# Grad Student Prep Course - Abstract Algebra - 2024

Nicholas Cecil

## Contents



These notes are a meant as a quick review of some basic concepts of group theory. Citations are provided to help a reader find more details in Dummit and Foote's *Abstract Algebra* [DF03] or Lang's *Algebra* [Lan02]. Specific citations will use the format [REFERENCE].Location; *e.g.* [DF03].3.3 refers to the third section of Chapter 3 in Dummit and Foote.

## 1 Groups and 4 Examples

In this section, we define groups and provide 5 examples which we will follow throughout these notes.

**Definition 1.0.1** **Group, [DF03].1.1, [Lan02]I.2**

A **group** $(G, \cdot)$ is a set $G$ paired with a function $\cdot : G \times G \to G$ satisfying the following:

(i) (Associativity) For all $g, h, k \in G$ there holds $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.

(ii) (Identity) There exists an element $e \in G$ such that for all $g \in G$ there holds $e \cdot g = g = g \cdot e$.

(iii) (Inverses) For all elements $g \in G$ there is an element $g^{-1} \in G$ such that $g^{-1} \cdot g = e = g \cdot g^{-1}$.

We say that a group is **Abelian** when the operation $\cdot$ is associative, *i.e.* when for all $g, h \in G$ there holds $g \cdot h = h \cdot g$.

**Notation** We will often drop the group operation from our notation. That is, if $G \ni g, h$ is a group, we write $g \cdot h = gh$. When a group is Abelian, it is customary to write the group operation as $+$ instead of $\cdot$. When additive notation is in use, the inverse of $g$ is written $-g$ and not $g^{-1}$ and the identity element is written as 0.

**Discussion** There is an interesting point here about how much of a group is *structure* (something extra put on a set, *e.g.* the group operation $\cdot$) and how much is *property* (something which is true about a set or structure, *e.g.* identities and inverses exist). On its face, we could get a different thing by saying a group is an ordered quadruple $(G, \cdot, e_H, (-)^{-1})$ where we specify identity and inverse as structure. Fortunately, in this context, there is no difference between group-as-pair and group-as-quadruple as the following lemma attests.

**Lemma 1.0.2** **Uniqueness of Identity and Inverse**

Fix a group $G$ and element $g \in G$. Let $e \in G$ be some element satisfying the identity axiom. Let $g^{-1} \in G$ be an inverse for $g$.

(i) If $h \in G$ satisfies $gh = g$ or $hg = g$, then $h = e$.

(ii) If $h \in G$ satisfies $gh = e$ or $hg = e$, then $h = g^{-1}$.

*Proof.* Consider (i). Assuming that $gh = g$, we get

$$h = e \cdot h = g^{-1}g \cdot h = g^{-1} \cdot gh = g^{-1} \cdot g = e$$

and the other case is similar.

Consider (ii). Assuming $gh = e$, we have

$$g^{-1} = g^{-1} \cdot e = g^{-1} \cdot gh = e \cdot h = h$$

and the other case is similar. QED

Given some sort of mathematical object manifesting as a structure on an underlying set (think vector spaces, topological spaces) it is fruitful to study those set maps between the underlying sets which preserve the structure (think linear map, continuous map). This is no less true for groups.

**Definition 1.0.3** **Group Homomorphism, [DF03].1.6, [Lan02]I.2**

If $G$ and $H$ are groups, a function $f : G \to H$ is called a **group homomorphism** or just a **homomorphism** when for $g, h \in G$ there holds $f(gh) = f(g)f(h)$.

The other parts of being a group, having an identity element and inverses, are also preserved by homomorphisms:

**Lemma 1.0.4** **Preservation of Identity and Inverse**

If $f : G \to H$ is a group homomorphism,

(i) there holds $f(e_G) = e_H$, and

(ii) for all $g \in G$ there holds $f(g^{-1}) = [f(g)]^{-1}$.

*Proof.* Consider (i). Observe that $f(e_G)f(e_G) = f(e_G e_G) = f(e_G)$. By uniqueness of identity, $f(e_G) = e_H$.

Consider (ii). Observe that $f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_H$. By uniqueness of inverses, $f(g^{-1}) = [f(g)]^{-1}$. QED

**Definition 1.0.5** **Isomorphism**

A group homomorphism $f : G \to H$ is called an **isomorphism** when there is a group homomorphism $f' : H \to G$ such that $ff' = 1_H$ and $f'f = 1_G$.

We can describe group isomorphisms in another way.

**Lemma 1.0.6** **Isomorphism Detection**

A group homomorphism $f : G \to H$ is an isomorphism if and only if it is a bijection.

*Proof.* Certainly and isomorphism is a bijection; the definition requires the existence of an inverse. For the converse, let $f : G \to H$ be a bijective group homomorphism. Let $f^{-1} : H \to G$ be its inverse function. We need only show that $f^{-1}$ is a group homomorphism. To this end, let $h, h' \in H$. We have

$$\begin{aligned} f^{-1}(h)f^{-1}(h') &= f^{-1}f(f^{-1}(h)f^{-1}(h')) \\ &= f^{-1}(ff^{-1}(h)ff^{-1}(h')) \\ &= f^{-1}(hh') \end{aligned}$$

as desired. QED

**Notation** When $G$ and $H$ are groups and there is a group isomorphism $G \to H$, we say that $G$ and $H$ are isomorphic and write $G \cong H$.

## 1.1 Example I: $\mathbb{Z}$, The Integers

The integers $\mathbb{Z}$ along with ordinary addition $+$ form an Abelian group.

**Warning** The integers do not form a group under multiplication; there is a multiplicative identity 1, but not every integer has a multiplicative inverse.

We recall the following crucial theorem about the integers.

**Theorem 1.1.1** **Division, [DF03].0.2**

For any integers $a, b$ there exists unique $q \in \mathbb{Z}$ and $r \in \{0, ..., |b| - 1\}$ such that

$$a = bq + r.$$

In this context we call $q$ the **quotient** and $r$ the **remainder** when $a$ is divided by $b$.

**Remark** In abstract language, this says that $\mathbb{Z}$ is a Euclidean domain, *c.f.* [DF03].8.1.

## 1.2 Example II: $\mathbb{Z}_n$, The Integers Modulo $n$

**Definition 1.2.1** **$\mathbb{Z}_n$, [DF03].0.3**

Fix a natural number $n \in \mathbb{Z}_{>0}$. Define an equivalence relation $\sim_n$ on $\mathbb{Z}$ by writing $a \sim_n b$ when $n$ divides $a - b$. We write $[a]_n$ for the equivalence class of $a$ under $\sim_n$. We write $\mathbb{Z}_n$ for the set of equivalence classes; that is

$$\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\}.$$

There is a function $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ satisfying

$$[a]_n + [b]_n = [a + b]_n$$

for all integers $a, b \in \mathbb{Z}$. With this, $(\mathbb{Z}_n, +)$ is an Abelian group.

