Contents

1. Modules and Categories

Wherever R appears in the text, it will be assumed that it is a ring. In addition, we will assume that every ring has unity, i.e. $1 \in R$ for all rings R.

Definition 1.1 (R-Module #1)**.** *Let R be a ring. A (left) R-module is an abelian group M equipped with a scalar multiplication $R \times M \to M$ by $(r, m) \mapsto r.m = rm$ such that the following four conditions hold:*

- *Right distribution: $r.(m_1 + m_2) = r.m_1 + r.m_2$ for all $r \in R$ and all $m_1, m_2 \in M$.*
- *Left distribution: $(r_1 + r_2).m = r_1.m + r_2.m$ for all $r_1, r_2 \in R$ and all $m \in M$.*
- *Associativity: $r_1.(r_2.m) = (r_1 r_2).m$ for all $r_1, r_2 \in R$ and all $m \in M$.*
- *Identity: $1.m = m$ for all $m \in M$.*

In particular, when R is a field, these are exactly the same axioms as a vector space, as long as M is an abelian group.

We also consider an equivalent definition to Definition 1.1:

Definition 1.2 (R-Module #2)**.** *A left R-module is an abelian group M with a ring homomorphism $\varphi : R \to End(M)$ where $End(M)$ denotes the ring of endomorphisms of M as an abelian group. The ring structure on $End(M)$ is given by the following:*

- *Addition: $f + g$ is given by $(f + g)(m) = f(m) + g(m)$ for all $f, g \in End(M)$ and all $m \in M$.*
- *Multiplication: fg is given by $(fg)(m) = f(g(m))$ for all $f, g \in End(M)$ and all $m \in M$.*
- *Identity: $1 = id_M$.*

Theorem 1.3. *Definition 1.1 and Definition 1.2 are equivalent.*

Proof. Given a scalar multiplication $R \times M \to M$ from Definition 1.1, define $\varphi : R \to \mathrm{End}(M)$ by $r \mapsto (m \mapsto r.m)$; in other words $(\varphi(r))(m) = r.m$. It suffices to show that φ is a ring homomorphism to show that Definition 1.1 implies Definition 1.2. Let $r_1, r_2 \in R$ and let $m \in M$, then

$$(\varphi(r_1 + r_2))(m) = (r_1 + r_2).m = r_1.m + r_2.m = (\varphi(r_1))(m) + (\varphi(r_2))(m),$$

so we have that $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$. Further,

$$(\varphi(r_1 r_2))(m) = r_1 r_2.m = r_1.(r_2.m) = r_1.(\varphi(r_2))(m) = (\varphi(r_1) \circ \varphi(r_2))(m),$$

which means that $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$. Lastly, $(\varphi(1))(m) = 1.m = m$, so $\varphi(1) = \mathrm{id}_M$.

In the other direction, let $\varphi : R \to \mathrm{End}(M)$ be a ring homomorphism and define the scalar multiplication $R \times M \to M$ by $(r, m) \mapsto (\varphi(r))(m) = r.m$. It is then an easy exercise to see that Definition 1.2 implies Definition 1.1. □

Definition 1.4 (Submodule)**.** *Let R be a ring and let M be an R-module. An R-submodule of M is a subgroup $N \leq M$ such that $r.n \in N$ for all $r \in R$ and $n \in N$.*

Lemma 1.5. *Let R be a ring and let M be an R-module, a subset $N \subset M$ is an R-submodule of M if and only if $N \neq \emptyset$ and $x + r.y \in N$ for all $r \in R$ and $x, y \in N$.*

Proof. If N is an R-submodule, then $0 \in N$, hence $N \neq \emptyset$; furthermore, N is closed under addition and action by elements of R.

