order p. □

Theorem 1.3.14 (First Sylow Theorem)**.** *For any finite group G and any prime p,* $\text{Syl}_p(G) \neq \emptyset$.

Proof. We shall proceed by induction on the order of $|G|$. Assume that this is known for all groups of order less than $|G|$. Take $p^\alpha \;\middle|\; |G|$ for maximal $\alpha \geq 1$. In the even that $\alpha = 0$ then $\{e\}$ is the desired Sylow p-group and we're done.

We will use the class equation to show our result. If $p \not| |Z(G)|$ then $\exists x_i$ such that $|G|/|C_G(x_i)|$ is not divisible by p. But note that since $p^\alpha \;\middle|\; |G|$ then for $p \not| |G|/|C_G(x_i)|$ we

must have that $p^\alpha \Big| |C_G(x_i)| < |G|$. Hence $C_G(x_i)$ is a strict subgroup of G with $p^\alpha || C_G(x_i)|$ so by induction, $\exists P < C_G(x_i)$ with $|P| = p^\alpha$ and we're done, since then $P < G$.

Otherwise, we have that $p \Big| |Z(G)|$ and $Z(G)$ is an abelian group. By Cauchy's theorem, there is an element $x \in Z(G)$ such that $|x| = p$. By induction, $\exists P' < G/\langle x \rangle$ such that $|P'| = p^{\alpha-1}$. Denote by $\pi : G \to G/\langle x \rangle$ the projection map. We can use the fourth isomorphism theorem $\pi^{-1}(P') < G$ such that $|\pi^{-1}(P')| = p^\alpha$. □

Lemma 1.3.15. *1. If $P \in \mathrm{Syl}_p(G)$ and $H < N_G(P)$ is a p-group then $H < P$.*

2. If $x \in G$ has order a power of p and $x \in N_G(P)$ (that is; $x^{-1}Px = P$) then $x \in P$.

Proof. Consider the second isomorphism theorem and the product PH. Now $P \cap H < P, H < PH$ and $P \cap H$ is a p-group. If $[P : P \cap H] = p^\gamma$ and $[H : P \cap H] = p^\gamma$ then we must have

$$[PH : H] = p^\gamma \qquad [PH : P] = p^\alpha$$

Now $|PH|$ is a power of P, so $P = PH$ and we conclude that $H < P$.

Let $H = \langle x \rangle$. □

Theorem 1.3.16 (Second Sylow Theorem)**.** *Every p-subgroup of a group G is contained is a Sylow-p subgroup of G.*

Theorem 1.3.17 (Third Sylow Theorem)**.** *Denote by $n_p(G) = |\mathrm{Syl}_p(G)|$ the number of Sylow p-subgroups. Then*

1. $n_p(G) \Big| |G|$
2. $n_p(G) \equiv 1 \mod p$

Furthermore, all Sylow-p subgroups of G are conjugate to each other.

Example: Let $|G| = 15$. Then by Third Sylow, we know that $n_3 \equiv 1 \mod 3$ but $n_3 \Big| 15$ so $n_3 = 1$. Similarly, $n_5 = 1$. Hence there is a unique Sylow 3-subgroup and a unique Sylow

5-subgroup. Thus $P_3 \triangleleft G, P_5 \triangleleft G$. Furthermore, their intersection $P_3 \cap P_5 = \{e\}$. The reason for this is that their intersection would be subgroups of both P_3 and P_5 and so the order of each element must divide both 3 and 5:: the only such element is idenity. Now P_3P_5 is divisible by 3 and 5, divides 15 and so $P_3P_5 = G$.

Proposition 1.3.18. *If $K \triangleleft G, H \triangleleft G$ and $K \cap H = \{e\}$ then $KH \cong K \times H$.*

Note that to say that two elements commute $xy = yx$ is equivalent to $xyx^{-1}y^{-1} = e$. The left hand side appears often in group theory, and so we denote $[x, y] = xyx^{-1}y^{-1}$ and is said to be the commutator of x and y. We can write $[x, y] = y^{x^{-1}}y^{-1}$ so we check tht the conjugate of y is equal to y. By loose association, we will write $[H, K] = \{e\}$ to mean that $\forall h \in H, \forall k \in K, hk = kh$.

Lemma 1.3.19. *If $H \triangleleft G, K \triangleleft G$ with $H \cap K = \{e\}$ then $[H, K] = \{e\}$.*

Proof. Let $h \in H$ and $k \in K$. Then

$$\underbrace{hkh^{-1}}_{\in K}k^{-1} \in K, \qquad h\underbrace{kh^{-1}k^{-1}}_{\in H} \in H$$

Hence $[h, k] \in H \cap K$ but the only such element is the identity, so $[h, k] = e$. □

Proof of Proposition 1.3.18. It suffices to construct an isomorphism $\phi : K \times H \to KH$. Define $\phi(k, h) = kh$. Now ϕ is a homomorphism, since

$$\begin{aligned}
\phi\Big((k_1, h_1)(k_2, h_2)\Big) &= \phi(k_1k_2, h_1h_2) \\
&= k_1k_2h_1h_2 \\
&= (k_1h_1)(k_2h_2) && \text{from the Lemma} \\
&= \phi(k_1, h_1)\phi(k_2, h_2)
\end{aligned}$$

Now we want to see what the kernel of this morphism is. Note that if $\phi(k, h) = e$ then $kh = e$ which implies that $k = h^{-1} \in K \cap H = \{e\}$ and so $(k, h) = e$. Finally, this function is clearly surjective. □

Note that a group P of prime order p is isomorphic to $\mathbb{Z}/p$. Indeed, take $x \in P$. Then since the order of x must divide the order of P, we know that $\langle x \rangle = P$. Then $P = \{e, x^1, x^2, \ldots\}$ and so we identify x^k with $k \in \mathbb{Z}/p$ for the desired isomorphism.

Lemma 1.3.20. *$\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/(ab)$ if $(a,b) = 1$.*

Proof. Assume that $(a,b) = 1$, then we can find $s,t \in \mathbb{Z}$ such that $as + bt = 1$. Define a map $\mathbb{Z}/(ab) \xrightarrow{\cdot t} \mathbb{Z}/a, \mathbb{Z}/(ab) \xrightarrow{\cdot s} \mathbb{Z}/b$, so that we have a mapping $\mathbb{Z}/(ab) \to \mathbb{Z}/a \times \mathbb{Z}/b$ by $n \mapsto (\overline{nt}, \overline{ns})$. Similarly, define the map $\mathbb{Z}/a \times \mathbb{Z}b \to \mathbb{Z}/(ab)$ by $(\bar{x}, \bar{y}) \mapsto \overline{ax} + \overline{by}$. Thus $n \mapsto \overline{n(as+bt)} = n$. Similarly, alternating the composition yields

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto bx + ay \mapsto \begin{pmatrix} (bx+ay)t \\ (bx+ay)s \end{pmatrix} \mapsto \begin{pmatrix} btx \\ asy \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \end{pmatrix}$$

where we've use the fact that $bt \equiv 1 \mod a$ and $as \equiv 1 \mod b$. □

Proposition 1.3.21. *If $P \in \mathrm{Syl}_p(G)$, let $n_p(G)$ denote the number of conjugates of P. We claim that $n_p(G) \equiv 1 \mod p$ and $n_p(G) \Big| |G|$.*

Proof. Define X_p denote the set of conugates of P. Then X_p has a right-G-action by conjugation. Clearly this action is also transitive. This implies that $n_p(G) \Big| |G|$. Restrict this to a right-P-action on X_p. This is not necessarily a transitive action. Now the sum of the sizes of the oribts is necessarily the size of X_p; that is, $n_p(G)$. Now $P \in X_p$ is an orbit of size of one, since any element of P acting on P by conjugation does nothing. We claim that all other orbits are non-trivial. Indeed suppose that $P' \in X_p$ is a distinct conjugate of P. We have that $P \not\subset N_G(P')$, because if it were then by Lemma 1.3.15 we would have that $P \subseteq P'$ which would imply that $P = P'$ which cannot be true. Thus $\exists x \in P$ such that $x^{-1}Px \neq P'$ and so the orbit of P' is non-trivial.

Now since $n_p(G)$ is the sum of the sizes of the orbits, $n_p(G)$ is the sum of sizes of nontrivial orbits of X_P plus the trivial orbit. Since all p divides the order of non-trivial orbits then

$$n_p(G) \equiv 1 \mod p$$

□

Proposition 1.3.22. *If H is a p-subgroup of G and $P \in \mathrm{Syl}_p(G)$ then H is a conjugate of P.*

Proof. Consider the right-group action of H on the set X_p of conjugates of P. Now the order of H is divisible by p since H is a p-subgroup. The size of X_p is $n_p(G) \equiv 1 \mod p$. But the orbits of H on X_p must have orbits whose sizes are powers of p, and so at least one of these must be a singleton orbit otherwise $n_p(G) \equiv 0 \mod p$. Let P' denote this trivial orbit. To say that H acts trivially on P' by conjugation means that $H \subseteq N_G(P')$, so $H < P'$. But $P' \in X_p$ implies that H is a subgroup of a conjugate of P which is what we wanted to show. □

Note that Propositions 1.3.21 and 1.3.22 yield the remaining Sylow theorems. Indeed, the we have already proven the first in entirety. We know that all Sylow p-subgroup must be conjugate since if $P, P' \in \mathrm{Syl}_p(G)$ then P' is a p-group and so by Proposition 1.3.22 P' is contained in a conjugate of P. However, conjugation preserves order, so P' is a conjugate of P. The criteria on $n_p(G)$ then follows from the fact that in the proof of Proposition 1.3.21 we have that $\mathrm{Syl}_p(G) = X_p$.

1.4 Products of Groups

If $N, H < G$ then we want to compare $N \times H$ with NH. Part of this analysis is quite obvious, as there is a always a map $\mu : N \times H \to NH$ that acts as $(n, h) \mapsto nh$. Generally speaking, this is only a set map; we cannot be assured that this is a group homomorphism. We showed before that we required the commutativity of N and H for the map to be a homomorphism.

In general, we are unable to say anything without additional restrictions on the interaction between N and H beyond surjectivity. In fact, NH need not even be a group. If $N \cap H = \{e\}$ then μ is injective. Indeed, suppose that $\mu(n_1, h_1) = \mu(n_2, h_2)$ so that $n_1h_1 = n_2h_2$. Then by multiplying by n_2^{-1} on the left we get $n_2^{-1}n_1h_1 = h_2$. Then multiplying by h_1^{-1} on the right we get $n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H$. So $n_2^{-1}n_1 = h_2h_1^{-1} = e$ so $n_2 = n_1$ and $h_2 = h_1$ allowing us to conclude that $(n_1, h_1) = (n_2, h_2)$ which shows that μ is injective.

If we additionally assume that $N \triangleleft G, H \triangleleft G$ then we have already seen that $N \times H \cong NH$ and μ is an isomorphism.

It remains to consider the case when $N \cap H = \{e\}, N \triangleleft G$ and $H < G$. In this case $H \subset N_G(H)$ and so NH is a group. However μ may not necesarily be the group homomorphism that we require. We notice that H acts on N by conjugation; alternatively, $\exists \phi : H \to \mathrm{Aut}(N)$ by $h \mapsto \phi_h$ where $\phi_h(n) = hnh^{-1}$. We claim that if one knows ϕ then we know everything there is to know about NH. Indeed, consider a general element of NH written as n_1h_1. We want to know how to multiply this by a general element $n_2h_2 \in NH$. Then

$$(n_1h_1)(n_2h_2) = n_1 \underbrace{h_1h_2h_1^{-1}}_{=\phi_{h_1}(n_2)} h_1h_2 = n_1\phi_{h_1}(n_2)h_1h_2$$

then identifying $\mu(n_i, h_i) = n_i h_i$ we see that

$$\mu(n_1, h_1)\mu(n_2, h_2) = \mu(n_1\phi_{h_1}(n_2), h_1 h_2)$$

Definition 1.4.1. Suppose N, H are groups and $\phi : H \to \mathrm{Aut}(N)$ is a group homomorphism. Then define the group $N \rtimes_\phi H = \left\{(n, h) \,\middle|\, n \in N, h \in H\right\}$ with the binary operator

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1 h_2).$$

Theorem 1.4.2. *1. The binary operator $(n_1, h_1) \cdot (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1 h_2)$ satisfies the group axioms.*

2. By identifying $H = \{(e_N, h) : h \in H\}$ we have $H < G$. Similarily, $N \triangleleft G$. Furthermore, $G/N \cong H$ and $G = NH$.