**Discussion** On could, and probably should, complain that this definition contains the unproven assertion that the function $+$ actually exists. Once this is believed, verifying the group axioms is easy. For instance, if $a, b, c \in \mathbb{Z}$ we have

$$\begin{aligned} ([a]_n + [b]_n) + [c]_n &= [a + b]_n + [c]_n \\ &= [(a + b) + c]_n \\ &= [a + (b + c)]_n && (\mathbb{Z} \text{ is a group}) \\ &= [a]_n + ([b]_n + [c]_n) \end{aligned}$$

so that addition is associative. We will now prove that + exists.

**Lemma 1.2.2** — **Well Definition of Modular Addition**

There is a function $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ satisfying

$$[a]_n + [b]_n = [a+b]_n$$

for all integers $a, b \in \mathbb{Z}$.

*Proof.* The only obstruction to the property

$$[a]_n + [b]_n = [a+b]_n$$

being a definition is that there may be $a, a', b, b' \in \mathbb{Z}$ so that $[a]_n = [a']_n$ and $[b]_n = [b']_n$ so that $[a+b]_n \neq [b+b']_n$. We will show that this obstruction cannot occur. Indeed, fix $a, a', b, b' \in \mathbb{Z}$. Suppose $[a]_n = [a']_n$ and $[b]_n = [b']_n$. By definition, there is $k, k' \in \mathbb{Z}$ such that $kn = a - a'$ and $k'n = b - b'$. But then $(k+k')n = (a+b) - (a'+b')$ so that $[a+b]_n = [a'+b']_n$ and the obstruction does not occur. QED

## 1.3 Example: $\mathfrak{S}_n$ The Symmetric Group

**Definition 1.3.1** — **Symmetric Group, [DF03].1.3**

Let $A$ be a set. An **automorphism** or **symmetry** or **permutation** of $A$ is a bijection $A \to A$. The set of all bijection is written as $\mathrm{Aut}(A)$ or as $\mathfrak{S}_A$. If $A = \{1, ..., n\}$ we use the notation $\mathfrak{S}_n = \mathfrak{S}_A$. Ordinary function composition $\circ$ makes $(\mathfrak{S}_A, \circ)$ into a group.

**Cycle Notation** Suppose that $A$ is some finite set. There is a convenient notation for elements of $\mathfrak{S}_A$ called cycle notation. If $a_0, ..., a_n \in A$, one write

$$\sigma = (a_n \ \cdots \ a_2 \ a_1 \ a_0)$$

for that permutation which carries $a_0$ to $a_1$ and $a_1$ to $a_2$ and so on up to $a_{n-1}$ to $a_n$ and $a_n$ to $a_0$. Any element of $A$ not written in the cycle is fixed by $\sigma$. On calls $\sigma$ an $n$-cycle.

**Example** In $\mathfrak{S}_3$, there is the cycle $\sigma = (1 \ 2)$. This is the symmetry $\sigma : \{1,2,3\} \to \{1,2,3\}$ given by

$$\sigma(1) = 2 \quad \sigma(2) = 1 \quad \sigma(3) = 3.$$

**Definition 1.3.2** — **$\sigma$-Orbit**

Let $A$ be a set. If $a, b \in A$ and $\sigma \in \mathfrak{S}_A$, we say that $a, b$ are in the same **orbit** of $\sigma$ when there is an integer $k$ such that $\sigma^k(a) = b$. We say that $\sigma$ is a **cycle** when it has at most one non-singleton orbit.

**Explanation** When $A$ is finite, the cycles $\sigma$ are exactly those permutations which can be written as

$$\sigma = (a_n \ \cdots \ a_2 \ a_1 \ a_0).$$

**Proposition 1.3.3** — **Cyclic Decomposition**

If $A$ is a finite set, every element of $\mathfrak{S}_A$ may be written as a product of cycles. The cycles may be chosen to be disjoint[a] and in this case, the decomposition into cycles is unique up to reordering and removal of identity cycles.

[a] Their non-singleton orbits being disjoint as sets.

*Proof.* Fix $\sigma \in \mathfrak{S}_A$. Define a equivalence relation on $A$ by $a \sim b$ iff $b$ lies in the orbit of $A$. An equivalence class will be called a $\sigma$-orbit; if $a \in A$ we write $[a]_\sigma$ for the $\sigma$-orbit containing $a$. Let $A' \subseteq A$ be a subset containing exactly one element of each equivalence class. For each $a \in A$, write $\sigma_a : A \to A$ for that function

$$\sigma_a(x) = \begin{cases} \sigma(x) & x \in [a]_\sigma \\ x & x \notin [a]_\sigma \end{cases}$$

On may then check that $\sigma_a$ is a cycle and that

$$\sigma = \prod_{a \in A'} \sigma_a$$

decomposes $\sigma$ as a product of disjoint cycles. Let $A'' \subseteq A$ be that set such that $a \in A''$ iff $|[a]_\sigma| > 1$. Suppose further that

$$\sigma = \prod_{i \in I} \tau_i$$

is another decomposition of $s$ into disjoint, non-identity cycles. Fix $a \in A''$. The is unique $f(a) \in I$ such that $\tau_{f(a)}$ does not fix $a$. This defines an injection $f : A'' \to I$. Now, fix $i \in I$. Since $\tau_i$ is non-identity, there is some $g(i) \in A$ such that $\tau_i$ does not fix $g(i)$. Since then $\sigma$ does not fix $g(i)$, we may assume that $g(i) \in A''$. This yields a map $g : I \to A''$. Observe that $f \circ g = \mathrm{id}_I$. From this and the injectivity of $f$, we have that $f, g$ are mutually inverse bijections.

Finally, one observes that the $\tau_{f(a)}$ orbit of $a$ is the $\sigma_a$ orbit of $a$ and on this orbit $\tau_{f(a)} = \sigma_a$. As both are cycles, $\tau_{f(a)} = \sigma_a$ and we have the desired uniqueness result. QED

**Definition 1.3.4** **Transposition**

If $A$ is a set, a transposition $\sigma \in \mathfrak{S}_A$ is an element of the form $\sigma = (a \;\; b)$ with $a \neq b$.

**Lemma 1.3.5** **Transposition Decomposition**

If $A$ is a finite set, every element of $\mathfrak{S}_A$ is a product of transpositions.