In the other direction, suppose $N \neq \emptyset$ and $x + r.y \in N$. Recall for a group G and a subset H, we say that H is a subgroup of G if H is nonempty and $xy^{-1} \in H$ for all $x, y \in H$. For abelian groups, this translates to $x - y \in H$ for all $x, y \in H$. Let $r = -1$, then $x + r.y = x - y \in N$ and N is nonempty by hypothesis, therefore $N \leq M$. Finally, let $x = 0$, then $r.y \in N$, hence N is closed under action by R, therefore N is an R-submodule. □

Definition 1.6 (R-Module Homomorphism)**.** *Let M and N be R-modules. An R-module homomorphism $f : M \to N$ is an abelian group homomorphism which preserves scalar multiplication, i.e. $f(r.m) = r.f(m)$ for all $r \in R$ and all $m \in M$.*

Definition 1.7 (R-Module Isomorphism)**.** *An R-module isomorphism $f : M \to N$ is an R-module homomorphism with an inverse R-module map $g : N \to M$ such that $g \circ f = id_M$ and $f \circ g = id_N$.*

Example 1.8. *When the underlying ring structure on a module is a field, the module is a vector space over said field.*

Take, for instance, $R = \mathbb{Q}$, the field of rational numbers. If we have a left $\mathbb{Q}$-module V, then V satisfies the axioms of a vector space when we consider its module structure in addition to the underlying field structure of $\mathbb{Q}$. Furthermore, we can assign a basis to V and we have that $V \cong \mathbb{Q}^{\alpha}$ where $\{v_\alpha\}_{\alpha \in A}$ is a basis of V. In the case that V is a finite-dimensional vector space, $V \cong \mathbb{Q}^n$ where n is the dimension of V, i.e., the number of basis elements needed to capture the structure of V.

Definition 1.9 (Hom_R)**.** *Let R be a ring and let M be a left R-module. Define $Hom_R(R, M)$ to be the set of all R-module homomorphisms $R \to M$.*

We then state the following lemma without proof.

Lemma 1.10. *Let R be a commutative ring. Then, the set $Hom_R(R, M)$ as in Definition 1.9 is an R-module with operations given by $(f + g)(x) = f(x) + g(x)$ for all $f, g \in Hom_R(R, M)$ and $x \in R$, and $(r.f)(x) = r.f(x)$ for all $r, x \in R$ and all $f \in Hom_R(R, M)$.*

Theorem 1.11. *Let R be a commutative ring, then there is an "evaluation" R-module isomorphism $\epsilon : Hom_R(R, M) \to M$ given by $f \mapsto f(1)$.*

Proof. We first show that ϵ is an R-module homomorphism. Let $r \in R$ and $f, g \in \mathrm{Hom}_R(R, M)$, then $\epsilon(r.f) = (r.f)(1) = r.f(1) = r.\epsilon(f)$, and $\epsilon(f + g) = (f + g)(1) = f(1) + g(1) = \epsilon(f) + \epsilon(g)$.

Let $m \in M$ and define $\varphi_m : R \to M$ by $r \mapsto r.m$. Then, $\varphi_m(r_1 r_2) = (r_1 r_2).m = r_1.(r_2.m) = r_1.\varphi_m(r_2)$, and $\varphi_m(r_1 + r_2) = (r_1 + r_2).m = r_1.m + r_2.m = \varphi_m(r_1) + \varphi_m(r_2)$, hence $\varphi_m \in \mathrm{Hom}_R(R, M)$.

Now, define $g : M \to \mathrm{Hom}_R(R, M)$ by $m \to \varphi_m$, we will show that g is an R-module homomorphism and is inverse to ϵ. First, $g(m_1 + m_2)(r) = \varphi_{m_1+m_2}(r) = r.(m_1 + m_2) = r.m_1 + r.m_2 = \varphi_{m_1}(r) + \varphi_{m_2}(r) = g(m_1)(r) + g(m_2)(r)$, and $g(r_1.m)(r_2) = \varphi_{r_1.m}(r_2) = r_2.(r_1.m) = (r_2r_1).m = (r_1r_2).m = \varphi_m(r_1r_2) = r_1.\varphi_m(r_2) = r_1.g(m)(r_2)$, so g is an R-module homomorphism.