3. If $G = NH$ where $N \triangleleft G, H < G$ and $H \cap N = \{e\}$ then $G \cong N \rtimes_\phi H$ where $\phi_h(n) = hnh^{-1}$.

Proof. 1. We need to find an identity element, which we claim is given by (e_1, e_2). Indeed note that

$$(e_N, e_H)(n_1, h_1) = (e_N\phi_{e_H}(n_2), e_H h_2) = (n_2, h_2)$$

In order to show associativity, we will need to exploit properties of homomorphisms. In particular, $\phi_{h_1h_2}(n) = \phi(h_1\phi_{h_2}(n))$ and $\phi_h(n_2n_3) = \phi_h(n_2)\phi_h(n_3)$. It can easily be checked that the inverse is given by $(n, h)^{-1} = (\phi_{h^{-1}}(n^{-1}), h^{-1})$.

2. The majority of this result is trivial and hence omitted. However, let us show that $G = NH$. Note that we can write $(n, h) = (n, e_H)(e_N, h)$ and $(n, e_H) \in N$ and $(e_N, h) \in H$. Furtheremore, we conjecture that the inverse can be calculated as

$$(n, h)^{-1} = (e_N, h)^{-1}(n, e_H)^{-1} = (e_N, h^{-1})(n^{-1}, e_H) = (\phi_{h^{-1}}(n^{-1}), h^{-1})$$

Simple substitution reveals that this is indeed the case.

3. The proof of this statement comes from our motivation and construction of the semidirect product just preceeding this theorem.

□

Example 1.4.3. Consider $\mathbb{Z}/n \rtimes \{\pm 1\} = D_{2n}$ which is referred to as the dihedral group with $2n$ elements. This is the group of symmetries of an $n-$gon. For example, D_{12} is the group of symmetries on the hexagon.

Example 1.4.4. Consider $\mathbb{R}^+$ the additive group of real numbers. By thinking about the set if automorphisms of $\mathbb{R}^+$, we recall that this will just be the linear maps on $\mathbb{R}$. In the one-dimensional case this corresponds to multiplication by a scalar, and so the multiplicative group $\mathbb{R}^\times$ acts on $\mathbb{R}^+$. Hence consider $\mathbb{R}^+ \rtimes \mathbb{R}^\times$. [Dror Notation: Denote by $H_x \times G_y$ to mean that whenever we write x or y then $x \in H$ and $y \in G$.]. Let $a \in \mathbb{R}^+$ and $b \in \mathbb{R}^\times$. We claim that $\mathbb{R}^+ \rtimes \mathbb{R}^\times = (ax+b)$-group; that is, the affine symmetries of the real line. Note that the composition of two such functions are another such function since

$$(a_1x + b_1) \circ (a_2x + b_2) = a_1(a_2x + b_2) + b_1 = (a_1a_2)x + (a_1b_2 + b_1). \tag{1.62}$$

Example 1.4.5. In the same spirit our of last example, there is a $\{Ax+b\}$ group which is the set of symmetries of the a vector space V. In particular, $\{Ax+b\} = V \rtimes GL(V)$. with $b \in V$ and $A \in GL(V)$.

Example 1.4.6. Let $SO(3,1)$ be the Lorentz group; the set of Lorentzian transformation which preserve the origin. Then $\mathbb{R}^4 \rtimes SO(3,1)$ is the Poincare group.

Notice that so far, we have always chosen our normal subgroup to always be abelian. However, this need not be the case. The following example will demonstrate this.

Example 1.4.7 (Braid Groups)**.** Let $B_n = \pi_1((\mathbb{C}^n \setminus \{\text{diags}\})/S_n)$ the fundamental group of this space. To be more precise about what the space is, note that

$$(\mathbb{C}^n \setminus \{\text{diags}\})/S_n = \{(z_1, \ldots, z_n) : \forall i \neq g, z_i \neq z_j\}/S_n$$

Note that taking the modulus by S_n means that we don't care about the order of the elements. The fundamental group tells us how to draw paths in such a space. Consider the set of paths between a set of points $\mathbb{C}_\mathbb{Z}$. Now two paths intercept at the point. This is hard to see in $\mathbb{C}^n$ by itself, so we multiply by $\mathbb{R}$ the time parameter, to visualize how these paths move. Note that the paths on points return to their same initial configuration. Then we modulu out by homotopies. All together, this is the Braid Group on n Strands.

There is another way to visualize this. Denote by σ_1 in which points 1 and 2 switch places. In general, let σ_k denote the configuration in which k and $k+1$ trade places. The braid group is the free group generated by this set, modulo the braid relations as follows

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} : \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| > 1, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \rangle$$

However, we can homomorphically map $\pi : B_n \to S_n$, where $\sigma_i \overset{\pi}{\mapsto} s_i = (i, i+1)$. In such a case, the presentation becomes $s_is_j = s_js_i$ and $s_is_{i+1}s_i = s_{i+1}s_is_{i+1}$. The difference between this braid group and the symmetric group is that the symmetric group also has the relation $\sigma_i^2 = 1$ which is clearly not true in the braid group.

Now let $PB_n = \ker \pi$, where the notation comes from the phrase "pure braids;" braids whose underlying permutation is the identity permutation. Now certainly $PB_n \triangleleft B_n$. We want to be able to write B_n as a semi-direct product of PB_n with another group. At first thought, we might try adding all the permutations, taking care of everything that isn't pure. If this were the case, then both $S_n, PB_n \leq B_n$; however, $S_n \not\leq B_n$. Given $\pi : B_n \to S_n$ we can find a set theoretic inverse $S_n \to B_n$ but not a group theoretic one, since the inverse will not be multiplicative.

Now $PB_{n-1} \hookrightarrow B_n$. Given an $n-1$ braid, we can always make it an n braid by adding a strand that does not interact with the other strands. Similarly, $\rho : PB_n \twoheadrightarrow PB_{n-1}$ by deleting any single strand. Now $\ker \rho \triangleleft PB_n$, so what do elements of $\ker \rho$ look like? Notice that if the first $n-1$ strands are vertical, then regardless of what the final strand does, this will be an element of the kernel, so $\ker \rho = \pi_1 (\mathbb{C} \setminus \{n-1 \text{points}\}) = F_{n-1}$ the free group on $n-1$ generators. This $F_{n-1} \triangleleft PB_n$ and $PB_{n-1} \leq PB_n$. We claim that $F_{n-1} \cap PB_{n-1} = \{e\}$. Furthermore, $F_{n-1} PB_{n-1} = PB_n$. We claim that

$$\begin{aligned} PB_n &= F_{n-1} \rtimes PB_{n-1} \\ &= F_{n-1} \rtimes (F_{n-2} \rtimes PB_{n-2}) \\ &= F_{n-1} \rtimes (F_{n-2} (\cdots \rtimes (F_2 \rtimes F_1))) \\ &= F_{n-1} \rtimes (F_{n-2} (\cdots \rtimes (F_2 \rtimes \mathbb{Z}))) \end{aligned}$$

Recall that we had considered $|G| = 15$ and shown that $P_3, P_5 \triangleleft G$ so $G = C_3 \times C_5 = C_{15}$. Next, let us try $|G| = 21 = 3 \cdot 7$. Now $n_3(G)$ could be 1 or 7. Similarly, $n_7(G) = 1$. So $P_7 \triangleleft G$.

Case 1: If $P_3 \triangleleft G$, then $G = C_3 \times C_7 = C_{21}$ since these are coprime.

Case 2: If $P_3 \not\triangleleft G$ then $G = P_7 \rtimes_\psi P_3$ where $\psi : P_3 \to \mathrm{Aut}(P_7)$ or $\psi : C_3 \to \mathrm{Aut}(P_7)$. Denote by $C_3 = \langle y : y^3 = e \rangle$. Similarly, $P_7 = C_y = \langle x : x^7 = e \rangle$. Let us examine $\mathrm{Aut}(C_7)$. If $\phi \in \mathrm{Aut}(C_7)$ then $\phi(x) = x^i$ for some i. But then $\phi(x^j) = x^{ij}$. Hence ϕ is completely determined by the index i. Furthermore, under automorphisms the image of a generator must be a generator. Hence $|\mathrm{Aut}(C_7)|$ is the number of elements less than 7 coprime to 7, so $|\mathrm{Aut}(C_7)| = 6$. Denote by ϕ_i the automorphism mapping $x \mapsto x^i$. Then $\phi_i \circ \phi_j(x) = \phi_i(x^j) = x^{ij} = \phi_{ij}(x)$ so $\phi_i \circ \phi_j = \phi_{ij}$. So $\mathrm{Aut}(C_7) = (\mathbb{Z}/7)^*$ the multiplicative group of $\mathbb{Z}/7$. In general, $\mathrm{Aut}\,(\mathbb{Z}/p) = (\mathbb{Z}/p)^*$. Later, we will show that $(\mathbb{Z}/p)^* \cong C_{p-1}$. For now however, we can show directly that $(\mathbb{Z}/7)^* \cong C_6$.

Claim: $\mathrm{Aut}(C_7) = \langle \phi_3 \rangle$.

This is easily checked simply by enumerating through ϕ_3^n for $n = 1, \ldots, 6$.

Going back to $\psi : C_3 \to C_6$ we must have that $\psi(y) \in \langle \phi_3 \rangle$ and so $\psi(y)^3 = \phi_1$ the identity element. Hence $\psi(y)$ must be $(\phi_3)^0 = \phi_1$ or $(\phi_3)^2 = \phi_4$ or $(\phi_3)^4 = \phi_4$. Thus there are potentially three groups of the type $G = P_7 \rtimes P_3$ depending on the choice of ψ.

If $\psi(y) = \phi_1$ then $\psi(y)^2 = \phi_1^2 = \phi_1$ so $\psi : P_3 \to \mathrm{id} \in \mathrm{Aut}(P_7)$. In this case $G = P_7 \rtimes P_3 =$

$P_7 \times P_3$ and so again $G = C_{21}$. Note that this is because P_3 is normal in this case. If $\psi(y) = \phi_2$ then $G_2 = C_7 \rtimes_{y \mapsto \phi_2} C_3$. Finally, if $\psi(y) = \phi_4$ then $G_4 = C_7 \rtimes_{y \mapsto \phi_4} C_3$. Hence we've found two non-abelian group of order 21; however, we need to check whether or not they are distinct.

Claim: $G_2 \cong G_4$.

Write $G_2 = \langle x, y : x^7 = y^3 = e, yxy^{-1} = x^2 \rangle$ and $G_4 = \langle x, y : x^7 = y^3 = e, yxy^{-1} = x^4 \rangle$. Define $\lambda : G_2 \to G_4$ by $\lambda(x) = x$ and $\lambda(y) = y^2$. Then

$$\begin{aligned} \lambda(yxy^{-1}) &= \lambda(y)\lambda(x)\lambda(y^{-1}) \\ &= y^2xy^{-2} = y(yxy^{-1})y^{-1} \\ &= yx^4y^{-1} = (yxy^{-1})^4 \\ &= (x^4)^4 = x^2 = \lambda(x^2) \end{aligned}$$

and hence λ maps one relation to the other relation.

Let $|G| = 12 = 2^2 \cdot 3$. Hence the Sylow 2-group has order 4. We claim that at least one of these is normal. Note that $n_2(G) \in \{1, 3\}$. Similarly, $n_3(G) \in \{1, 4\}$. If neither P_2 or P_3 is normal then $n_2 = 3$ and $n_3 = 4$. The intersection of any two distinct Sylow 3-subgroups must be trivial since their intersection must also be a subgroup of both and hence have order dividing 3 which cannot be the case. It follows that G has at least $4 \cdot 2 = 8$ elements of order 3. None of these elements are in any Sylow 2-group since they have coprime order to 4. Including the identity, we have accounted for 9 elements leaving only 3 more elements. However, a single Sylow 2-subgroup has 3 non-trivial elements, so there is room for only one Sylow 2-subgroup.