*Proof.* By cycle decomposition, it suffices to show that every cycle is a product of transpositions. Consider $a_0, ..., a_n \in A$. Observe

$$(a_n \;\; \cdots \;\; a_2 \;\; a_1 \;\; a_0) = (a_n \;\; \cdots \;\; a_2 \;\; a_0)(a_1 \;\; a_0)$$

so that a cycle of $n+1$ elements can be written as a product of transpositions if a cycle of $n$ elements can be. We reduce in this manner to the case of $n = 2$ which is a transposition. QED

**Discussion** Unlike the decomposition into cycles, the decomposition into transpositions is wildly non-unique. What is conserved in such a decomposition is the parity of the number of transpositions.

**Proposition 1.3.6** **Even/Odd Permutation**

If $\sigma \in \mathfrak{S}_A$ and

$$\sigma = \prod_{i \in I} \sigma_i \quad \text{and} \quad \sigma = \prod_{j \in J} \tau_j$$

are decompositions of $\sigma$ into finitely many transpositions, then $|I|$ is even iff $|J|$ is. In that case, we say that $\sigma$ is an **even** permutation. Else, we say that $\sigma$ is **odd**.

*Proof.* There is no loss in assuming that $A$ is finite. We define the linear map $M_\sigma : \mathbb{R}^{|A|} \to \mathbb{R}^{|A|}$ such that $M_\sigma(e_a) = e_{\sigma(a)}$ where $a \in A$ and $e_a$ is the $a$-th standard basis vector. We observe that of $\sigma$ is a transposition then $\det(M_\sigma) = -1$. Indeed, since $M_\sigma M_\tau = M_{\sigma\tau}$ for any $\sigma, \tau \in \mathfrak{S}_A$, we have that $\sigma$ is odd iff $\det(M_\sigma) = (-1)$ and from this the result follows. QED

**Remark** Depending on how one learned about determinants, one might object that this proof is circular. After all, the Leibniz formula for the determinant makes explicit use of the parity of permutations (*c.f.* [DF03].11.4). However, the determinant can be developed without using the parity of permutations (*c.f.* the appendix).

We end this section with an observation which we could have made long ago.

**Proposition 1.3.7** — **$\mathfrak{S}_A$ is not Abelian**

If for any set $|A| > 2$, the permutation group $\mathfrak{S}_A$ is not Abelian.

*Proof.* Fix elements $a, b, c \in A$. Write $\sigma = (a\ \ b)$ and $\tau = (b\ \ c)$. We have

$$(\sigma\tau)(b) = c \quad \text{but} \quad (\tau\sigma)(b) = a$$

so that $\sigma\tau \neq \tau\sigma$ and $\mathfrak{S}_A$ is not Abelian. QED

### 1.4 Dihedral Groups

# 2 New Groups from Old Groups

In this section, we consider various ways to extract new groups from old groups.

## 2.1 Subgroups

It is not unusual to have one group contain a smaller group. For instance $(\mathbb{R}, +) \subseteq (\mathbb{C}, +)$. There is a name for this situation.

**Definition 2.1.1** — **Subgroup, [DF03].2.1, [Lan02]I.2**

If $(G, \cdot)$ is a group, a **subgroup** of $G$ is a subset $H \subseteq G$ such that

(i) If $h, h' \in H$ then $h \cdot h' \in H$

(ii) the set $H$ with the domain-codomain restricted $\cdot : H \times H \to H$ is a group. Equivalently, $e_G \in H$ and if $h \in H$ then $h^{-1} \in H$.

**Remark** Note that if $H \subseteq G$ is a subgroup, the inclusion map $H \hookrightarrow G$ is a group homomorphism. There are various ways to generate subgroups.

**Definition 2.1.2** — **Subgroup Generated by a Set, [DF03].2.4, [Lan02]I.2**

Given a group $G$ and s subset $S \subseteq G$, the group $\langle S \rangle \subseteq G$ is the smallest[a] subgroup of $G$ containing $S$. Explicitly, its elements are all elements of $G$ which can be written as products of elements of $S$ and their inverses.

[a] In the poset of subgroups

**Example** Consider the non-zero complex numbers $\mathbb{C}^\times$ which is a group under multiplication. Consider $\langle i \rangle \subseteq \mathbb{C}$. We have

$$\langle i \rangle = \{i, -1, -i, 1\}$$

which is isomorphic to $\mathbb{Z}_4$ as a group.

**Definition 2.1.3** — **Kernel, [DF03].3.1, [Lan02]I.2**

If $f : G \to H$ is a group homomorphism, its **kernel** is

$$\ker f = f^{-1}(\{e_H\}) = \{g \in G : f(g) = e_H\}.$$

Observe that $\ker f \subseteq G$ is a subgroup.

**Example** Any vector space has an underlying additive Abelian group. A linear map of vector spaces is a homomorphism of these underlying groups. The kernel of this map is typically called the null space of the linear map.

Kernels can be used to detect whether homomorphisms are injective.

**Proposition 2.1.4** — **Injective $\iff$ $\ker = \{e\}$**

A group homomorphism $f : G \to H$ is injective if and only if $\ker f = \{e_G\}$.

*Proof.* We have already proven that $f(e_G) = e_H$. So, $\{e_G\} \subseteq \ker f$. If $f$ is injective, this must be equality. It remains to show the converse: that $\ker f = \{e_G\}$ implies $f$ is injective. Indeed, fix $g, g' \in G$ with $f(g) = f(g')$. Then

$$e_H = f(g^{-1})f(g') = f(g^{-1}g')$$

whence $e_G = g^{-1}g'$. Multiplying on the left by $g$, we obtain $g = g'$. So, $f$ is injective. QED

**Example** Consider the map $q : \mathbb{Z} \to \mathbb{Z}_2$ given by $x \mapsto [x]_2$. The the kernel $\ker q \subseteq \mathbb{Z}$ is the set of even integers.

As it turns out, all groups can be obtained as a subgroup of a particular family of groups.

**Theorem 2.1.5** — **Cayley-Yoneda, [DF03].4.2**

For every group $G$ there is a set $A$, a subgroup $S \subseteq \mathfrak{S}_A$, and a group isomorphism $f : G \to S$.

*Proof.* We choose $A = G$, the underlying set of $G$. For each $g \in G$, define $f_g : A \to A$ by $f_g(x) = g \cdot x$ where $\cdot$ is the group multiplication. Note that $f_g$ is a bijection; its inverse is $f_{g^{-1}}$.

Define $S = \{f_g \in \mathfrak{S}_A : g \in G\}$. This is a subgroup of $f_g$ since $f_e$ is identity on $A$ and $f_g f_h = f_{gh}$ for all $g, h \in G$. Moreover, this last says that $f : G \to S$ by $f(g) = f_g$ is a group homomorphism. It is evidently surjective.