Lastly, observe that $(\epsilon \circ g)(m) = \epsilon(g(m)) = \epsilon(\varphi_m) = \varphi_m(1) = 1.m = m$, hence $\epsilon \circ g = \mathrm{id}$, and $(g \circ \epsilon)(f) = g(\epsilon(f)) = g(f(1)) = \varphi_{f(1)}$. It then follows that $\varphi_{f(1)}(r) = r.f(1) = f(r)$, so $\varphi_{f(1)} = f$, hence $(g \circ \epsilon)(f) = f$, and ϵ is an R-module isomorphism. □

Definition 1.12 (Category)**.** *A category $\mathcal{C}$ consists of*

- *A class of objects, denoted $Ob(\mathcal{C})$.*
- *For objects $X, Y \in Ob(\mathcal{C})$, a set of morphisms (or arrows), denoted $Hom_{\mathcal{C}}(X, Y)$.*
- *For objects $X, Y, Z \in Ob(\mathcal{C})$, a composition operation*

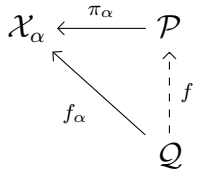
$$Hom_{\mathcal{C}}(Y, Z) \times Hom_{\mathcal{C}}(X, Y) \to Hom_{\mathcal{C}}(X, Z)$$

  given by $(g, f) \mapsto g \circ f$ that is associative when defined, i.e. $h \circ (g \circ f) = (h \circ g) \circ f$.
- *For $X \in Ob(\mathcal{C})$, there is a morphism, denoted id_X or 1_X in $Hom_{\mathcal{C}}(X, X)$ such that $f \circ 1_X = f$ and $1_X \circ g = g$ for all appropriately chosen morphisms f and g.*

Definition 1.13 (Covariant Functor)**.** *Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. A (covariant) functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ associates*

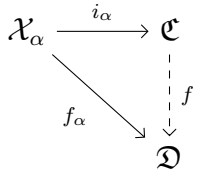
- *to each object $X \in Ob(\mathcal{C})$ an object $\mathcal{F}(X) \in Ob(\mathcal{D})$.*
- *to each arrow/morphism $f : X \to Y$ in $Hom_{\mathcal{C}}(X, Y)$ an arrow $\mathcal{F}(f) : \mathcal{F}(X) \to \mathcal{F}(Y)$ in $Hom_{\mathcal{D}}(\mathcal{F}(X), \mathcal{F}(Y))$ in such a way that preserves composition: $\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$ and identities $\mathcal{F}(1_X) = 1_{\mathcal{F}(X)}$.*

Definition 1.14 (Categorical Products)**.** *Let $\mathcal{C}$ be a category. Let $\mathcal{F} = \{\mathcal{X}_\alpha\}_\alpha$ be a family of objects such that $\mathcal{X}_\alpha \in Ob(\mathcal{C})$ for all α. A product of $\mathcal{F}$ is an object $\mathcal{P} \in Ob(\mathcal{C})$ equipped with a family of maps $\{\mathcal{P} \xrightarrow{\pi_\alpha} \mathcal{X}_\alpha\}_\alpha$ that is universal: given any object $\mathcal{Q} \in Ob(\mathcal{C})$ and any family $\{\mathcal{Q} \xrightarrow{f_\alpha} \mathcal{X}_\alpha\}_\alpha$ of objects, there exists a unique arrow $f : \mathcal{Q} \to \mathcal{P}$ such that the diagram commutes for all α:*



Definition 1.15 (Categorical Coproducts)**.** *Let $\mathcal{C}$ be a category. Let $\mathcal{F}$ be a family of objects as in Definition 1.14. A coproduct of $\mathcal{F}$ is an object $\mathfrak{C}$ equipped with arrows*

$\{\mathcal{X}_\alpha \xrightarrow{i_\alpha} \mathfrak{C}\}_\alpha$ *which is couniversal: given any object* $\mathfrak{D}$ *and any family* $\{\mathcal{X}_\alpha \xrightarrow{i_\alpha} \mathfrak{D}\}_\alpha$ *of arrows, there is a unique* $f : \mathfrak{C} \to \mathfrak{D}$ *such that the diagram commutes for all* α*:*



Theorem 1.16 (Uniqueness of Universality of Categorical Products)**.** *In Definition 1.14, if* $\mathcal{P}$ *exists, then it is unique up to canonical isomorphism.*