Group:	$P_3 \triangleleft G, P_2 \triangleleft G$	$P_3 \triangleleft G$ only	$P_2 \triangleleft G$ only
C_4	$G \cong C_4 \times C_3 \cong C_{12}$	$C_4 \to \mathrm{Aut}(C_3)$ $G = C_3 \rtimes_\phi C_4$	Impossible
$C_2 \times C_2$	$G \cong C_2 \times C_2 \times C_3 \cong C_2 \times C_6$	D_{12}	A_4

Note that for C_4 to act on C_2, write $C_4 = \langle y \rangle$ and $\mathrm{Aut}(C_3) = \langle x \rangle$. Then $\phi_y(x) = x^2$.

Claim 1.4.8. $(\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/3 \cong A_4$

Proof. $\mathbb{Z}/2 \times \mathbb{Z}/2$ has 4 elements, the identity $(0, 0)$ and three non-identity elements $(0, 1), (1, 0), (1, 1)$. The action of $\mathbb{Z}/3$ on these elements is then to permute the non-identity elements.

However, recall that we had a mapping $\phi : S_4 \to S_3$ which restricts to $A_4 \to A_3 = \mathbb{Z}/3$. But the kernel of this restriction is $\mathbb{Z}/2 \times \mathbb{Z}/2$. Labelling the indices of the tetrahedron, the kernel is given by $\{(14)(23), (24)(13), (12)(34), e\}$ which is precisely the Klein four group. □

Note in general, if $|G| = pq$ for primes p and q, then we have two cases. If $p \not| q - 1$ then $G = C_p \times C_q$. On the other hand, if $p | q - 1$ then we $G = C_{pq}$ or $G = C_q \rtimes C_p$.

1.5 Solvable Groups

Definition 1.5.1. A group G is solvable if it has Jordan-Hölder decomposition series $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\}$ and all composition factors G_k/G_{k+1} are abelian.

As an example of a group that isn't solvable, consider A_n for $n \geq 5$.

Theorem 1.5.2. *If $N \triangleleft G$ then G is solvable if and only if N and G/N are solvable.*

Theorem 1.5.3. *If $H < G$ and G is solvable then H is solvable.*

Proof. If $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$ is a tower for G, then we claim

$$H = G_0 \cap H > G_1 \cap H > G_2 \cap H > \cdots > G_n \cap H = \{e\}$$

is a tower with abelian factors. We claim the following holds in general:

Claim 1.5.4. *If $H < G$ and $A \triangleleft B < G$ then $H \cap A \triangleleft H \cap B$ and if B/A is abelian then so is $(H \cap B)/(H \cap A)$.*

Proof. We first show normality. Let $x \in H \cap A, y \in H \cap B$. We want to show that $x^y \in H \cap A$. Now $x^y \in H$ since both $x, y \in H$. On the other hand, $x \in A$ and $y \in B$ and $A \triangleleft B$ so $x^y \in A$. Hence x^y is in both H and A so $x^y \in H \cap A$.

To show abelianism, define a map $\phi : \frac{H \cap B}{H \cap A} \to B/A$ as follows: If $x \in H \cap B$ then $[x]_{H \cap A} \overset{\phi}{\mapsto} [x]_A$. This is clearly a homomorphism. To see that ϕ is well defined, notice that if two objects are equivalent in $H \cap A$ then they are certainly equivalent in the bigger equivalence relation of A. To characterize the kernel, assume that $[x]_A = [e]_A$ then $x \in A \cap (H \cap B) = (H \cap A)$ since $A \triangleleft B$ so $[x]_{H \cap A} = e$ so $\ker \phi$ is trivial and ϕ is injective. Thus we can identify $(H \cap B)/(H \cap A)$ with a subgroup of B/A and all subgroups of abelian groups are abelian. □

But this claim tells us that this tower for H is a composition series with abelian factors, so H is solvable as required.

□

Chapter 2

Rings

2.1 Introduction

Definition 2.1.1. A ring is a set R with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ and two special elements $0, 1 \in R$ with $0 \neq 1$, such that for every $a, b, c \in R$ we have

1. $(R, +, 0)$ is an abelian group.
2. The product relation is associative, so $(ab)c = a(bc)$.
3. 1 is the multiplicative identity, so $1 \cdot a = a \cdot 1 = a$.
4. Addition and multiplication are distributive, so $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$.

Note that some people omit the existence of the multiplicative identity in the ring. In such cases, rings with 1 are called unital rings. If R is a commutative ring, then $ab = ba$.

Example 2.1.2. The integers $\mathbb{Z}$ are a ring with standard addition and multiplication. Similarly, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings. In fact, even $\mathbb{Z}/(n)$ are rings.

Example 2.1.3. Let R be a ring and consider $R[x]$ the set of polynomials with coefficients in R. Write

$$R[x] = \left\{ \sum_{i=0}^{d} a_i x^i : a_i \in R, d \in \mathbb{N} \right\}$$

where addition is pointwise in x^i, and multiplication is given by

$$\left[\sum_{i=1}^{d_1} a_i x^i\right]\left[\sum_{j=1}^{d_2} b_i x^j\right] = \sum_{k=0}^{d_1+d_2}\left(\sum_{i=0}^{k} a_i b_{k-i}\right)x^k.$$

Note that since $R[x]$ is again a ring, we can adjoin another variable, say $R[x][y]$. Indeed, it turns out that $R[x][y] \cong R[x,y]$.

Example 2.1.4. The set of $n \times n$ matrices with entries in a ringe R is denoted by $M_n(R)$. This is a ring under the usual operations of matrix addition and multiplication. In particular, if $A = [a_{ij}], B = [b_{ij}]$ then

$$C = [c_{ik}] = AB = \sum_{j=1}^{n} a_{ij}b_{jk}.$$

Note that if R is non-commutative, this is in some sense "doubly"' non-commutative. We know matrix multiplication is non-commutative, but as the ring need not be commutative, we need to be careful about how we perform the multiplication above.

Definition 2.1.5. A quandle is a couple $(Q, \star)$ such that $(a \star b) \star c = (a \star c) \star (b \star c)$. There are other axioms, but this is the important one.

If G is a group then $(G, \star)$ where $\star$ is conjugation, is a quandle. This is because $(a^b)^c = (a^c)^{(b^c)}$. As an exercise, prove that this is true and find further examples (Exam alert!).

Definition 2.1.6. If R, S are rings, a ring homomorphism $\phi : R \to S$ is a set map $\phi : R \to S$ such that

1. $\phi(0_R) = 0_S, \phi(1_R) = 1_S$
2. $\phi(a + b) = \phi(a) + \phi(b)$
3. $\phi(ab) = \phi(a)\phi(b)$

Theorem 2.1.7. *Rings along with ring homomorphisms form a category.*

Example:

1. Consider the map $\mathbb{Z} \to \mathbb{Z}/n$ which maps $k \mapsto k \mod n$. This is a ring homomorphism.
2. Consider the map $R \mapsto R[x]$ by $a \mapsto ax^0$. This is a ring homomorphism and gives us an identification of R in $R[x]$.
3. $R \to M_n(R)$ by $a \mapsto aI_n$ is a ring homomorphism.
4. Consider the evaluation map $\mathrm{ev}_u : R[x] \to R$ which maps $\sum_{i=1}^{n} a_i x^i \mapsto \sum_{i=1}^{n} a_i u^i$. This is a ring homomorphism when $u \in Z(R) = \{x \in R : xy = yx, \forall y \in R\}$ the center of the ring. Indeed, note that if $\sum a_i x^i$ and $\sum b_j x^j$ are two polynomials, then
$$\mathrm{ev}_u\left(\sum a_i x^i\right)\mathrm{ev}_u\left(\sum b_j x^j\right) = \sum_{i,j} a_i u^i b_j u^j, \qquad \mathrm{ev}_u\left(\sum a_i x^i \cdot \sum b_j x^j\right) = \sum_{i,j} a_i b_j u^{i+j}$$
and these are not equal unless we can move the u^i across the b_j.
5. We have already seen two ways of turning a ring R into another ring; that is, by consider the polynomials and the matrices over R. That being said, note that we can combine these to create $M_n(R[x])$ the set of matrices with polynomial entries, and $M_n(R)[x]$ the set of polynomials with matrix coefficients. As a general rule, these objects have very different inherent structures. However, it is clear that we can map these to one another. As a simple example, let $R = \mathbb{Z}$ and
$$\begin{pmatrix} 2x+7 & -3x \\ x^2-2 & 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} x^2 + \begin{pmatrix} 2 & -3 \\ 0 & 0 \end{pmatrix} x + \begin{pmatrix} 7 & 0 \\ -2 & 0 \end{pmatrix}$$
The two maps illustrated above are in fact isomorphisms, and so $M_n(R[x]) \cong M_n(R)[x]$.

Definition 2.1.8. A subring [insert definition here].

Given $\phi : R \to S$ a morphism of rings. Then $\mathrm{im}\,\phi \subseteq S$ is $\mathrm{im}\,\phi = \{y \in S : \exists x \in R, \phi(r) = s\}$, and $\ker\phi \subseteq R$ is $\phi^{-1}(0)$

Definition 2.1.9. For $I \subseteq R$ is an ideal if it is an additive subgroup and $\forall r \in R$ and $\forall s \in I$ we have that $sr \in I$ and $rs \in I$.

Proposition 2.1.10. *1.* $\operatorname{im}\phi$ *is a subring of* S.

2. $\ker\phi$ *is an ideal of* R.

Proof. If $r \in R$ and $a \in \ker\phi$ then

$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0 \tag{2.1}$$

so $ra \in \ker\phi$ and we conclude that $\ker\phi$ is an ideal. □

Question: Given $I \subseteq R$ an ideal in a ring, is there always a morphism $\phi : R \to S$ such that $\ker\phi = I$? The answer is yes, and motivates our definition of ring quotients.

Proposition 2.1.11. *For every ideal* $I \subseteq R$ *there exists a ring homomorphism* $\phi : R \to S$ *such that* $I = \ker\phi$.

Proof. Define $\sim$ on R by $r_1 \sim r_2$ if $r_1 - r_2 \in I$ which is an equivalence relation. Define the set

$$S = R/\sim = \{[r]_I = \bar{r} = r + i : r \in R\} \tag{2.2}$$

Now S is a ring: indeed, it contains $[0]_S = \bar{0}$ and $[1]_S = \bar{1}$. We can define addition in precisely the same sense as in an abelian group, by $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$. Finally, multiplication is defined as $[r_1][r_2] = [r_1 r_2]$, which we now show is well defined. Suppose that $r \sim r'$ and $s \sim s'$ so that $r - r' \in I$ and $s - s' \in I$. Then to show that $[r][s] = [r'][s']$ we notice that $rs - r's = (r - r')s$ which is in I since $r - r' \in I$. □

We note that ring theory draws many analogies to ring theory so far. Indeed, rings also have isomorphism theorems, as we see below.

Theorem 2.1.12 (The Isomorphisms Theorems)**.** *The following are the isomorphism theorems for rings.*

1. First Ring Isomorphism Theorem: *Given two rings R, S and a ring homomorphism $\phi : R \to S$ then $R/\ker\phi \cong \operatorname{im}\phi$.*
2. Second Ring Isomorphism Theorem: *Given that $A \subseteq R$ a subring and $I \subseteq R$ we have that*
$$\frac{A+I}{I} \cong \frac{A}{A \cap I} \tag{2.3}$$
3. Third Ring Isomorphism Theorem: *Let $I \subseteq J \subseteq R$ be ideals, so that*
$$\frac{R/I}{J/I} \cong \frac{R}{J} \tag{2.4}$$
4. Fourth Ring Isomorphism Theorem: *If I is an ideal in R then there is a bijection between ideals in R/I and ideals of R containing I.*

Example 2.1.13.