To prove the theorem, it remains to show that $f$ is an injection. It is enough that $\ker f = \{e\}$. Indeed, if $g \in \ker f$ then $f_g = 1_A$. So, $g \cdot e = f_g(e) = e$. But this says that $g = e$ as desired. QED

## 2.2 Quotient Groups, Normal Subgroups

**Definition 2.2.1** — **Quotient by a Subgroup, [DF03].3.1, [Lan02]I.2**

Let $G$ be a group with subgroup $S$. For each $g \in G$, the $S$-**coset**

$$gS = \{gs \in G : s \in S\}.$$

We define the **quotient**

$$G/S = \{gS : g \in G\}$$

to be the set of $S$-cosets

**Lemma 2.2.2** — **Coset Partition**

If $S \subseteq G$ is a subgroup, the cosets $gS$ form a partition of $G$.

*Proof.* Define the relation $\sim$ on $G$ by $g \sim h$ iff $g \cdot s = h$ for some $s \in S$. Since $S$ is a subgroup, it contains identity and is closed under inverses. So, $\sim$ is an equivalence relation. We observe that the equivalence class of $g$ is $gS$. QED

It is tempting to define a group operation on $G/S$ by $gS \cdot hS = (gh)S$. Were this a well defined product, it would make $G/S$ a group. Unfortunately, it is not well defined for a generic subgroup $S$.

**Definition 2.2.3** — **Normal Subgroup, [DF03].3.1, [Lan02].I.3**

A subgroup $S \subseteq G$ is **normal** when for all $g \in G$ and $s \in S$ there holds $gsg^{-1} \in S$; that is

$$gSg^{-1} \subseteq S.$$

We write $S \trianglelefteq G$ to mean $S \subseteq G$ is a normal subgroup.

It turns out that $S \trianglelefteq G$ is the condition needed for $G/S$ to be a group.

**Proposition 2.2.4** — **Quotient Group, [DF03].3.1, [Lan02].I.3**

If $S \subseteq G$ is a subgroup, the product

$$gS \cdot hS = (gh)S$$

is well defined if and only if $S \trianglelefteq G$. We then say that $G/S$ is the **quotient group** of $G$ by $S$.

*Proof.* Suppose that $S \trianglelefteq G$. Fix $s \in S$ and $t \in S$. Fix $g, h \in G$ and write $g' = gs$ and $h' = ht$. We then have

$$\begin{aligned} g'h' &= gsht \\ &= gh(h^{-1}sh)t \\ &\in (gh)S \end{aligned}$$

since $S \trianglelefteq G$. So, $(g'h')S = (gh)S$ and the product is well defined.

Now, consider the converse. Suppose the group operation is well defined. Fix $g \in G$ and $s \in S$. We have that $(gS) \circ (g^{-1}S) = S$ since the product is well defined. Thus,

$$gs \cdot g^{-1}e \in S$$

which tells us that $S \trianglelefteq G$. QED

**Proposition 2.2.5** — **Universal Property of Quotients**

If $f : G \to S$ is a group homomorphism and $S \subseteq G$ is a subgroup such that $S \subseteq \ker f$, there is a unique map $\widetilde{f} : G/S \to H$ making

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle g \mapsto gS}\downarrow & \nearrow_{\widetilde{f}} & \\ G/S & & \end{array}$$

commute. If $S \trianglelefteq G$, the map $\widetilde{f}$ is a group homomorphism.

*Proof.* Should it exist, $\widetilde{f}$ must satisfy $\widetilde{f}(gS) = f(g)$ for all $g \in G$, this so that the diagram commutes. At once, if this action is well defined it is unique. Moreover, inspection of the group law on $G/S$ with $S \trianglelefteq G$ shows that $\widetilde{f}$ is a group homomorphism.

So, we need only prove that $\widetilde{f}(gS) = f(g)$ is well defined. Indeed, if $gS = g'S$, then there is $s \in S$ such that $g's = g$. Then $ff(g) = (g's) = f(g')f(s) = f(g')$ since $s \in S \subseteq \ker f$. So, $\widetilde{f}(gS) = f(g)$ is well defined and the proof is complete. QED

We next comment on the relationship between kernels and normal subgroups.

**Proposition 2.2.6** **Kernel = Normal Subgroup, [DF03].3.1**

If $G$ is a group, a subgroup $S \subseteq G$ is normal if and only if there is group $H$ and group homomorphism $f : G \to H$ so that $S = \ker f$.

*Proof.* If $S \trianglelefteq G$, consider $q : G \to G/S$ given by $q(g) = gS$ for all $g \in G$. This is clearly a group homomorphism one checks that its kernel is $S$.

On the other hand, we need only show that if $f : G \to H$ is a homomorphism, then $\ker f$ is normal in $G$. Indeed, if $g \in G$ and $s \in \ker f$ then

$$f(gsg^{-1}) = f(g)f(s)f(g)^{-1} = f(g)f(g)^{-1} = e$$

so that $gsg^{-1} \in \ker f$ and $\ker f \trianglelefteq G$ as needed. QED

We end this section with Lagrange's Theorem.

**Lemma 2.2.7** **A Bijection**

Let $G$ be a group and $S \subseteq G$ some subgroup and write $q : G \to G/S$ be the usual projection. Choose some set-theoretic section $\sigma : G/S \to G$ of $q$. Define $\Phi : G \to S \times G/S$ by

$$\Phi(g) = (g(\sigma(gS)^{-1}, gS).$$

The map $\Phi$ is a bijection.

*Proof.* We exhibit an inverse for $\Phi$. Define $\Psi : S \times G/S \to G$ by

$$\Psi(s, gS) = s\sigma(gS).$$

Indeed, we have that if $g \in G$ then

$$\begin{aligned}\Psi(\Phi(G)) &= \Psi(g(\sigma(gS))^{-1}, gS) \\ &= g(\sigma(gS))^{-1}\sigma(gS) \\ &= g.\end{aligned}$$

Moreover, if $s \in S$,

$$\begin{aligned}\Phi(\Psi(s, gS)) &= \Phi(s\sigma(gS)) \\ &= (s\sigma(gS)(\sigma(s(\sigma(gS)S)))^{-1}, s\sigma(gS)S) \\ &= (s\sigma(gS)(\sigma(s(\sigma(gS)S)))^{-1}, gS) && (s \in S \text{ and } \sigma \text{ a section of } q) \\ &= (s\sigma(gS)(\sigma(gS))^{-1}, gS) && (s \in S \text{ and } \sigma \text{ a section of } q) \\ &= (s, gS).\end{aligned}$$

QED

**Corollary 2.2.8** **Lagrange's Theorem, [DF03].3.2, [Lan02]I.2**

If $G$ is a finite group and $S \subseteq G$ is a subgroup, then $|S|$ divides $|G|$ with

$$|G/S| = \frac{|G|}{|S|}.$$

*Proof.* Using the bijection from the preceding lemma, we have

$$|G| = |S \times G/S| = |S| \times |G/S|.$$

Now divide by $|S|$ to complete the proof. QED

**Definition 2.2.9** — **Degree**

If $S \subseteq G$ is a subgroup, we write $[G : S]$ for the cardinality of the quotient $G/S$. This cardinal is called the **degree** of $S$ i $G$.