Proof. Suppose there is another solution to the universal property, i.e. there exists an object $\mathcal{P}'$ equipped with a family of maps $\{\mathcal{P}' \xrightarrow{\pi'_\alpha} \mathcal{X}_\alpha\}_\alpha$ which is also universal. By universality of $\mathcal{P}$, the maps $\{\pi'_\alpha\}_\alpha$ induce a unique map $\pi' : \mathcal{P}' \to \mathcal{P}$ such that $\pi'_\alpha = \pi_\alpha \circ \pi'$. Likewise, by universality of $\mathcal{P}'$, the maps $\{\pi_\alpha\}_\alpha$ induce a unique map $\pi : \mathcal{P} \to \mathcal{P}'$ such that $\pi_\alpha = \pi'_\alpha \circ \pi$. It follows that $\pi_\alpha = \pi'_\alpha \circ (\pi \circ \pi' \circ \pi)$, and uniqueness of π implies that $\pi \circ \pi' \circ \pi = \pi$. Likewise, we have that $\pi' = \pi' \circ \pi \circ \pi'$. It's then easy to see that $\pi \circ \pi' = \mathrm{id}$ and $\pi' \circ \pi = \mathrm{id}$ since identity maps are unique, hence $\mathcal{P}$ and $\mathcal{P}'$ are isomorphic. □

The technique used in proving Theorem 1.16 can be extended to any universal mapping problem. This means that any object satisfying a universal mapping problem is unique up to canonical isomorphism. More importantly, this means that if such an object exists, it is independent of its construction. This means is that if we were to construct such an object in radically different ways, in the end we actual construct the same object.

Example 1.17 (Products of Sets)**.** *Let* $\mathfrak{Sets}$ *be the category of sets, and let* $\mathcal{F} = \{\mathcal{X}_\alpha\}_\alpha$ *be a family of sets. Define* $\mathcal{P} := \prod_\alpha \mathcal{X}_\alpha = \{(x_\alpha)_\alpha : x_\alpha \in \mathcal{X}_\alpha \text{ for all } \alpha\}$*. Define* $\pi_\alpha : \mathcal{P} \to \mathcal{X}_\alpha$ *as projections, i.e.* $\pi_\alpha((x_\beta)_\beta) = x_\alpha$*. We claim that* $\mathcal{P}$ *is a product of* $\mathcal{F}$*.*

Proof. Let $\mathcal{Q}$ be any set, and let $\{\mathcal{Q} \xrightarrow{f_\alpha} \mathcal{X}_\alpha\}_\alpha$ be any family of set maps. Define $f : \mathcal{Q} \to \mathcal{P}$ by $f(q) = (f_\alpha(q))_\alpha$. Then, $(\pi_\alpha \circ f)(q) = \pi_\alpha(f(q)) = \pi_\alpha((f_\beta(q))_\beta) = f_\alpha(q)$, hence $\pi_\alpha \circ f = f_\alpha$. □

While this example may seem easy and innocent, it is incredibly powerful in its generality. We will now be able to consider products of arbitrary classifications of sets in a very natural, straightforward manner that is consistent with our intuition on products.

Example 1.18 (Products of R-Modules)**.** *Let* R *be a ring and let* $\mathcal{C}$ *be the category of* R*-modules. Let* $\mathcal{F} = \{\mathcal{X}_\alpha\}_\alpha$ *be a family of* R*-modules. Define* $\mathcal{P}$ *(as a set) as* $\mathcal{P} = \prod_\alpha \mathcal{X}_\alpha$ *equipped with projections* $\{\pi_\alpha\}_\alpha$ *as per Example 1.17. Define the module operations component-wise by* $(x_\alpha)_\alpha + (y_\alpha)_\alpha = (x_\alpha + y_\alpha)_\alpha$ *and* $r.(x_\alpha)_\alpha = (r.x_\alpha)_\alpha$*. We claim that* $\mathcal{P}$ *is a product of* R*-modules.*

Proof. We must first check that π_α are actually R-module maps as per Definition 1.6. This follows from our definition of the module operations:

$$\pi_\alpha(r.(x_\beta)_\beta) = \pi_\alpha((r.x_\beta)_\beta) = r.x_\alpha = r.\pi_\alpha((x_\beta)_\beta),$$

and

$$\pi_\alpha((x_\beta)_\beta + (y_\beta)_\beta) = \pi_\alpha((x_\beta + y_\beta)_\beta) = x_\alpha + y_\alpha = \pi_\alpha(x_\beta)_\beta) + \pi_\alpha(y_\beta)_\beta).$$