1. Recall the ring of integers $\mathbb{Z}$ of which $n\mathbb{Z}$ is an ideal. Then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$.
2. Let $A \subseteq R$ be a subset and denote by $\langle A\rangle$ the deal generated by A. Then $\langle A\rangle$ is the smallest ideal containing A and is in the intersection of all ideals containing A. Finally, to see what $\langle A\rangle$ looks like explicitly, note that in order to be closed under addition, we need to take finite sums of elements. That is,
$$\langle A\rangle = \left\{ \sum_{i=1}^{n} r_i a_i r_i' : a_i \in A, r_i, r_i' \in R, n \in \mathbb{N} \right\} \tag{2.5}$$
3. Consider the quotient $\mathbb{R}[x]/\langle x^2+1\rangle$. It turns out that this is a very well known ring and to do this we will use the first isomorphism theorem. Take $R = \mathbb{R}[x]$ and $S = \mathbb{C}$. Let $\phi = \mathrm{ev}_i$ be the evaluation morphism so that $\sum_k a_k x^k \mapsto \sum_k a_k i^k$. Now the kernel of this homomorphism is
$$\ker\phi = \left\{ f \in \mathbb{R}[x] : f(i) = 0 = \overline{f(i)} = f(\bar{i}) = f(-i) \right\} \tag{2.6}$$
But then we see that $x - i \,\middle|\, f, x+i \,\middle|\, f$ and so it follows that $(x-i)(x+i) \,\middle|\, f$. Hence $x^2+1 \,\middle|\, f$ which implies that $f \in \langle x^2+1\rangle$ so $\ker\phi = \langle x^2+1\rangle$. Finally, it is simple to see that ϕ is surjective, and so by the first isomorphism theorem for rings tells us that
$$\mathbb{R}[x]/\left\langle x^2+1\right\rangle \cong \mathbb{C} \tag{2.7}$$

Definition 2.1.14. If R is commutative and $R^* = R \setminus \{0\}$ is a group, we say that R is a field.

Definition 2.1.15. If R^* is a group but R is not necessarily commutative, then we say R is a division ring.

Example 2.1.16. The real Quaternions are denoted by $\mathbb{H}$ and are given by

$$\mathbb{H} = \{a + ib + jc + kd : a, b, c, d \in \mathbb{R}\}. \tag{2.8}$$

The basis elements satisfy $i^2 = j^2 = k^2 = 1$ but $ij = k, jk = i, ki = j$. The multiplication law follows from associativity and linearity of $\mathbb{R}$, and is well-defined and consistent by utilizing the basis-relations above. Alternatively, we can associate $\mathbb{H} = \mathbb{R} \times \mathbb{R}^3$ with representation (α, v) where $\alpha \in \mathbb{R}$ and $v \in \mathbb{R}^3$. Then the multiplication law is

$$(\alpha, v) \cdot (\beta, w) = (\alpha\beta - v \cdot w, \alpha v + \beta w + v \times w). \tag{2.9}$$

Now we claim that this is a division ring. Recall that in the complex numers, if $z = a + ib$ then $\bar{z} = a - bi$ and so $z\bar{z} = a^2 + b^2$ and so $z\frac{\bar{z}}{a^2+b^2} = 1$ so $z^{-1} = \frac{\bar{z}}{a^2+b^2}$. In $\mathbb{H}$, we set $z = a + bi + cj + dk$ and $\bar{z} = a - bi - cj - dk$, and a similar procedure tells us that $z^{-1} = \frac{\bar{z}}{a^2+b^2+c^2+d^2}$.

From this point on, R is commutative unless otherwise explicitly stated.

Definition 2.1.17. Let R be a ring. If $a \neq 0$ and there exists a $b \neq 0$ such that $ab = 0$ then we say that a is a *zero divisor*.

Definition 2.1.18. R is an integral domain (or sometimes just a domain) if whenever $a, b \in R$ satisfy $ab = 0$ implies that one of a or $b = 0$. That is, R is an integral domain if and only if it has no zero divisors.

We note that this is really an "if and only if" statement, although the converse direction is not particularly interesting. Note that in such a domain, if $ab = ac$ and $a \neq 0$ then $b = c$. Indeed, if $ab = ac$ then $ab - ac = a(b - c) = 0$. But since $a \neq 0$ we must have $b - c = 0$ so $b = c$ as required.

Example 2.1.19.

1. Note that every field or division ring is an integral domain.
2. The integers $\mathbb{Z}$ are an integral domain.
3. If R is a domain then so is $R[x]$
4. Note that $\mathbb{Z}/n$ is not an integral domain if n is not prime.

2.2 Prime and Maximal Ideals

2.2.1 Maximal Ideals

Definition 2.2.1. An ideal $I \subseteq R$ is *maximal* if $I \neq R$ and whenever $I \subseteq J \subseteq R$ then $I = J$ or $J = R$.

Lemma 2.2.2. *A ring F is a field if and only if it has no proper non-trivial ideals.*

Proof. Let F be a field and J an ideal. If $J = \{0\}$ we are done, so assume $J \neq 0$. Let $a \in J$, and note then that $1 = aa^{-1} \in J$ which implies that $J = R$.

Conversely, assume that F has no proper non-trivial ideals. If $a \neq 0$ then $I = \langle a \rangle$ must be the whole ring F, and so in particular, $\exists b \in F$ such that $ab = 1$ so a has an inverse. Since a was arbitrary, F is a field. □

Theorem 2.2.3. *If R is a ring and M is an ideal then R/M is a field if and only if M is maximal.*

Proof. A field F is a ring whose only ideals are $\{0\}$ and F itself. Hence if R/M is a field, let $M \subseteq J$ be any other ideal. Notice then that either J/M is an ideal of R/M. But R/M is a

field, so either $J/M = M$ or $J/M = R/M$ which means that either $J = M$ or $J = R$ and so J is maximal. Conversely, if I is maximal, notice that R/M has no proper non-trivial ideals, and hence must be a field. □

Alternate Proof. ($\Rightarrow$) Suppose J is a proper, strictly larger ideal than I so that $I \subsetneq J$. Choose $a \in J \setminus I$ then $[a]_i \neq 0$ in R/I so $\exists b \in R$ such that $[b][a] = [a]$ since R/I is a field. This implies that $ab - 1 \in I$, so that $\exists c \in I$ with $1 = ab - c$. However, $ab \in J$ and $c \in I \subset J$ so $J = R$ a contradiction.

($\Leftarrow$) Assume that $[a] \in R/I$ such that $a \notin I$. Let $J = \langle a \rangle + I$. Now $I \subsetneq J$ but I is maximal so $J = R$. Hence we can write $1 = ba + c$ for $b \in R, c \in I$. But then $[1] = [b][a]$ and so we have found an inverse for $[a]$. Since a was arbitrary, R/I is a field. □

Example 2.2.4.

1. Note that if p is a prime, then $p\mathbb{Z} \subseteq \mathbb{Z}$ is maximal and so $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p$ is a field.
2. Consider the ideal $\langle x^2 + 1 \rangle$. This is maximal in $\mathbb{R}[x]$ since the quotient $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$ which is a field.
3. Let $S = \ell^\infty$ the set of bounded sequence of $\mathbb{R}$. Define for each $n \in \mathbb{N}$ the ideal $I_n = \{\{a_i\}_{i=1}^\infty : a_n = 0\}$. We claim that I_n is maximal, since $S/I_n \cong \mathbb{R}$. One can see this explicitly by taking the map $\phi : S \to \mathbb{R}$ mapping $\{a_i\}_{i=1}^\infty \mapsto a_n$. This is a surjective ring homomorphism whose kernel is I_n.

We recall that a partially ordered set is couple $(X, \leq)$ where X is a set and $\leq$ is a binary relation, where $\leq$ is transitive, transitive, and symmetric. However, note that not every pair of elements can be compared (hence the terminology "partially" ordered). A chain of a poset is a collection $C \subseteq X$ such that every element can be compared. A chain is bounded if $\exists z \in C$ such that $z \geq x$ for all $x \in C$. Finally, a maximal element of a poset if an element m such that $\forall x \in X$ if $x \geq m$ then $x = m$.

Lemma 2.2.5 (Zorn's Lemma)**.** *In a partially ordered set, if every chain is bounded, then there exists a maximal element.*

Note that the axiom of choice implies Zorn's Lemma.

Theorem 2.2.6. *Every ideal is contained in a maximal ideal.*

Proof. Let $I \subseteq R$ be an ideal in a ring and set

$$X = \left\{ J : \begin{array}{c} J \subseteq \mathbb{R} \text{ is an ideal} \\ I \subseteq J \subsetneq R \end{array} \right\}. \tag{2.10}$$

Now X is a partially ordered set under inclusion. For a fixed chain $\mathcal{C}$, define $J = \bigcup_{I\in\mathcal{C}} I$ then J is an upper bound for $\mathcal{C}$ and is itself an ideal, so $\mathcal{C}$ is bounded. By Zorn's lemma, there is a maximal element in X, and this element is the ideal we wanted. □

Example 2.2.7. Consider $S = \ell^\infty$ and let I be the set of sequence that vanish beyond a certian point. More explicitly

$$I = \{\{a_n\}_{n=1}^\infty : \exists N \in \mathbb{N}, \forall i \geq N a_i = 0\}. \tag{2.11}$$

Clearly this is not a maximal ideal, since it is contained in many other proper ideals in which this is contained. For example, the set of sequences which converge to zero, the set of sequences at which, beyond a certain point all even indices are zero, etc. However, by Theorem 2.2.6 there must exist a maximal ideal $I \subset J \subset S$.

Claim 2.2.8. *1. It is necessary that $S/J \cong \mathbb{R}$.*

2. If we denote by the projection map $\operatorname{Lim} : S \to S/J$ so that $\operatorname{Lim} : \ell^\infty \to \mathbb{R}$. Then Lim satisfies

$$\operatorname{Lim}(a_n + b_n) = \operatorname{Lim} a_n + \operatorname{Lim} b_n, \qquad \operatorname{Lim}(a_n b_n) = \operatorname{Lim}(a_n) \cdot \operatorname{Lim}(b_n). \tag{2.12}$$

3. If $\{a_i\} \in I$ is eventually 0, then $\operatorname{Lim} a_n = 0$. If $\lim a_n = \alpha$ then in $\mathbb{R}$ then $\operatorname{Lim}(a_n) = \alpha$.

2.2.2 Prime Ideals

Definition 2.2.9. An ideal $P \subseteq R$ is called *prime* if whenever $ab \in P$ then $a \in P$ or $b \in P$.

Theorem 2.2.10. *An ideal $P \subseteq R$ is prime if and only if R/P is a domain.*

Proof. ($\Rightarrow$) Assume that P is a prime ideal, and consider $[a][b] = 0$ in R/P. We want to show that one of a or b must be zero, so that R/P has no zero divisors. However, for $[a][b] = 0$ is R/P means that $ab \in P$ and since P is prime then either a or b is in P. Projecting back into the quotient space, we see that either $[a]$ or $[b]$ is zero in R/P.

($\Leftarrow$) Conversely, assume that R/P is a domain. Let $ab \in P$ and note that in the quotient space $[ab] = [a][b] = 0$. However, since R/P is a domain then either $[a]$ or $[b] = 0$. Without loss of generality, assume that $[a] = 0$. But then $a \in P$ and we are done. □

Theorem 2.2.11. *Every maximal ideal is prime.*

Proof. We note that every field is a domain, and so we are done. □

Example 2.2.12. Consider $\mathbb{Z}[x]$ and consider $P = (x)$ which is an ideal. Then $\mathbb{Z}[x]/P = \mathbb{Z}[x]/(x) \cong \mathbb{Z}$ which is a domain but not a field, so P is prime but not maximal.

2.3 Between Fields and Domains

From here onwards, R is a domain unless stated otherwise.

2.3.1 Divisibility/Euclidean Domains

Definition 2.3.1. If R is a domain and $a, b \in R$ then we say that a *divides* b and write $a \mid b$ if $\exists c \in R$ such that $ac = b$.

Proposition 2.3.2. *If $a \mid b$ and $b \mid a$ then $a = ub$ where u is a unit of R.*

Proof. By hypothesis and definition, we know $\exists c, d \in R$ such that $ac = b$ and $bd = a$. Hence we can write $a = bd = acd$. Since we are in a domain, we are able to cancel and so $1 = cd$ so both c and d are units, and the result follows. □

When a and b are equal up to a unit, then we can write $a \sim b$. This is an equivalence relation and we say that a and b are associated.

Definition 2.3.3. Given two elements $a, b \in R$ we say that q is a *greatest common divisor* of a and b if

1. $q \mid a$ and $q \mid b$.
2. If $c \mid a$ and $c \mid b$ then $c \mid q$.