**Remark** Lagrange's Theorem now simply says that if $S \subseteq G$ is a subgroup of finite $G$ then $[G : S] = |G|/|S|$.

**Proposition 2.2.10** — **Multiplicativity of Degree**

If $A \subseteq B \subseteq G$ is a family of subgroups,

$$[G : A] = [G : B] \cdot [B : A].$$

# 3 Isomorphism Theorems

In this section, we prove a family of results called the isomorphism theorems. They are all corollaries to the universal property of quotients.

**Theorem 3.0.1** — **First Isomorphism Theorem, [DF03].3.3, [Lan02]I.3**

If $f : G \to H$ is a surjective group homomorphism, $G/\ker f \cong H$.

*Proof.* By the universal property of quotients, there is a group homomorphism $\widetilde{f} : G/\ker f \to H$ satisfying $\widetilde{f}(gN) = f(g)$ where $N := \ker f$. Since $f$ is surjective, so is $\widetilde{f}$. It remains to show that $\widetilde{f}$ is injective. If $\widetilde{f}(gN) = e_H$, we then have that $f(g) = e_H$. So, $g \in \ker f$. Then $gN = N$ since $N = \ker f$ is a subgroup of $G$. At once, $\ker \widetilde{f}$ is a singleton and $\widetilde{f}$ is injective. As it is already surjective, it is bijective, whence an isomorphism. QED

Before stating the second isomorphism theorem, we will need a few definitions.

**Definition 3.0.1** — **Normalizer**

If $G$ is a group with subgroup $S$, the **normalizer** of $S$ in $G$ is largest subgroup $N_G(B)$ of $G$ with $S \trianglelefteq N_G(S)$.

**Existence** Any subgroup $S \subseteq G$ has a nomalizer given by

$$N_G(S) = \bigcup_{S \trianglelefteq K \subseteq G} K.$$

The union is not empty since $S \trianglelefteq S \subseteq G$.

**Lemma 3.0.2** — **Subgroup Product**

If $A, B \subseteq G$ are subgroups and $A \subseteq N_G(B)$, then

$$AB := \{ab \in G : a \in A, \ \ b \in B\}$$

is a subgroup of $G$. Moreover, $B \trianglelefteq AB$ and $A \cap B \trianglelefteq A$.

*Proof.* Since $e \in A, B$, we need only show that $AB$ is closed under products and inverses. Indeed, if $a, a' \in A$ and $b, b' \in B$

$$(ab)(a'b') = aa'(a')^{-1}ba'b \in AB$$

since $a'(a')^{-1}ba' \in B$ from $A \subseteq N_G(B)$. Similarly

$$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}(aba^{-1}) \in AB.$$

Now, we show that $B \trianglelefteq AB$. Fix $b_0, b \in B$ and $a \in A$. Then

$$(ab)b_0(ab)^{-1} = a(bb_0b^{-1})a^{-1} \in aBa^{-1} \subseteq B$$

since $A \subseteq N_G(B)$. To show that $a \cap B \trianglelefteq A$, fix $c \in A \cap B$ and $a \in A$. Then $aca^{-1} \in A$ since $A$ is closed under the group operation. It remains only to note $aca^{-1} \in B$ since $c \in B$ and $A \subseteq N_G(G)$. QED

**Theorem 3.0.3** **Second Isomorphism Theorem, [DF03].3.3, [Lan02]I.3**

If $G$ is a group with subgroups $A, B$ such that $A \subseteq N_G(B)$, then

$$AB/B \cong A/(A \cap B).$$

*Proof.* Define $\phi : A \to AB/B$ by $\phi(a) = aB$ which is a homomorphism by inspection. Observe that a generic element of $AB/B$ is of the form $(ab)B$ for some $a \in A$ and $b \in B$. In the quotient,

$$(ab)B = aB \cdot bB = aB.$$

Thus, $\phi$ is surjective. By the first isomorphism theorem, $A/\ker\phi \cong AB/B$. We are done once we show $\ker\phi \subseteq A \cap B$.

By inspection, $A \cap B \subseteq \ker\phi$ since $bB = eB = B$ for any $b \in B$. Indeed, if $g \in G$ then $gB = B$ iff $g \in B$. Thus

$$\ker\phi = \{a \in A : a \in B\} = A \cap B$$

and the proof is complete. QED

**Theorem 3.0.3** **Third Isomorphism Theorem, [DF03].3.3, [Lan02]I.3**

If $G$ is a group and $A, B \trianglelefteq G$ with $A \subseteq B$, then

$$A \trianglelefteq B \quad \text{and } B/A \trianglelefteq G/A$$

and moreover

$$G/A \cong (G/B)/(B/A).$$

*Proof.* The normal containment $A \trianglelefteq B$ follows from $A \trianglelefteq G$. Then $B, A \trianglelefteq G$ implies $B/A \trianglelefteq G/A$ by definition of product in the quotient. It remains to show $G/A \cong (G/B)/(B/A)$.

For this, define $\phi : G \to (G/B)/(B/A)$ by $\phi(g) = (gB)(B/A)$. By inspection, we see that $\phi$ is surjective. Then, if $g \in G$, we have

$$\begin{aligned} \phi(g) = 0 &\iff (gB)(B/A) = 0 \\ &\iff gB \in B/A \\ &\iff g \in A \end{aligned}$$

whence $\ker\phi = A$. So, the result follows from the first isomorphism theorem. QED

**Definition 3.0.3** **Lattice of Subgroups**

If $G$ is a group, there is a poset $\mathbf{sub}(G)$ whose elements are subgroups of $G$ and whose order relation is set containment. If $S \subseteq G$ is a subgroup, we write $\mathbf{sub}_{S\subseteq}(G)$ for the subset whose elements contain $S$.

# 4 Group Actions

Many groups come to us as the group of symmetries of something. The general linear group on a vector space $V$ is a the group of linear symmetries $V \to V$. The symmetric group $\mathfrak{S}_A$ is the set of set-theoretic symmetries of the set $A$. From this, there is a sense that groups should act on objects. Group actions formalize this.