Let $\mathcal{Q}$ be any R-module and let $\{\mathcal{Q} \xrightarrow{f_\alpha} \mathcal{X}_\alpha\}_\alpha$ be a family of R-module maps. As sets, these induce a unique map $f : \mathcal{Q} \to \mathcal{P}$ such that $f_\alpha = \pi_\alpha \circ f$, i.e., $f(q) = (f_\alpha(q))_\alpha$. We now need to check that f is an R-module map; so,

$$f(q + q') = (f_\alpha(q + q'))_\alpha = (f_\alpha(q) + f_\alpha(q'))_\alpha = (f_\alpha(q))_\alpha + (f_\alpha(q'))_\alpha = f(q) + f(q'),$$

and

$$f(r.q) = (f_\alpha(r.q))_\alpha = (r.f_\alpha(q))_\alpha = r.(f_\alpha(q))_\alpha = r.f(q);$$

hence f is an R-module map. □

Now that we've answered the question of what the product of R-modules are, we will now look at the coproduct of R-modules.

Example 1.19 (Coproducts of R-Modules)**.** *Let R be a ring, let $\mathcal{C}$ be the category of R-modules, and let $\mathcal{F} = \{\mathcal{X}_\alpha\}_\alpha$ be a family of R-modules. Let $\mathfrak{C} = \{(x_\alpha)_\alpha \in \prod_\alpha \mathcal{X}_\alpha : x_\alpha = 0$ for all but finitely many $\alpha\}$. We claim that $\mathfrak{C}$ is the coproduct of R-modules.*

Proof. Let $\mathfrak{D}$ be any R-module and let $\{\mathcal{X}_\alpha \xrightarrow{f_\alpha} \mathfrak{D}\}_\alpha$ be any family of R-module maps. Let $\{i_\alpha\}_\alpha$ be the family of canonical inclusions and denote $e_\alpha := i_\alpha(1)$. Define $f : \mathfrak{C} \to \mathfrak{D}$ by $f((x_\alpha)_\alpha) = \sum_\alpha f_\alpha(x_\alpha)$. Then, $f(i_\alpha(x)) = f(xe_\alpha) = f_\alpha(x)$, so $f \circ i_\alpha = f_\alpha$. We now consider the following:

$$f(r.(x_\alpha)_\alpha) = f((r.x_\alpha)_\alpha) = \sum_\alpha f_\alpha(r.x_\alpha) = r.\sum_\alpha f_\alpha(x_\alpha) = r.f((x_\alpha)_\alpha),$$

and

$$\begin{aligned} f((x_\alpha)_\alpha + (y_\alpha)_\alpha) &= f((x_\alpha + y_\alpha)_\alpha) = \sum_\alpha f_\alpha(x_\alpha + y_\alpha) = \sum_\alpha f_\alpha(x_\alpha) + \sum_\alpha f_\alpha(y_\alpha) \\ &= f((x_\alpha)_\alpha) + f((y_\alpha)_\alpha); \end{aligned}$$

hence f is an R-module map. Now that we've shown that f is an R-module map, we must show that it is unique, thereby proving our claim. Suppose there is an R-module map $g : \mathfrak{C} \to \mathfrak{D}$ such that $f_\alpha = g \circ i_\alpha$ for all α. We then have

$$g((x_\alpha)_\alpha) = \sum_\alpha g(i_\alpha(x_\alpha)) = \sum_\alpha f_\alpha(x_\alpha) = \sum_\alpha f(i_\alpha(x_\alpha)) = f((x_\alpha)_\alpha),$$

and so $f = g$, thus f is unique. □

This construction works because of a key restriction we placed on $\mathfrak{C}$, namely that its elements are zero at all but *finitely many* positions. Without this restriction, we could not exploit linearity as cavalierly as we did. Furthermore, these two examples demonstrate a useful characteristic of products and coproducts in the category of R-modules: products and coproducts of *finite* families of modules coincide. What this means is that for a *finite* family of R-modules $\{M_1, \ldots, M_n\}$, we have that $M_1 \oplus \cdots \oplus M_n = M_1 \times \cdots \times M_n$.

In light of Definitions 1.14 and 1.15, we make the following observations.