Note that we have made no statement about the existence of a greatest common divisor. We recall that in the integers such a number always exists, and we will see special cases in which it always exists.

Proposition 2.3.4. *A greatest common divisor, if it exists, is unique up to association. More precisely, if q and q' are both greatest common divisors of $a, b \in R$ then $q' = uq$ where $u \in R^*$.*

Proof. Since q and q' are both greatest common divisors then $q \mid q'$ and $q' \mid q$ and so $q \sim q'$ as required. □

We recall that in the integers, we say that p is a prime if it has no non-unit divisors. This number has the property that if it divides a product of two elements, it must divide one of the two elements. We will see that in general, it is more prudent to use this "property" of the primes in $\mathbb{Z}$ as a definition, from which the divisability property will be shown as a result.

Definition 2.3.5. If $p \in R$ is non-zero and non-unit, then we say that p is *prime* if whenever $p \mid ab$ then $p \mid a$ or $p \mid b$.

Note that $p \mid ab$ is equivalent to saying that $ab \in (p)$. Then by the above definition, if p is a prime we must have that either $a \in (p)$ or $b \in (p)$. Thus $p \in R$ is prime if and only if (p) is a prime ideal.

Definition 2.3.6. A non-zero, non-element $x \in R$ is *irreducible* if whenever $x = ab$ then either a or b is a unit.

Theorem 2.3.7. *All primes are irreducible.*

Proof. Suppose that p is prime and $p = ab$. Then $p \mid p = ab$ and since p is prime either $p \mid a$ or $p \mid b$. Without loss of generality assume that $p \mid a$. Then $a = pc$ for some $c \in R$. Substituting this back into our expression for p we get that

$$p = ab = (pc)b = pcb. \tag{2.13}$$

Since cancellation holds in integral domains, we have that $cb = 1$ and so b is a unit. □

Note however that not all irreducibles are prime. The following is an example of why this is the case.

Example 2.3.8. Let $R = \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\} \cong \mathbb{Z}[x]/(x^2 + 5)$. This ring behaves somewhat like the complex numbers, in that it contains "conjugates" and a "norm." Indeed, define

$$\overline{a + b\sqrt{-5}} = a - b\sqrt{-5}, \qquad \left\|a + b\sqrt{-5}\right\|^2 = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2. \tag{2.14}$$

It is easily shown that $\|ab\| = \|a\| \, \|b\|$. We claim that 2 is irreducible but not prime. Indeed, suppose that $2 = z_1 z_2$ so that $2 = \|2\| = \|z_1\| \, \|z_2\|$. However, we see that the norm is always an integers, and so one of z_1 or z_2 must have norm 1 and hence be a unit. This implies that 2 is irreducible.

On the other hand, 2 is not prime. Indeed, we see that

$$2 \mid 6 \Rightarrow 2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{2.15}$$

but 2 does not divide $1 \pm \sqrt{-5}$ so it cannot be prime.

2.3.2 Unique Factorization Domains

Definition 2.3.9. A ring R is a unique factorization domain (UFD) if every non-zero element in R can be factored as a product of primes. More precisely, if $x \neq 0$ then $\exists p_1, \ldots, p_n$ primes such that $x = up_1 \cdots p_n$ where u is a unit.

Theorem 2.3.10. *Such a decomposition is unique up to units and a possible permutation of indices.*

Proof. We shall for the moment exclude the unit as it will appear later. Assume that we have two representations of x given by

$$x = up_1 \cdots p_n = vq_1 \cdots q_m \tag{2.16}$$

where p_i and q_j are primes, u and v are units, and assume that $m \geq n$. Now $p_1 \mid x$ and so $p_1 \mid q_1 \cdots q_m$. However, since p_1 is prime, it must divide one of the q_i. By re-arranging if necessary, we can assume that $i = 1$ so that $p_1 \mid q_1$. Since p_1 is also irreducible, $p_1 \sim q_1$ and so $p_1 = u_1 q_1$. Since we are in a domain, we can cancel the q_1 leaving us with

$$x = uu_1 p_2 \cdots p_n = vq_2 \cdots q_m. \tag{2.17}$$

We can continue this process until we exhaust the left hand side. Note that there cannot be any additional terms remainins when we are done, since otherwise there is some s such that $q_s \cdots q_m = 1$ which implies at least one of these elements is a unit, contradicting the fact that they are primes. Hence $m = n$ and the p_i are equal to the q_i up to association. □

Theorem 2.3.11. *1. In a unique factorization domain, an element is a prime if and only if it is irreducible.*

2. A ring R is a unique factorization domain if and only if every non-zero element has a unique decomposition into irreducibles.

Proof. 1. We already know that all primes are irreducible so it is sufficient to show that that all irreducibles are prime. Let $x \in R$ be irreducible, so that it has a factorization of length one into primes. This implies that x is prime.

2. If R is a UFD, clearly it has a unique decomposition into primes, which are irreducible. Conversely, assume that every element of has a decomposition into irreducibles. It is sufficient to show that every irreducible is prime. Suppose that $x \in R$ is irreducible and that $x \mid ab$. By hypothesis, we can write

$$a = \prod_i a_i, \qquad b = \prod b_i, \tag{2.18}$$

where the a_i and b_i are irreducible. Then $\exists z$ such that $xz = ab = \prod_i a_i \prod_j b_j$. But then the element xz has two decompositions; namely, the one arising from ab and the one arising for xz. Since all factorizations are unique and x is irreducible, either $x = a_i$ or $x = b_j$ for some i and j. In either case, either $x \mid a$ or $x \mid b$ and so x is prime.

□

Recall that $q \in \gcd(a, b)$ is a member of the set of all greatest common divisors of a, b if $q \mid a$ and $q \mid b$ and if r divides both a and b then $r \mid q$. We have shown that if a greatest common divisor exists, it must be unique up to association and say that $q = \gcd(a, b)$.

Proposition 2.3.12. *In a unique factorization domain, the greatest common divisor always exists.*

Proof. Let R be a unique factorization domain and choose $a, b \in R$. We can write $a = \prod_i p_i^{s_i}, b = \prod_i p_i^{t_i}$, where $s_i, t_i \geq 0$ and the set of primes are the same. Define $q = \prod_i p_i^{\min(s_i, t_i)}$, for which it is an exercise to check that q satisfies all the criteria for a greatest common divisor. □

2.3.3 Euclidean Domains

Definition 2.3.13. A ring R is a Euclidean domain if it has a "Euclidean valuation," where a Euclidean valuation is a function

$$e : R \setminus \{0\} \to \mathbb{N}, \tag{2.19}$$

satisfying

1. For all $a, b \in R$ we have $e(ab) \geq e(a)$ and $e(ab) \geq e(b)$.
2. For all $a, b \in R \setminus \{0\}$, there exists $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $e(b) < e(r)$.

Example 2.3.14.

1. The integers $\mathbb{Z}$ are a Euclidean domain with the standard Euclidean norm $|\cdot|$.
2. Let F be a field and define $R = F[x]$. Then $F[x]$ is a Euclidean domain with valuation $e(f) = \deg f$.

2.3.4 Principal Ideal Domains

Definition 2.3.15. A ring R is a *principal ideal domain* (PID) if every ideal in R is "principal." That is, every ideal of R is generated by a single element.

Theorem 2.3.16. *A Euclidean domain is always a principal ideal domain.*

Proof. If I is an ideal in a Euclidean domain (R, e). Let x be an element of I with minimal norm. We claim that $\langle x \rangle = I$ which would show that I is principal. Note that since $x \subseteq I$ then $\langle x \rangle \subseteq I$. On the other hand, let $y \in I \setminus 0$ and take $q, r \in R$ such that $y = qx + r$ since R is a Euclidean domain. Now either $r = 0$ or $e(r) < e(x)$. However, notice that $r = y - qx \in I$ so $r = 0$ since x is minimal amongst all elements of I. Thus $y = qx$ so $y \in \langle x \rangle$ and $I \subseteq \langle x \rangle$ as required. □

Proposition 2.3.17. *In a principal ideal domain, every prime ideal is maximal.*

Proof. For the sake of contradiction, assume that I is prime but not maximal; that is, there exists a non-trivial proper ideal $J \supsetneq I$. Since we are in a principal ideal domain, it must be the case that $I = (p)$ for some prime element $p \in R$. Similarly $J = (x)$ for some $x \in R$. Since $I \subsetneq J$ then $p \in (x)$ so $p = ax$, but p is prime and hence irreducible so either a is a unit or x is a unit. If a is a unit, then $(x) = (p)$ a contradiction. If x is a unit then $J = R$ a contradiction. □

Our final goal will be to show that all PIDs are UFDs. In order to do this, we will use the fact that all PIDs are actually Noetherian domains.

Definition 2.3.18. R is Noetherian if every increasing chain of ideals terminates: R satisfies the ascending chain condition. More precisely, if $I_1 \subset I_2 \subset I_3 \subset \cdot$ then this chain stabilizes, so that $\exists N \in \mathbb{N}$ satisfying $\forall n \geq N, I_n = I_{n+1}$.

Theorem 2.3.19. *Every principal ideal domain is Noetherian.*

Proof. Suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an ascending chain, and set $I = \bigcup_{n=1}^{\infty} I_n$. Now I is an ideal, and if $I = R$ then $1 \in I$. If this is the case, there exists some finite index n such that $1 \in I_n$ and so the chain stabilizes. Thus assume that $I \neq R$, and let $I = (a)$ for some $a \in R$. Now $a \in I_N$ for some finite index N, an dso $x \in I_n$ for every $n \geq N$ which implies that $I_n \supseteq (x) = I$ and so the chain stabilizes. □

Theorem 2.3.20. *All principal ideal domains are unique factorization domains.*

Proof. Let $x = x_1$ be a non-zero element of a principal ideal domain. Unless $x_1 \in R^*$ we can find a maximal ideal $M_1 = (p_1)$ containing (x_1) where p_1 is prime. Now $x_1 = px_2$ for some x_2. Unless $x_2 \in R^*$ we can find a maximal ideal $M = (p_2)$ for some prime p_2 containing x_2. Now $x_2 = p_2x_3$. We can continue by induction.

If this process terminates, then $x_{n+1} \in R^*$ for some n and

$$x_1 = p_1 \cdots p_n x_{n+1} \tag{2.20}$$

but x_{n+1} must be a unit for termination, so $x = x_1$ has a factorization into primes. On the other hand, since $x_i = px_{i+1}$ then $(x_i) \subset (x_{i+1})$ and so we get an infinite chain of ideals

$$(x_1) \subset (x_2) \subset (x_3) \subset \cdots . \tag{2.21}$$

This chain is actually strict, since if $(x_n) = (x_{n+1})$ then $x_{n+1} \in (x_n)$ and so $x_{n+1} = ax_n = ap_n x_{n+1}$ so $ap = 1$ since we are in an integral domain. This implies that p is a unit, which is a contradiction. But a principal ideal domain is Noetherian so this cannot happen and we are done. □

In a PID, we have that $(\gcd(a, b)) = (a, b)$ and so $\gcd(a, b) = sa + tb$ for some $s, t \in R$. Indeed, suppose that $(q) = (a, b)$. Then $a \in (a, b) \in (q)$ so $q \,\Big|\, a$. Similarly, $q \,\Big|\, b$. Now assume that q' satisfies $q' \,\Big|\, a$ and $q' \,\Big|\, b$ then q' divides any linear combination of a and b so it divides any element of $(a, b) = (q)$ so $q' \,\Big|\, q$ and we conclude that $(q) = (\gcd(a, b)) = (a, b)$.

Furthermore, in any Euclidean domain there is a practical way to find the coefficients s, t such that $\gcd(a, b) = as + tb$, termed the *Euclidean algorithm.* Fix $a, b \in R$ and without loss of generality assume that $e(a) \geq e(b)$ for a Euclidean valuation e. Write $a = qb + r$ where either $r = 0$ or $e(r) < e(b)$. If $r = 0$ then $(a, b) = (b)$ and so

$$\gcd(a, b) = b = 0 \cdot a + 1 \cdot b \tag{2.22}$$

and we are done. Now $a = qb + r \in (b, r)$ so $(a, b) \subseteq (b, r)$. On the other hand, $r = a - qb \in (a, b)$ so $(b, r) \subseteq (a, b)$. Both inclusion imply that $(a, b) = (b, r)$. However (b, r) has a smaller sum of norms, and so $(q) = (a, b) = (b, r)$ implies that $\exists s', t' \in R$ satisfying

$$q = s'b + t'r = s'b + t'(a - qb) = t'a + (s' - qt')b \tag{2.23}$$

so defining $s = t'$ and $t = s' - qt'$ gives the desired coefficients.