**Definition 4.0.1** **Group Action, [DF03]1.7**

If $G$ is a group and $X$ is a set, a (left) **group action** of $G$ on $X$ is a map

$$\cdot : G \times X \to X$$

satisfying

1. (identity) for all $x \in X$ there holds $e_G \cdot x = x$, and
2. (associativity) for all $g, h \in G$ and $x \in X$ there holds $g \cdot (h \cdot x) = (gh) \cdot x$.

A set $X$ together with a (left) $G$ action is called a (left) $G$ **set**.

**Example** Any group $G$ acts on itself by multiplication. That is, the group multiplication $G \times G \to G$ is also a group action. More generally, if $S \subseteq G$ is a subgroup, $G$ acts on the quotient $G/S$ by left multiplication $g \cdot hS := (gh)S$.

There is another way to package the data of a group action.

**Proposition 4.0.2** **Action as Homomorphism, [DF03].4.1**

Fix a group $G$ and set $X$. There is a bijection between maps $\mu : G \times X \to X$ and maps $M : G \to X^X$; indeed if $M$ is such a map, the corresponding $\mu$ is given for $(g, x) \in G \times X$ by $\mu(g, x) = M(g)(x)$. Under this bijection, $\mu$ is a group action if and only if $M : G \to \mathfrak{S}_X$ is a well defined group homomorphism.

The following is some terminology associated with group homomorphisms.

**Definition 4.0.3** **Kernel, Faithful, [DF03].4.1**

Fix a left $G$ set $X$. The **kernel** of the action is that subgroup $K \trianglelefteq G$

$$K = \{g \in G : g \cdot x = x \text{ for all } x \in X\}$$

If we realize the action as a group homomorphism $G \to \mathfrak{S}_X$, then the kernel of the action is the kernel of the homomorphism. If the kernel is trivial, we say the action is **faithful**.

**Definition 4.0.4** **Stabilizer, Free, [DF03].4.1**

If $X$ is a left $G$ set and $x \in X$, the **stabilizer** of $x$ is that subgroup $\text{stab}_x \subseteq G$ given by

$$\text{stab}_x = \{g \in G : g \cdot x = x\}.$$

If each stabilizer is trivial, we say the action is **free**.

**Definition 4.0.5** **Orbit, Transitive, [DF03].4.1**

If $X$ is a left $G$ set and $x \in X$, the **orbit** of $x$ is that set $Gx \subseteq X$ given by

$$Gx = \{g \cdot x : g \in G\}.$$

One observe that the orbits form a partition of $X$. If there is only a single orbit $Gx = X$, then we say the action is **transitive**.

# A Determinants

In this section, we develop the theory of determinants from (relative) scratch. The exposition is motivated by some notes by Keith Conrad[1] and [Lan02]XIII.4. The plan in to construct an object called the exterior power of a module. We will study this construction in Section 1. In Section 2, we use it to produce the determinant.

A minor sub-goal is to show that once can construct determinants without referring to the sign of permutations. Then, one can use the determinants of permutation matrices to define the sign of a permutation.

We work over a fixed commutative ring $R$ with unit. Module means left, unital $R$-module. If the reader is not familiar with rings and modules, pretend that $R$ is some field, *e.g.* $\mathbb{R}$ or $\mathbb{C}$, and replace the word "module" with "vector space." We assume the reader is familiar with the free modules[2] and quotients.

## A.1 The Tensor and Exterior Power

**Definition 1.1.1** **Multilinear Maps**

If $M_1, ..., M_n, N$ are $R$-modules, an **$n$-multilinear map** $f : M_1 \times \cdots \times M_n \to N$ is a function such that for any $i = 1, ..., n$ and any choice of $m_j \in M_j$ for all $j \neq i$, the induced map

$$f(m_1, ..., m_{i-1}, -, m_{i+1}, ..., m_n) : M_i \to N$$

is linear.

We will single out a specific type of alternating multilinear map for special study.

**Definition 1.1.2** **Alternating Multilinear Maps**

If $M, N$ are $R$-modules, an **alternating multilinear map** $f : M^n \to N$ is an $n$-multilinear map such if $i = 1, ..., n-1$ then for any $m_1, ..., m_n \in M$ there holds

$$f(m_1, ...., m_i, m_{i+1}, ..., m_n) = 0$$

if for any $i, j$ there holds $m_i = m_j$.

These are closely related to another type of map.

**Definition 1.1.3** **Skew Symmetric Multilinear Maps**

If $M, N$ are $R$-modules, an **skew symmetric multilinear map** $f : M^n \to N$ is an $n$-multilinear map such if $i = 1, ..., n-1$ then for any $m_1, ..., m_n \in M$ there holds

$$f(m_1, ...., m_i, m_{i+1}, ..., m_n) = -f(m_1, ..., m_{i+1}, m_i, ..., m_n).$$

**Discussion** It is easy to show (exercise) that over a ring in which 2 is a unit - say over a field of characteristic different from 2 - that skew symmetric maps and alternating maps are exactly the same thing. However, this is not true in general. Consider the usual product $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ which is $\mathbb{Z}_2$-multilinear. It is also skew symmetric since $-1 = 1$ in $\mathbb{Z}_2$. However, it is clearly not alternating. We do have the following lemma.

**Lemma 1.1.4** **Alternating Implies Skew**

Any alternating multilinear map is skew symmetric.

(Alternating) multilinear maps abound in practice, and it would be nice to be able to study them, though the reader is currently asked to take this on faith. However, despite being related to linear maps, multilinear maps are not linear. So, the basic tools of linear algebra can't be brought to bear. The following construction

[1] https://kconrad.math.uconn.edu/blurbs/linmultialg/extmod.pdf

[2] For the reader not familiar with modules, free just means has basis. All vector spaces are free and so this condition be safely ignored.

can be though of as a way around this obstruction: a method of bringing alternating multilinear algebra fully under the preview of standard linear algebra.

**Definition 1.1.5** **Exterior Power**

Fix a module $M$ and a natural number $k$. Let $F^k(M)$ be the free module spanned by the set $M^k$. Consider the submodule $S$ spanned by all elements of the form

$$(m_1, ..., m_i, ..., m_k) + r(m_1, ..., m_i', ..., m_k) - (m_1, ..., m_i + rm_i', ..., m_k)$$
$$\text{for all } i = 1, ..., n \text{ and } m_1, ..., m_i, m_i', ..., m_k \in M \text{ and } r \in R$$

$$(m_1, ..., m_i, ..., m_i, ..., m_k)$$
$$\text{for all } i = 1, ..., k \text{ and all } m_1, ..., m_k \in$$

We define the **$k$-th exterior power of** $M$ to be that module $\Lambda^k M := F^k(M)/S$.