Corollary 1.20. *Let $\mathcal{C}$ be a category, let $\mathcal{F} = \{\mathcal{X}_\alpha\}_\alpha$ with product $\mathcal{P} = \prod_\alpha \mathcal{X}_\alpha$ their product, along with a family of maps $\{\mathcal{P} \xrightarrow{\pi_\alpha} \mathcal{X}_\alpha\}_\alpha$ which are universal. Given any object $\mathcal{Q} \in Ob(\mathcal{C})$ with maps $\{\mathcal{Q} \xrightarrow{f_\alpha} \mathcal{X}_\alpha\}_\alpha$, then*

$$\varphi : Hom_{\mathcal{C}}\left(\mathcal{Q}, \prod_\alpha \mathcal{X}_\alpha\right) \to \prod_\alpha Hom_{\mathcal{C}}(\mathcal{Q}, \mathcal{X}_\alpha)$$

given by $g \mapsto (\pi_\alpha \circ g)_\alpha$ is a natural bijection.

Proof. Using Defintion 1.14 on $\mathcal{Q}$ and its associated maps, we induce a unique map in $\mathrm{Hom}_{\mathcal{C}}(\mathcal{Q}, \mathcal{P})$, so surjetivity is done. We now show that φ is injective; let f, g be maps such that $\varphi(f) = \varphi(g)$, thus $(\pi_\alpha \circ f)_\alpha = (\pi_\alpha \circ g)_\alpha$. For all α, we have $\pi_\alpha \circ f = \pi_\alpha \circ g$, and since $\{\pi_\alpha\}_\alpha$ is universal, it follows that $f = g$, hence φ is injective. □

Corollary 1.21. *Let $\mathcal{C}$ be a category, $\mathcal{F} = \{\mathcal{X}_\alpha\}_\alpha$ a family of objects, and coproduct $\mathfrak{C} = \coprod_\alpha \mathcal{X}_\alpha$ equipped with a family of maps $\{\mathcal{X}_\alpha \xrightarrow{i_\alpha} \mathfrak{C}\}_\alpha$ which is universal. Given any $\mathfrak{D} \in Ob(\mathcal{C})$ with maps $\{\mathcal{X}_\alpha \xrightarrow{f_\alpha} \mathfrak{D}\}_\alpha$, then*

$$\psi : Hom_{\mathcal{C}}\left(\coprod_\alpha \mathcal{X}_\alpha, \mathfrak{D}\right) \to \prod_\alpha Hom_{\mathcal{C}}(\mathcal{X}_\alpha, \mathfrak{D})$$

given by $g \mapsto (g \circ i_\alpha)_\alpha$ is a natural bijection.

Proof. Definition 1.15 induces a unique map in $\mathrm{Hom}_{\mathcal{C}}(\mathfrak{C}, \mathfrak{D})$ for the given object $\mathfrak{D}$ and its morphisms, hence ψ is surjective. Similar to the method used in Theorem 1.20 we conclude that ψ is injective. □

These two corollaries tell us that not only can we induce unique morphisms using universality of products and coproducts, but that the converse is also true. Given a morphism either in to a product or out of a coproduct, we can induce a unique family of morphisms in the same direction. The importance of this observation cannot be overstated, as the next theorem will illustrate.

Theorem 1.22 (Representing Matrices)**.** *Let R be a ring, let $M_1, \ldots, M_n, N_1, \ldots, N_m$ be R-modules, and let $f \in Hom_R(M_1 \oplus \cdots \oplus M_n, N_1 \oplus \cdots \oplus N_m)$. Let $\lambda_i : M_i \to M_1 \oplus \cdots \oplus M_n$ and $\pi_j : N_1 \oplus \cdots \oplus N_m \to N_j$ be the canonical inclusion and projection maps. The representing matrix of f is given by*

$$[f] = \begin{bmatrix} \pi_1 \circ f \circ \lambda_1 & \pi_1 \circ f \circ \lambda_2 & \cdots & \pi_1 \circ f \circ \lambda_n \\ \pi_2 \circ f \circ \lambda_1 & \pi_2 \circ f \circ \lambda_2 & \cdots & \pi_2 \circ f \circ \lambda_n \\ \vdots & \vdots & \ddots & \vdots \\ \pi_m \circ f \circ \lambda_1 & \pi_m \circ f \circ \lambda_2 & \cdots & \pi_m \circ f \circ \lambda_n \end{bmatrix}$$