Finally, R is a principal ideal domain if and only if *Dedekin-Hasse* valuation. Such a valuation is a function $d : R \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ such that if $a, b \neq 0$ then either $a \in (b)$ (that is, $b|a$) or there exists $x \in (a, b)$ non-zero such that $d(x) < d(b)$. Notice that by saying $x \in (a, b)$ we mean that x can be an arbitrary linear combination of a and b. This is in contrast to the Euclidean algorithm, in which case x satisfies the property of the remainer but we demand that the remainder has the form $a + b(-q)$ (forcing the coefficient of a to be one).

The proof of this fact is as follows. Note that if the ring has a Dedekind-Hasse norm we proceed as in the proof that Euclidean domains are PIDs by taking a an element of minimal order for an arbitrary ideal I. Conversely, given $x \in R$ we write $x = \prod_{i=1}^{n} p_i$ a product of

primes. Define $d(x) = 2^n$. Now d is easily seen as multiplicative: $d(ab) = d(a)d(b)$. More importantly, d is a Dedekind-Hasse valuation. Indeed, if $a, b \neq 0$ let $q = \gcd(a, b)$ so that $(q) = (a, b)$. If $b|a$ we are done. Otherwise, write $a = \prod_i p_i^{s_i}$ and $b = \prod_i p_i^{t_i}$ and for some k we must have $t_k > s_k = \min(s_k, t_k)$ and $t_i \geq \min(s_i, t_i)$. Then

$$d(b) = 2^{\sum t_i} > 2^{\sum \min(s_i, t_i)} = d(q). \tag{2.24}$$

Chapter 3

Modules

3.1 Introduction

Definition 3.1.1. A *left R-module* M is an Abelian group with a product $R \times M \to M$ mapping $(r, m) \to rm$ that satisfies the following properties:

1. $1 \cdot m = m$ for all $m \in M$.
2. $a(bm) = (ab)m$ for all $a, b \in R$ and $m \in M$.
3. $(a + b)m = am + bm$ for all $a, b \in R$ and $m \in M$.

There was no particular reason why we have chosen to define left R-modules above. We could also define a *right R-module* when the action is given by $M \times R \to M$.

Example 3.1.2.

1. A vector space over a field is a module. The ring is just the field.
2. Any abelian group A is a module over $\mathbb{Z}$. This is done by defining $\mathbb{Z} \times A \to A$ by $na = \underbrace{a + a + \cdots + a}_{n-\text{times}}$.
3. Suppse that V is a vector space over a field F and $T : V \to V$ is a linear map. Then V is also a module over $F[x]$ by

$$(\sum a_i x^i)v = \sum a_i T^i(v). \tag{3.1}$$

The converse is also true. Namely, if M is a module over $F[x]$ for F a field, then it will be of the above form. This can be done by defining a map $T : x \mapsto sv$.

4. If I is an ideal of R then I and R/I is an R-module.
5. Let $R = M_n(S)$ over a ring S so that S^n is a left-R-module. And $(S^n)^T$ is a right-R-module.

Theorem 3.1.3. *The set of left R-modules forms a category. Similarly, the set of R-modules forms a category.*

Definition 3.1.4. If M and N are left R-modules, then $\phi : M \to n$ is an R-module homomorphism if ϕ is an abelian group homomorphism and $\phi(rm) = r\phi(m)$.

Definition 3.1.5. A submodule is N of M is a subset of M that is still a module under the action of R. If $\phi : M \to N$ is a module homomorphism, then

$$\ker \phi = \{m \in M : \phi(m) = 0\}, \qquad \operatorname{im} \phi = \{\phi(x) : x \in M\} \tag{3.2}$$

and if A is a submodule of M then M/A is a submodule, where the quotient is taken as abelian groups.

Theorem 3.1.6.
1. *If $\phi : M \to N$ is a module homomorphism, then $M/\ker \phi \cong \operatorname{im} \phi$.*
2. *If $A, B \subseteq M$ then $\dfrac{A+B}{A} = \dfrac{B}{A \cap B}$.*
3. *If $A \subseteq B \subseteq M$ then $\frac{M/A}{B/A} \cong M/B$.*
4. *If $A \subseteq M$ then there is a bijective correspondence between submodule of M/A and submodules of M containing A.*

Again, since M is really an abelian group these theorems come from their equivalence theorems for abelian groups. All that needs to be checked is that these morphisms preserve scalar multiplication.

Definition 3.1.7. Let M and N be R-modules. Then the *direct sum* of M and N is

1. $M \oplus N = \{(m, n) : m \in M, n \in N\}$ where $r(m, n) = (rm, rn)$.
2. The direct sum is the coproduct in the category of modules. That is, the direct sum is endowed with two morphisms $i_M : M \to M \oplus N$ and $i_N : N \to M \oplus N$ satisfying the following universal property: For all R-modules P and morphisms $\phi_1 : M \to P$ and $\phi_2 : N \to P$ there exists a unique morphism $\sigma : M \oplus N \to P$ such that the diagram commutes.
3. The direct sum is also a product of modules. For every R module P and morphisms $\phi_A : P \to A$ and $\phi_B : P \to B$ then there exists a unique morphism $\sigma : Z \to A \times B$ such that the diagram commutes.

These definitions can be extended to a finite collection of modules, in which case the latter two definitions are still equivalent. However, in the eventt that we allow infinite collections, Definition 2 is called the direct sum, and Definition 3 is called the direct product and the definitions are no longer equivalent.

Note now that $\mathrm{Hom}(M \oplus N, P) = (\phi_1, \phi_2)$ while $\mathrm{Hom}(P, M \oplus N) = \begin{pmatrix} \varphi_1 : P \to M \\ \varphi_2 : P \to N \end{pmatrix}$ More generally,

$$\mathrm{Hom}\left(\bigoplus_{j=1}^{\nu} N_j, \oplus_{i=1}^{\mu} M_i\right) = \{A \in M_{\mu\times\nu}(R) : a_{ij} \in \mathrm{Hom}(N_j, M_i)\}. \tag{3.3}$$

3.2 Finitely Generated Modules

The Jordan Canonical form is essentially Gaussian elimination done on principal ideal domains. What we will show is that there is a surjective map from the set of matrices to the set of finitely generated modules, modulo an equivalence relation relating row and column operations.

$$\{\text{matrices}\} / \sim \twoheadrightarrow \left\{ \begin{array}{c} \text{finite generated} \\ \text{modules} \end{array} \right\}.$$

We make no assumption in these instances about "finiteness" of the matrices, though this will not significantly impact our work.

Definition 3.2.1. An R-module M is finitely generated if $\exists g_1, \dots, g_n \in M$ such that

$$M = \left\{ \sum_i a_i g_i : a_i \in R \right\}. \tag{3.4}$$

That is, the set of R-linear combinations of the elements $g_1, \dots, g_n$.

Note that we make no assumption on the number n, which is not unique for general modules. Note that given a finitely generated module on n elements, there is a surjective map $R^n \twoheadrightarrow M$ corresponding to the components of R. If we think of R^n as a column vector with components of R, this map acts as

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_{i=1}^{n} a_i g_i.$$

By the first isomorphism theorem, we see that $M \cong \operatorname{im} \pi \cong R^n / \ker \pi$ where $\ker \pi \subseteq \mathbb{R}^n$. Let X be a generated set for $\ker \pi$ so that

$$\ker \pi = \left\{ \sum a_x x : x \in X, a_x \in R \right\}. \tag{3.5}$$

Such a set X always exists, since we can always take $X = \ker \pi$. For a general set X, we can define

$$R^{\oplus X} = \{ \alpha : X \to R : \alpha(n) \neq 0 \text{ for finitely many } n \}.$$

We can thus get a mapping

$$R^X \xrightarrow{A} R^n \xrightarrow{\pi} M$$

where $A(b) = \sum_{x \in X} b(x)x$. Thus one can think of the map $A \in M_{n \times |X|}(R)$, a $n \times |X|$ matrix with elements in R but with the added condition that in each row, there are only finitely many non-zero entries (also known as *row-finite*). To see this, realize that such a matrix is a function $A : \{1, \dots, n\} \times X \to R$ by setting $A_{ix} = x_i$ in which case

$$[A(b)]_i = \sum b(x) \cdot x_i = \sum A_{ix} b(x). \tag{3.6}$$

Suppose then that we had the following commutative diagram

$$\begin{array}{ccccc} R^X & \xrightarrow{A} & R^n & \longrightarrow & M_A = \dfrac{R^n}{\operatorname{im} A} \\ \uparrow{\scriptstyle Q} & & \downarrow{\scriptstyle P} & & \\ R^X & \xrightarrow{A'} & R^n & \longrightarrow & M_{A'} = \dfrac{R^n}{\operatorname{im} A} \end{array}$$

where Q, P are invertible. Then in this situation, $M_A \cong M_{A'}$. Indeed, let $\Phi : M_A \to M_{A'}$ as follows: For some $[\alpha]_{\operatorname{im} A} \in R^n$ let $\Phi\left([a]_{\operatorname{im} A}\right) = [P\alpha]_{\operatorname{im} A'}$. This map is well defined: if $[\alpha]_{\operatorname{im} A} = 0$ then $\alpha \in \operatorname{im} A$ so $\alpha = A\beta$ for some $\beta \in R^X$. Let $\gamma = Q^{-1}\beta$, so that

$$P\alpha = PA\beta = PAQQ^{-1}\beta = PAQ\gamma = A'\gamma.$$

Hence $[P\alpha]_{\operatorname{im} A'} = 0$ so the map is well-defined.

3.2.1 Fundamental Theorem of Finitely Generated Modules over Principal Ideal Domains

Over $\mathbb{Z}$ take a matrix $A \in M_n(\mathbb{Z})$ and pinpoint the value a which has the smallest absolute value which can be attained by doing row and column operations. Without loss of generality, we may assume that a is in the upper left corner, since otherwise we can just move it there. Now a must divide all elements in its rows and columns. Indeed, note that if it divide all such elements, there would be an element b such that $b = aq + r$ with $0 < |r| < |a|$ and we could attain r by appropriate row operations. Since a divides everything in its rows and columns, we can remove all these elements with appropriate row and column operations.

We may now assume that the $(2, 2)$ entry is divisble by a, since otherwise we can add the second row the first row and repeat the process. By continuing inductively, we may conclude that every matrix over $\mathbb{Z}$ can be reduced to a matrix of the form

$$\begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_n & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

where $a_1 | a_2 | a_3 | a_4 | \cdots$. This is known as the *Smith Normal Form*.

Given a matrix $A \in M_{n \times |X|}(R)$ how far can we go by taking $A \mapsto A' = PAQ$ where $P \in M_n(R)$ is invertible and $Q \in M_{|X|}(R)$ is a column-finite invertible? Note that permutation matrices are invertible and swap rows and columns. The matrix $a_{ij}(b)$ which is identity plus b in the (i, j) position is invertible, and adds a multiple of b times a row/column to a row/column. Finally, we can take an identity matrix plus a row containing arbitrary things, which is still invertible. That is, $\displaystyle\sum_{\substack{i=1 \\ i \neq j}}^{|X|} a_{ij}(b_i)$ is invertible and will add a multiple of column j to column i for all i.

Let a be the smallest element (minimal in the Dedekind-Hasse norm; that is, the least number of primes in its factorization) in all matrices reachable from A of the form PAQ. Without loss of generality, $a = a_{11}$. We claim that a divides every entry in the first row and column. Indeed, fix some b in a row or column of A and set $q = \gcd(a, b)$ so that $q = sa + tb$ for some $s, t \in R$. Then

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} s & -\frac{b}{q} \\ t & \frac{a}{q} \end{pmatrix} = \begin{pmatrix} q & 0 \end{pmatrix}.$$

The determinant of this matrix is 1 and so its inverse is given by

$$\begin{pmatrix} s & -\frac{b}{q} \\ t & \frac{a}{q} \end{pmatrix}^{-1} = \begin{pmatrix} \frac{a}{q} & \frac{b}{q} \\ -t & s \end{pmatrix}$$

which implies that $a \sim q$ so $a|b$. Since b was arbitrary, this must hold for all elements in the rows and columns of a.