**Notation** By definition, there is a linear map $F^k(M) \to \Lambda^k M$ which is surjective: it sends each element to its equivalence class in the quotient - its $S$ coset. If $(m_1, ..., m_k) \in M^k$ is some tuple, one writes its image under this quotient as $m_1 \wedge \cdots \wedge m_k$. Such a thing could be called an *elementary wedge* As the quotient map is surjective, every element of $\Lambda^k M$ is a linear combination of elementary wedges.

**Discussion** What in the world motivates this definition of $\Lambda^k M$? Let's restrict our attention to the case of $k = 2$ to simplify notation. Observe that if $a, b, c \in M$ and $r \in R$, the submodule $S$ was chosen so that

$$(a + rb) \wedge c = (a \wedge c) + r(b \wedge c)$$

and

$$a \wedge (b + rc) = (a \wedge b) + r(a \wedge c)$$

and

$$a \wedge a = 0.$$

In other words, the formal symbol $\wedge$ is like an "alternating multilinear product on $M$." Indeed, the three equalities above are exactly equivalent to the claim

> The map $\eta : M \times M \to \Lambda^2 M$ by $(a, b) \mapsto a \wedge b$ is alternating multilinear.

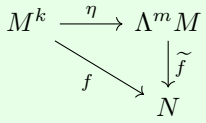
We chose $S$ to force this to happen and otherwise made $S$ as small as possible. In fact, $\Lambda^2 M$ is the "universal" or "best possible" recipient of an alternating multilinear map from $M^2$. We formalize this as follows.

**Theorem 1.1.6** **Universal Property of the Exterior Power**

Fix module $M$ and natural number $k$. The map $\eta : M^k \to \Lambda^k$ given by

$$\eta(m_1, ..., m_k) = m_1 \wedge \cdots \wedge m_k$$

is alternating multilinear. Furthermore, for any other module $N$ and any $f : M^k \to N$ alternating multilinear, there is a unique linear map $\widetilde{f} : \Lambda^k M \to N$ such that the diagram




That is, $f = \widetilde{f} \circ \eta$.

*Proof.* There is a unique linear map $\overline{f} : F^k(M) \to N$ satisfying $\overline{f}(m_1, ..., m_k) = f(m_1, ..., m_k)$ for all $m_1, ..., m_k \in M$ (this just because $F^m(M)$ is free; we specify $\overline{f}$ on the basis). Now, we observe that since $f$ is alternating multilinear, there holds $S \subseteq \ker \overline{f}$ where $S$ is the submodule above yielding $\Lambda^k M = F^k(M)/S$. So, by the fundamental homomorphism theorem, there is unique linear $\widetilde{f} : \Lambda^k M \to N$ making

$$\begin{array}{ccc} F^k(M) & \xrightarrow{\overline{f}} & N \\ \downarrow & \nearrow_{\widetilde{f}} & \\ \Lambda^k M & & \end{array}$$

commute. Explicitly, $\widetilde{f}(m_1 \wedge \cdots \wedge m_k) = f(m_1, ..., m_k)$. From this, $\widetilde{f}$ is the unique map satisfying the desired conclusions of the theorem. QED

The virtue of this theorem is the following:

$$\{\text{Alternating multilinear maps out of } M^k\} = \{\text{linear maps out of } \Lambda^k M\}.$$

A priori, we have no idea how to study the LHS. But, the RHS is subject to the techniques of linear algebra which are well understood.

**Lemma 1.1.6** **Coordinate Choice**

Let $M$ be a rank $n$ free module with basis $B = \{e_1, ..., e_n\}$. For each natural $k$, let

$$A_k = \{(a_1, ..., a_k) \in \{1, ..., n\}^k : a_1 < \cdots < a_k\}.$$

For each $a \in A_k$, let

$$e_{\wedge a} = e_{a_1} \wedge \cdots \wedge e_{a_k}.$$

For each $a \in A_k$, there exists a function $\varphi^a : \Lambda^k M \to R$ such that

$$\varphi^a(e_{\wedge b}) = \begin{cases} 1 & b = a \\ 0 & b \neq a \end{cases}$$

*Proof.* We induct on $k$. The base case in which $\Lambda^1 M = M$ follows from the fact that $M$ is free.

Now, suppose that $k > 1$ and that we have $\varphi^a$ for each $a \in A, A_{k-1}$. Fix $a \in A_k$ and let $a' \in A_{k-1}$ be given by $a' = (a_2, ..., a_k)$. Without loss of generality, suppose that $a = (1, ..., k)$ so that $a' = (2, ..., k)$. For each $m \in M$, let $m' \in M$ be given by the formula

$$m' = \sum_{i=2}^{k} \varphi^i(m) e_i.$$

That is, we identify the hyperplane spanned by the $a'$-indexed basis elements and $m'$ is the linear projection of $m$ onto this hyperplane.

Define $D : M^k \to R$ by the formula

$$D(m_1, ..., m_k) = \sum_{i=1}^{k} (-1)^{i+1} \varphi^1(m_i) \varphi^{a'}(m_1' \wedge \cdots \wedge \widehat{m_i} \wedge \cdots \wedge m_k')$$

where the $\widehat{m_i}$ indicates that this factor is removed. We check that $D$ is multilinear and alternating. Multilinearity is clear since each $m_j$ appears once in each summand and all the maps involved are linear or multilinear. We turn our attention to the alternating property. Fix $i < j$ in $1, ..., k$. Let $m_i = m = m_j$.

Using the fact that $\varphi^{a'}$ is alternating, we have that

$$\begin{aligned} D(...,m,...,m,...) &= (-1)^{i+1}\varphi^1(m)\varphi^{a'}(,...,\widehat{m},...,m,...) + (-1)^{j+1}\varphi^1(m)\varphi(...,m,...,\widehat{m},...) \\ &= (-1)^{i+1}\varphi^1(m)\varphi^{a'}(,...,\widehat{m},...,m,...) + (-1)^{i+(j-i)+1}\varphi^1(m)\varphi(...,m,...,\widehat{m},...) \\ &= (-1)^{i+1}\varphi^1(m)\varphi^{a'}(,...,\widehat{m},...,m,...) + (-1)^{i+(j-i)+1}(-1)^{(j-i)+1}\varphi^1(m)\varphi^{a'}(,...,\widehat{m},...,m,...) \\ &= 0 \end{aligned}$$

where here we use that $\varphi^{a'}$ is skew symmetric. So, $D$ induces $D : \Lambda^k M \to R$. Finally, we check

$$D(e_{\wedge b}) = \begin{cases} 1 & b = (1,...,k) \\ 0 & b \neq (1,...,k) \end{cases}$$