Proof. This is an immediate consequence of Corollaries 1.20 and 1.21. Since we are considering a finite family of R-modules, then products and coproducts coincide as previous noted, hence

$$\mathrm{Hom}_R\left(\coprod_{i=1}^{n} M_i, \prod_{j=1}^{m} N_j\right) \longleftrightarrow \prod_{j=1}^{m} \mathrm{Hom}_R\left(\coprod_{i=1}^{n} M_i, N_j\right) \longleftrightarrow \prod_{j=1}^{m}\prod_{i=1}^{n} \mathrm{Hom}_R(M_i, N_j)$$

given by

$$f \mapsto \begin{bmatrix} \pi_1 \circ f \\ \pi_2 \circ f \\ \vdots \\ \pi_j \circ f \end{bmatrix} \mapsto [f].$$

Since the maps we are dealing with are bijective, we can reverse the process and recover f from $[f]$. □

This allows us to consider R-module maps between (finite) products in a way similar to that of matrix multiplication! Of course, the next natural question is whether the representation matrix of a composite of two such functions can be represented as a product of the individual representation matrices.

Theorem 1.23 (Matrix Composition)**.** *Let R be a ring, let $f \in Hom_R(M_1 \oplus \cdots \oplus M_n, N_1 \oplus \cdots \oplus N_m)$, and let $g \in Hom_R(N_1 \oplus \cdots \oplus N_m, P_1 \oplus \cdots \oplus P_r)$. Let $\{\lambda_j\}$ be canonical inclusion maps for the M modules, let $\{\rho_k\}$ and $\{\mu_k\}$ be canonical projection and inclusion maps for the N modules, and let $\{\pi_i\}$ be canonical projection maps for the P modules. Then, $[g \circ f] = [g][f]$.*

Proof. Define $[g]_{ik} := \pi_i \circ g \circ \mu_k$, define $[f]_{kj} := \rho_k \circ f \circ \lambda_j$, and define $[g \circ f]_{ij} = \pi_i \circ (g \circ f) \circ \lambda_j$. Fix i and j and consider the following:

$$\begin{aligned} ([g][f])_{ij} = \sum_{k=1}^{m} [g]_{ik} \circ [f]_{kj} &= \sum_{k=1}^{m} \pi_i \circ g \circ (\mu_k \circ \rho_k) \circ f \circ \lambda_j \\ &= \pi_i \circ g \circ \left(\sum_{k=1}^{m} \mu_k \circ \rho_k\right) \circ f \circ \lambda_j. \end{aligned}$$

Fix k and consider $(\mu_k \circ \rho_k)(n_1, \ldots, n_m) = \mu_k(n_k) = (0, \ldots, 0, n_k, 0, \ldots, 0)$ where all but the k-th coordinate is zero. It then follows that the sum of the $\mu_k \circ \rho_k$ terms yields the identity. This means that $([g][f])_{ij} = \pi_i \circ (g \circ f) \circ \lambda_j = [g \circ f]_{ij}$, hence $[g][f] = [g \circ f]$. □

2. Exact Sequences

Definition 2.1 (Exact Sequences)**.** *Let R be a ring. Let $M_2 \xrightarrow{u} M_1 \xrightarrow{v} M_0$ be a sequence of maps.*

- *The sequence is said to be a complex if $v \circ u = 0$; in other words, $Im(u) \subset Ker(v)$.*
- *The sequence is exact at M_1 if $Im(u) = Ker(v)$.*

- *A sequence* $\cdots \longrightarrow C_{n+1} \longrightarrow C_n \longrightarrow C_{n-1} \longrightarrow \cdots$ *is said to be an exact sequence if it is exact at* C_n *for all* n*.*
- *An exact sequence of the form* $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ *is said to be a short exact sequence.*

Example 2.2. $0 \longrightarrow Ker(v) \longrightarrow M \xrightarrow{v} M'' \longrightarrow 0$.

Example 2.3. $0 \to M' \to M \to M/M' \to 0$.