We can now make every element in the rows and columns of a identically 0. As before a must divide everything that remains. This again gives us a matrix of the form

$$A' = \begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_n & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}.$$

Hence our original module $M \cong M_A \cong M_{A'}$ and so, without loss of generality, we can replace A' by A'' which is square by adding/removing zero-columns. Furthermore $a_1|a_2|a_3|\cdots|a_n$. Write $A'' = \operatorname{diag}(a_1, \ldots, a_\ell, 0, \ldots, 0)$. This is (trivially) a block diagonal matrix and so

$$M \cong M_{A''} = M_{(a_1)} \oplus M_{(a_2)} \oplus \cdots \oplus M_{(a_\ell)} \oplus M_{(0)}^k \tag{3.7}$$

so we endeavour to analyze what each of these constituents looks like. This module induces a map $R^1 \xrightarrow{a} R^1 \to M_{(a)}$ and so $M_{(a)} \cong R^1/\operatorname{im}(a) \cong R/\langle a \rangle$ which we can write as

$$M_{(a)} \cong R/\langle a \rangle = \begin{cases} R & a = 0 \\ 0 & a \sim 1 \\ R/\langle a \rangle & \text{otherwise} \end{cases}. \tag{3.8}$$

Hence we can write

$$M \cong R^k \oplus \bigoplus_{j=1}^{m} R/\langle a_j \rangle \tag{3.9}$$

where $a_1|a_2|\cdots|a_m$. However, this is not quite the form we want.

Theorem 3.2.2 (Chinese Remainder Theorem)**.** *In a principal ideal domain, if* $\gcd(a,b) = 1$ *then* $R/\langle a\rangle \oplus R/\langle b\rangle = R/\langle ab\rangle$.

Proof. We can row and column reduce to find the following to find

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} q & 0 \\ 0 & \frac{ab}{q} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}$$

so the result follows. □

We now apply the Chinese Remainder Theorem to (3.9) to get our desired form.

Corollary 3.2.3. *If* A *is a finitely generated abelian group, then*

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}. \tag{3.10}$$

Proof. Note that all finitely generated abelian groups are finitely generated modules over $\mathbb{Z}$, and $\mathbb{Z}$ is a principal ideal domain. Hence by the fundamental theorem, the result follows. □

3.3 Tensors

Consider a series of R-modules $M_i, i = 1, \ldots, 3$, and let us examine how similar they are as abelian groups. Now $(M_1 \oplus M_2) \oplus M_3 \cong M_1 \oplus (M_2 \oplus M_3)$ and $M_1 \oplus M_2 \cong M_2 \oplus M_1$. By defining the zero module 0 containing only an element 0, we have that $M \oplus 0 \cong M$. Unfortunately, there are no inverses for the modules, and so in a sense $(R-\text{mod}, \oplus, 0)$ is an abelian semigroup.

On the other hand, let us move to the operation of "multiplication."

Definition 3.3.1. Given $M, N \in R$-mod we define

$$M \otimes_R N = \left\{ \sum a_i m_i \otimes n_i : \begin{smallmatrix} a_i \in R \\ m_i \in M \\ n_i \in N \end{smallmatrix} \right\} / K \tag{3.11}$$

equipped with a canonical map $M \times N \to M \otimes N$ sending $(m, n) \mapsto m \otimes n$ where K is the ideal generated by

- $(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n$
- $m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2$
- $(rm) \otimes n - r(m \otimes n)$
- $m \otimes (rn) - r(m \otimes n)$

Example 3.3.2. If V, W are vector spaces then $V \otimes W$ is a vector space over the same underlying field and $\dim(V \otimes W) = (\dim V)(\dim W)$. Indeed, let $v_i, i = 1, \ldots, n$ be a basis for V and $w_j, j = 1, \ldots, m$ a basis for W. We claim that

$$\mathcal{B} = \left\{ v_i \otimes w_j, \begin{smallmatrix} i=1,\ldots,n \\ j=1,\ldots,m \end{smallmatrix} \right\} \tag{3.12}$$

is a basis for $V \otimes W$. If this is the case, then we are done since $|\mathcal{B}| = mn = (\dim V)(\dim W)$. To show that $\mathcal{B}$ spans $V \otimes W$ it is sufficient to show that an arbitrary $v \otimes w \in V \otimes W$ can be expressed in terms of $\mathcal{B}$. If $v \in V$ we can write $v = \sum_i \alpha_i v_i$ and similarly, $w = \sum_j \beta_j w_j$. Hence

$$\begin{aligned} v \otimes w &= \left(\sum_{i=1}^{n} \alpha_i v_i \right) \otimes \left(\sum_{j=1}^{m} \beta_j w_j \right) \\ &= \sum_{i=1}^{n} (\alpha_i v_i) \otimes \sum_{j=1}^{m} (\beta_j w_j) \\ &= \ldots \\ &= \sum_{i,j=1}^{m,n} \alpha_i \beta_j v_i \otimes w_j \end{aligned}$$

so $\mathcal{B}$ does indeed span $V \otimes W$.

To show linear independence, Let v^i be the duel basis of v_i so that $v^i \in V^*$ such that $v^i(v_k) = \delta^i_k$ where δ^i_k is the Kronecker delta. Likewise, let w^j be the dual basis to w_j. Define a map $\phi^{ij} : V \otimes W \to F$ where F is the base field, so that $\phi^{ij} \in (V \otimes W)^*$ and

$$\phi^{ij} \left(\sum_p a_p \tilde{v}_p \otimes \tilde{w}_p \right) = \sum_p a_p v^i(\tilde{v}_p) \cdot w^j(\tilde{w}_p). \tag{3.13}$$

As an exercise, show that this is well defined. By acting this on the basis elements, we then get

$$\phi^{ij}(v_k \otimes w_\ell) = \delta^i_k \delta^j_\ell = \delta^{ij}_{k\ell} \tag{3.14}$$

hence we have found a basis for the dual space, which implies that $\{v_k \otimes w_\ell\}$ is indeed linearly independent.

Example 3.3.3. If X and Y are finite sets let $\mathcal{F}(X) = \{f : X \to \mathbb{F}\}$ for some field $\mathbb{F}$. Then $\mathcal{F}(X) \otimes \mathcal{F}(Y) \cong \mathcal{F}(X \times Y)$. Note however that it is *not* true that $L^2(\mathbb{R}) \otimes L^2(\mathbb{R}) \cong L^2(\mathbb{R}^2)$, and the reason this is not the case is because $L^2(\mathbb{R})$ is not finite dimensional. However, this is a dense mapping from one into the other.

Example 3.3.4. If $q = \gcd(a, b) = sa + tb$ then $R/\langle a\rangle \otimes R/\langle b\rangle \cong R/\langle q\rangle$. For example, $\mathbb{Z}/\langle 3\rangle \otimes \mathbb{Z}\langle 7\rangle \cong \mathbb{Z}/\langle 1\rangle = 0$. On the other hand, note that $\mathbb{Z}/3 \oplus \mathbb{Z}/7 \cong \mathbb{Z}/21$.

To see this, we will explicitly construct bijections between $R/\langle a\rangle \otimes R/\langle b\rangle$ and $R/\langle q\rangle$. Begin with the mapping

$$R/\langle a\rangle \otimes R/\langle b\rangle \to R/\langle q\rangle, \qquad [r_1]_a \otimes [r_2]_b \mapsto [r_1 \cdot r_2]_q.$$

This map is bilinear and well-defined (exercise). Conversely, define

$$R/\langle q\rangle \to R/\langle a\rangle \otimes R/\langle b\rangle, \qquad [r]_q \mapsto r \cdot [1]_a \otimes [1]_b$$

and all that remains is to check is that this map is well defined. Note that

$$\begin{aligned}[q]_q &= q[1]_a \otimes [1]_b = (sa + tb)[1] \otimes [1] \\ &= s[a]_a \otimes [1]_b + t[1]_a \otimes [b]_b\end{aligned}$$

and so zero maps to zero by this mapping. Finally, composing these maps yields the identity, since

$$[r_1]_a \otimes [r_2]_b \mapsto [r_1 r_2]_q \mapsto r_1 r_2 [1]_a \otimes [1]_b = [r_1]_a \otimes [r_2]_b.$$

Theorem 3.3.5. *The set $(R\text{-mod}, \oplus, \otimes, 0, R)$ is a commutative "ring." That is for all $M, N, P \in R\text{-mod}$ we have*

- $(M \oplus N) \oplus P \cong M \oplus (N \oplus P)$
- $M \oplus 0 \cong M$
- $M \oplus N \cong N \oplus M$
- $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$
- $M \otimes R \cong M$
- $M \otimes (N \oplus P) = M \otimes N \oplus M \otimes P$
- $M \otimes N \cong N \otimes M$

Example 3.3.6. Consider $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n$. Notice that we can write this as

$$\begin{aligned} \mathbb{Q} \otimes \mathbb{Z}^n &= \mathbb{Q} \otimes (\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}) \\ &= (\mathbb{Q} \otimes \mathbb{Z}) \oplus \cdots \oplus (\mathbb{Q} \otimes \mathbb{Z}) \\ &= \mathbb{Q} \oplus \cdots \oplus \mathbb{Q} = \mathbb{Q}^n \end{aligned}$$

If $\phi : R \to S$ is a morphism of rings, then S is an R-module by defining $r \cdot s = \phi(r) \cdot s$. Hence given an R-module M we define $M_S = S \otimes_R M$. This is in fact an S-module by $s(s' \otimes m) = (ss') \otimes m$. So this gives us an "extension of scalars" as can be seen in the following way:

Example 3.3.7. Let $M = \mathbb{Z}^n/\mathbb{Z}$ and $\iota : \mathbb{Z} \to \mathbb{Q}$ is the inclusion map then $M_{\mathbb{Q}} = \mathbb{Q}^n$. Similarly, if $M = \mathbb{R}^n/\mathbb{R}$ and $\iota : \mathbb{R} \to \mathbb{C}$ is the inclusion map then $(\mathbb{R}^n)_{\mathbb{C}} = \mathbb{C}^N$. In general, if $M = R^n$ and $\phi : R \to S$ then $M_S = S^n$.

If there is a R-module morphism $M_1 \xrightarrow{f} M_2$ then for any module R-module N a bi-functor is a map $M_1 \otimes N \xrightarrow{f \otimes 1} M_2 \otimes N$ acting as $m_1 \otimes n \mapsto f(m_1) \otimes n$. Furthermore, if there is an R-module morphism $N_1 \xrightarrow{g} N_2$ then for any other R-module M we have a map $M \otimes N_1 \xrightarrow{1 \otimes g} M \otimes N_2$ acting as $m \otimes n \mapsto m \otimes f(n)$. If we have two maps $f : M_1 \to M_2$ and $g : N_1 \to N_2$ then we get the map $f \otimes g : M_1 \otimes N_1 \to M_2 \otimes N_2$ sending $m \otimes n \mapsto f(m) \otimes f(n)$.

Theorem 3.3.8. *There is a mapping $R\text{-mod} \times R\text{-mod} \to R\text{-mod}$ taking $(M, N) \mapsto M \otimes N$ which is a bi-functor satisfying the following "all the obvious properties."*

Interestingly, note that $(\mathbb{Z}/3) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. To see this, note that an element of the left hand side can be written as $a \otimes q = 1 \otimes \left(3\frac{1}{3}q\right) = 3a \otimes \frac{1}{3}q = 0$.

Theorem 3.3.9. *If R is a domain then there exists a field $Q(R)$ containing R. More precisely, there exists a field $Q(R)$ and a map $\iota : R \to Q(R)$ which is an injection.*

Definition 3.3.10. We say that an R-module M is a *torsion module* if $\forall m \in M, \exists r \in R \setminus \{0\}$ such that $rm = 0$.