Indeed,

$$D(1,...,k) = \varphi^{a'}(2,...,k) - 0 + 0 - \cdots = 1$$

by definition of $\varphi^{a'}$. Indeed, we see that

$$D(e_{b_1},...,e_{b_k}) = \varphi^1(b_1)\varphi^{a'}(e_{b_2} \wedge \cdots \wedge e_{b_k})$$

since the $b$ multi-index is strictly increasing. Then $\varphi^1(b_1) \neq 0$ iff $b_1 = 1$ and $\varphi^{a'}(e_{b_2} \wedge \cdots \wedge e_{b_k}) \neq 0$ iff $b' = a'$. This concludes the proof. QED

**Remark** Up till this last lemma, the exposition has closely followed Conrad's notes. However, the approach there to this lemma (*c.f.* Theorem 4.2) uses the sign of a permutation in a critical way. To avoid using signs, we adapted Lang's implementation of the cofactor expansion (*c.f.* [Lan02]XIII.4 and the discussion following Corollary 4.9).

**Proposition 1.1.7** **Exterior Power of Free is Free**

If $M$ is a rank $n$ free module with basis $B = \{e_1,...,e_n\}$, then $\Lambda^k M$ is a free module of rank $\binom{n}{k}$ with basis

$$B_k = \{e_{i_1} \wedge \cdots \wedge e_{i_k} : i_1 < \cdots < i_k\}$$

*Proof.* Since $M$ is spanned by $B$ and $\eta : M^k \to \Lambda^k M$ is surjective, multilinear, and alternating, it is not hard to see that $B_k$ spans $\Lambda^k M$. Just take any elementary wedge $m_1 \wedge \cdots \wedge m_k$ write each $m_i$ using the $B$ basis, expand using multilinearity to get a sum of elementary wedges whose "factors" lie in $B$, and use the alternating property to reorder factors till you get an element of $B_k$. So, the real work is showing that $B_k$ is linearly independent, but this follows at once from the preceding coordinate choice lemma. QED

**Corollary 1.1.8** **Top Exterior Power**

If $M$ is a rank $n$ free module, $\Lambda^n M$ is a free module of rank 1. It is called the **top exterior power**.

We finish this section by showing that the exterior powers play well with linear maps.

**Proposition 1.1.9** **Functoriality of $\Lambda^k$**

If $f : M \to N$ is a linear map of modules, there exists a linear map $\Lambda^k f : \Lambda^k M \to \Lambda^k N$ satisfying

$$f(m_1 \wedge \cdots \wedge m_k) = f(m_1) \wedge \cdots \wedge f(m_k)$$

for all $m_1,...,m_k \in M$. Furthermore, if $g : N \to L$ is another map of modules, there holds

$$\Lambda^k g \circ \Lambda^k f = \Lambda^k(g \circ f).$$

Lastly, $\Lambda^k(1_M) = 1_{\Lambda^k M}$.

*Proof.* The claims

$$\Lambda^k g \circ \Lambda^k f = \Lambda^k (g \circ f) \quad \text{and} \quad \Lambda^k (1_M) = 1_{\Lambda^k M}$$

follow by inspection from

$$f(m_1 \wedge \cdots \wedge m_k) = f(m_1) \wedge \cdots \wedge f(m_k)$$

and the fact that $\Lambda^k M$ is spanned by elementary wedges. So, we need only show this last equation.

Define $L^k f : M^k \to N$ by

$$L^k f(m_1, ..., m_k) = f(m_1) \wedge \cdots \wedge f(m_k).$$

This is multilinear and alternating since $f$ is linear and by properties of $\wedge$. By universal property, we get a map $\Lambda^k M \to N$ satisfying

$$f(m_1 \wedge \cdots \wedge m_k) = f(m_1) \wedge \cdots \wedge f(m_k)$$

which concludes the proof. QED

## A.2 The Determinant

We can now define the determinant.

**Definition 1.2.1** **Determinant**

Fix a rank $n$ module $M$ and a linear map $f : M \to M$. The top exterior power $\Lambda^n f : \Lambda^n M \to \Lambda^n M$ is a linear map of rank 1 free modules. That is, it is multiplication by an element of $R$. Call that ring element $\det f$.

From this definition, one can prove all the usual properties of the determinant. Indeed, the crucial fact that $\det(f \circ g) = \det(f) \det(g)$ follows at once from the functoriality property $\Lambda^k(f \circ g) = \Lambda^k f \circ \Lambda^k g$.

Moreover, while *prima facie* abstract , this definition lends itself well to computation. Consider the matrix

$$A = \begin{pmatrix} 3 & 0 & 1 \\ 1 & 2 & 6 \\ 0 & 7 & 0 \end{pmatrix}$$

and suppose we want to compute $\det A$.

First, view $A$ as a linear map $A : \mathbb{Z}^3 \to \mathbb{Z}^3$ (or $\mathbb{R}^3 \to \mathbb{R}^3$, *etc.*) and let $e_1, e_2, e_3$ denote the standard basis. Then $e_1 \wedge e_2 \wedge e_3$ is a basis for $\Lambda^3 \mathbb{Z}^3$. Observe

$$\begin{aligned}
(\Lambda^3 A)(e_1 \wedge e_2 \wedge e_3) &= Ae_1 \wedge Ae_2 \wedge Ae_3 \\
&= (3e_1 + e_2) \wedge (2e_2 + 7e_3) \wedge (e_1 + 6e_2) \\
&= [3e_1 \wedge (2e_2 + 7e_3) \wedge (e_1 + 6e_2)] + [e_2 \wedge (2e_2 + 7e_3) \wedge (e_1 + 6e_2)] \qquad \text{(multilinearity)} \\
&= [3e_1 \wedge 7e_3 \wedge 6e_2] + [e_2 \wedge 7e_3 \wedge e_1] \qquad \text{(alternating property)} \\
&= -126(e_1 \wedge e_2 \wedge e_3) + 7(e_1 \wedge e_2 \wedge e_3) \\
&= (-119)e_1 \wedge e_2 \wedge e_3
\end{aligned}$$

Since

$$(\Lambda^3 A)(e_1 \wedge e_2 \wedge e_3) = \det(A) e_1 \wedge e_2 \wedge e_3,$$

we conclude that $\det(A) = -119$.

# References

[DF03] David S Dummit and Richard M Foote. *Abstract Algebra*. John Wiley & Sons, Nashville, TN, 3 edition, June 2003.

[Lan02] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer, New York, NY, 3 edition, August 2002.