Theorem 3.3.11. *If M is a torsion module over R then $M_{Q(R)} = M \otimes_R Q(R) = 0$.*

Proof. Take a general element $m \otimes q \in M \otimes_R Q(R)$. Since M is torsion, we know $\exists r \in R \setminus \{0\}$ such that $rm = 0$. Since $r \in R$ and we can identify R with a subset of $Q(R)$ then r^{-1} exists in $Q(R)$ so

$$m \otimes q = m \otimes (rr^{-1}q) = (rm) \otimes (r^{-1}q) = 0.$$

Since this element was arbitrary, we conclude that this is true for all elements of $M \otimes Q(R)$ and the result follows. □

Proposition 3.3.12. *If we write*

$$M \cong R^k \oplus \bigoplus R/(p_i^{s_i})$$

then k is uniquely determined.

Proof. The space $M_{Q(R)}$ is a vector space and so we can compute

$$\begin{aligned}\dim_{Q(R)} M_{Q(R)} &= \dim_{Q(R)} \left(R^k \oplus \bigoplus R/(p_i^{s_i})\right) \otimes Q(r) \\ &= \dim_{Q(R)} \left(Q(R)^k \oplus \bigoplus_i R/(p_i^{s_i}) \otimes Q(R)\right) \\ &= \dim_{Q(R)} Q(R)^k = k\end{aligned}$$

□

Definition 3.3.13. A multiplicative subset S of $R \setminus \{0\}$ is a subset S such that

- $1 \in S$
- If $a, b \in S$ then $ab \in S$.

Example 3.3.14.

1. For an arbitrary domain R, we can take $S = R \setminus \{0\}$.
2. If P is a prime ideal then $S = R \setminus P$ is multiplicative. Indeed, suppose that $a, b \in R \setminus P$ then $ab \in R \setminus P$. If this were not the case then $ab \in P$ which would imply that either $a \in P$ or $b \in P$ which is a contradiction.
3. Consider the set $\{2^n\}_{n \geq 0} \subseteq \mathbb{Z}$ which is also multiplicative.

Definition 3.3.15. Given a multiplicative subset $S \subseteq R \setminus \{0\}$ define *localization of R at S* as

$$S^{-1}R = \left\{\frac{r}{s} : r \in R, s \in S\right\} / \sim$$

where $\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$ whenever $r_1 s_2 = r_2 s_1$.

The relation given in the above definition is an equivalence relation. Clearly $\sim$ is symmetric and reflexive, so we will now show transitivity. Assume that

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2}, \qquad \frac{r_2}{s_2} \sim \frac{r_3}{s_3}. \tag{3.15}$$

This implies that $r_1 s_2 = r_2 s_1$ and $r_2 s_3 = r_3 s_2$ and we want to show that $r_1 s_3 = r_3 s_1$. Multplying the first equation by s_3 and the second equation by s_1 we get a common factor

which we can combine as follows

$$r_1 s_2 s_3 = r_2 s_1 s_3 = r_3 s_2 s_1. \tag{3.16}$$

by cancelling out s_2 on each side, we get the desired result.

The set $S^{-1}R$ has two distinguished elements called $0_{S^{-1}R} = \frac{0}{1}$ and $1_{S^{-1}R} = \frac{1}{1}$. Then we can define multiplication and addition in $S^{-1}R$ by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \qquad \frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

Finally, there is an identification of R in $S^{-1}R$ via $\iota : R \to S^{-1}R$ by $\iota(r) = \frac{r}{1}$.

Theorem 3.3.16. *The operations of addition and multiplication on $S^{-1}R$ are well-defined and make $S^{-1}R$ into a ring in which all elements of S are invertible. Furthermore, $\iota : R \to S^{-1}R$ is an injection.*

If we take $S = R \setminus \{0\}$ then $S^{-1}R$ is $Q(R)$, the *field of fractions*. When $S = R \setminus P$ for some prime ideal P then we term $S^{-1}R$ simply the localization about P. It intuitively means that if no prime number occurs in the denominator of a fraction, it won't occur in the sum or product of its elements. Finally, in the case where $S = \{2^n\}_{n\geq 0} \subseteq \mathbb{Z}$ we get

$$S^{-1}\mathbb{Z} = \left\{ \frac{k}{2^n} \right\}$$

the dyadic integers.

Proposition 3.3.17. *If $M \cong R^K \oplus \bigoplus R/(p_i^{s_i})$ and p is a prime and $s \in \mathbb{N}$ then*

1. $\dim_{Q(R)} M_{Q(R)} = k$
2. $\dim_{R/(p)} M_{R/(p)} = k + |\{i : p_i \sim p\}|$
3. *Since $p \in M$ and $s \in \mathbb{N}$ have been specified, we have a natural map $\phi : m \mapsto p^s m$. Then the dimension of the image of ϕ as an $R/(p)$ module is*

$$\dim_{R/(p)} \mathrm{im}(\phi)_{R/(p)} = k + |\{i : p_i \sim p, s_i > s\}|. \tag{3.17}$$

Proof. 1. We have already proven this result in Prop 3.3.12.

2. Since we are in a principal ideal domain, all prime ideals are maximal and so $R/(p)$ is a field. Since there is a natural projection map $R \to R/(p)$ then R is also a $R/(p)$ module. Now $R \otimes R/(p) = R/(p)$ and so

$$R/(p_i^{s_i}) \otimes R/(p) = \begin{cases} R/(p) & p_i = p \\ 0 & p_i \not\sim p \end{cases}. \tag{3.18}$$

   Thus when we consider $M_{R/(p)}$ the torsionfree part R^k will remain unchanged, and all terms will disappear unless they are associates of the prime p.

3. Note that the image of ϕ on elements of R is the ideal $p^s R$. However, we are not interested in this structure as an ideal but rather as a module, in which case we notice that $p^s R \cong R$. In this case $\dim_{R/(p)} \operatorname{im}(\phi)_{R/(p)} = 1$, which will contribute k-dimensions when taken over all of M.

   If q is a prime that is not asociated to p then the image of ϕ on $R/(q^t)$ is $R/(q^t)$. Indeed, since p^s and q^t are coprime we can write $1 = ap^s + bq^t$ so in $R/(q^t)$ we have $1 = ap^s$. Since 1 is in the image, everything is in the image. Then $\dim_{R/(p)} \operatorname{im}(\phi)_{R/(p)} = 0$ in this instance and so does not contribute to the dimension when taken over the entire module.

   If $t \leq s$ then the image of ϕ on $R/(p^t)$ is 0, since multiplication by p^s will always ensure that the product is "divisible" by p^s meaning that all elements go to 0. Hence the dimension of the image is also zero, and this does not affect the dimension of the entire module.

   Finally, consider the image of ϕ on $R/(p^t)$ for $t > s$, which is $R/(p^{t-s})$. Consider a typical element in the image, which is of the form $[p^s a]_{p^t}$. We can define two maps $[p^s a]_{p^t} \mapsto [a]_{p^{t-s}}$ and $[b]_{p^t} \mapsto \left[\frac{b}{p^s}\right]_{p^{t-s}}$ which is a well defined map. Hence $\dim_{R/(p)} \operatorname{im}(\phi)_{R/(p)} = 1$ in this instance.

   Hence the sum total of the contributions by tensoring yields

$$\dim_{R/(p)} \operatorname{im}(\phi)_{R/(p)} = k + |\{i : p_i \sim p, s_i > s\}|$$

   .

□

Corollary 3.3.18. *If $M \cong R^k \oplus \bigoplus R/(p_i^{s_i})$ then k and the set of pairs (p_i, s_i) are uniquely determined up to permutation.*

3.4 Jordan Canonical Form

Let F be an algebraically closed field and set $R = F[x]$. Let V be a finite dimensional vector space over F (so that $V = F^n$ for some n), and take $T : V \to V$ to be a linear transformation (which we may think of as $T \in M_n(F)$). We have already seen that V may be endowed with the structure of an R module by identifying the action as $xu = Tu$.

Now let R be a prinical ideal domain and V finitely generated by the set $\{e_i\}$. Then by the fundamental theorem of finitely generated modules over principal ideal domains, we know that we can write

$$V \cong R^k \oplus \bigoplus R/(p_i^{s_i}), \qquad k \in \mathbb{N}, s_i \in \mathbb{N}, p_i \in F[x] \text{ prime.} \tag{3.19}$$

Note that k must be zero as the left-hand-side is finite dimensional and if $k \neq 0$ then the right-hand-side would be infinite dimensional.

Note that a prime in $F[x]$ is a linear polynomial of the form $x - \lambda$ for some $\lambda \in F$. Indeed, these are clearly prime since $x - \lambda$ is irreducible and hence a prime. Furthermore, if the degree of any polynomial $f(x)$ is greater than 1 then since we are in an algebraically closed field, the polynomial has a root λ and so we can write $f(x) = (x-\lambda)q + r$. Note then that $f(\lambda) = r = 0$ so $(x - \lambda)|f$.

Thus every summand is of the form $F[x]/(x - \lambda)^s$ which, as a vector space, has a basis

$$F_0 = (x-\lambda)^0, F_1 = (x-\lambda)^1, F_2 = (x-\lambda)^2, F_3 = (x-\lambda)^3, \ldots, F_{s-1} = (x-\lambda)^{s-1}. \tag{3.20}$$

Acting on a basis element by $(x - \lambda$ it is easy to see that $(x - \lambda)F_k = F_{k+1}$ and the corresponding matrix is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

and so corresponding matrix representing multiplication by x is given by

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}. \tag{3.21}$$

Hence there exists a matrix $C \in M_n(F)$ such that CTC^{-1} is block diagonal where each block is of the form given in (3.21).

In our case, consider the map $R^n \xrightarrow{\pi} V = F^n$ taking points $e_i \mapsto e_i$ so that in general $x^k \mapsto A^k e_i$. Now $xe_i - Ae_i \in \ker \pi$. Indeed, notice that

$$xe_i - Ae_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x \\ 0 \\ \vdots \\ 0 \end{pmatrix} - \begin{pmatrix} a_{1i} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ a_{ni} \end{pmatrix} = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{i(i-1)} \\ x - a_{ii} \\ a_{i(i+1)} \\ \vdots \\ a_{n_i} \end{pmatrix}. \tag{3.22}$$

Hence we have a sequence of maps

$$R^n \xrightarrow{xI - A} R^n \xrightarrow{\pi} V = F^n$$

We claim that $\ker \pi = (r_i = xe_i - Ae_i)$. Indeed, one inclusion is obvious since we have already shown that $(r_i) \subseteq \ker \pi$ above. Conversely, consider the following diagram

$$\begin{array}{ccccc} F^n & \xrightarrow{\beta} & \dfrac{R^n}{(r_i)} & \xrightarrow{\alpha} & \dfrac{R^n}{\ker \pi} \\ & \searrow^{id} & & & \downarrow \\ & & & & F^n \end{array}$$

Where $\beta : e_i \mapsto e_i$. We know that α is well-defined by the first part of the proof. Furthermore if we can show that α is injective we will be done, since then $(r_i) \subseteq \ker \pi$. But this will be true precisely if β is surjective since otherwise this would contradict the fact that the total composition is the identity. To show that β is surjective, note that

$$[x^k e_i] = x^{k-1}[xe_i] = x^{k-1}[Ae_i] \tag{3.23}$$

and so we have reduced the power of x by one. we can continue this recursively until we get that $[x^k e_i] = [A^k e_i]$. Now $[A^k e_i]$ contains only scalars, so it can be written as $\beta(A^k e_i)$ and we conclude that β is surjective as required.

$$\begin{array}{ccccc} R^n & \xrightarrow[M]{xI - A} & R^n & \xrightarrow{\pi_A} & F^n \\ \uparrow Q & & \downarrow P & & \downarrow c \\ R^n & \xrightarrow[N]{xI - B} & R^n & \xrightarrow{\pi_B} & F^n \end{array}$$

where $c : F^n \to F^n$ is defined as $ce_i = \pi_B(Pe_i)$. However, applying π_B is highly non-trivial. Note that $\pi_B(x^k u) = B^k u$ and write $P = \sum_k x^k P_k$ where $P_k \in M_n(F)$. Then

$$\begin{aligned} ce_i &= \pi_B(Pe_i) \\ &= \pi\left(\sum_k x^k P_k e_i\right) \\ &= \sum_k B^k P_k e_i \end{aligned}$$

and so $C = \sum_k B^k P_k$.