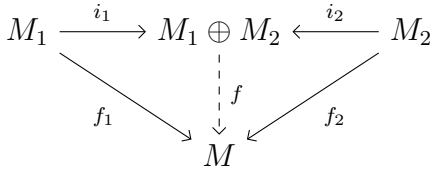
Proposition 2.4. *Let* $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ *of* R*-modules. Then,* u *is injective,* v *is surjective, and* $M'' \cong M/Im(u)$*.*

Proof. Exactness at M' implies that $\mathrm{Ker}(u) = 0$, hence u is injective. Exactness at M'' implies that $\mathrm{Im}(v) = M''$, hence v is surjective. Lastly, we have $M'' = \mathrm{Im}(v) \cong M/\mathrm{Ker}(v) = M/\mathrm{Im}(u)$. □

Short exact sequences are going to play an integral role in helping us recognize direct sums of R-modules. The next few propositions and theorems will address a few situations in which direct sums arise.

Proposition 2.5. *Let* M *be an* R*-module with submodules* $M_1, M_2 \subset M$ *satisfying* $M_1 + M_2 = M$ *and* $M_1 \cap M_2 = 0$*, then* $M \cong M_1 \oplus M_2$*.*

Proof. Define $f_1 : M_1 \hookrightarrow M$ and $f_2 : M_2 \hookrightarrow M$. These maps are clearly R-module maps and therefore induce a unique map $f : M_1 \oplus M_2 \to M$ such that the diagram



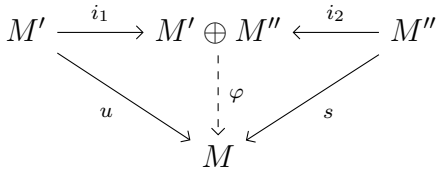
commutes, where i_1 and i_2 are the universal inclusion maps. Let $(m_1, m_2) \in \mathrm{Ker}(f)$, then by definition of f_1 and f_2, this means that $m_1 + m_2 = 0$, and it follows that $m_1 = m_2 = 0$, so f is injective. Let $m \in M$, and let $m_1 \in M_1$ and $m_2 \in M_2$ such that $m = m_1 + m_2$. We then have that $f(m_1, m_2) = f_1(m_1) + f_2(m_2) = m_1 + m_2 = m$, so f is surjective. □

Definition 2.6 (Sections)**.** *A section of a map* $p : M \to M''$ *is a map* $s : M'' \to M$ *such that* $p \circ s = id_{M''}$*.*

Definition 2.7 (Retractions)**.** *Given a map* $i : M' \to M$*, a retraction of* i *is a map* $r : M \to M'$ *such that* $r \circ i = id_{M'}$*.*

Theorem 2.8. *Let* $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{p} M'' \longrightarrow 0$ *be an exact sequence of* R*-modules. Suppose* $s : M'' \to M$ *is a section of* p*, i.e.* s *is an* R*-module map such that* $p \circ s = id_{M''}$*. Then,* $M \cong M' \oplus M''$*.*

Proof. We have maps $u : M' \to M$ and $s : M'' \to M$, hence the universal mapping property of coproducts induces a unique R-module map $\varphi : M' \oplus M'' \to M$ such that the diagram

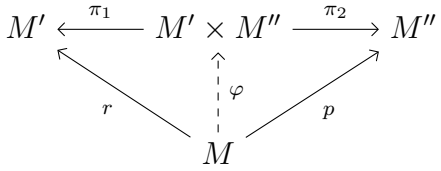


commutes. In particular, this means that $\varphi(m', m'') = u(m') + s(m'')$. Our goal will now be to show that φ is in fact an isomorphism. Let $(m', m'') \in \mathrm{Ker}(\varphi)$, so it follows that $u(m') + s(m'') = 0$ and $pu(m') + ps(m'') = 0$. Since $p \circ u = 0$ and $p \circ s = \mathrm{id}_{M''}$, then $m'' = 0$. This implies that $u(m') = 0$ and since u is an injection, we therefore conclude that φ is an injection as well. Now, let $m \in M$ and note that $m - sp(m) \in \mathrm{Ker}(p)$, since $p(m) - psp(m) = p(m) - p(m)$ by the property that $p \circ s = \mathrm{id}_{M''}$. This means that $m - sp(m) \in \mathrm{Im}(u)$, so there is some $m' \in M'$ such that $u(m') = m - sp(m)$. It then follows that $\varphi(m', p(m)) = u(m') + p(m'') = m - sp(m) + sp(m) = m$, so φ is surjective. □

Theorem 2.9. *Let* $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{p} M'' \longrightarrow 0$ *be an exact sequence of* R*-modules. Suppose* $r : M \to M'$ *is a retraction of* u*, i.e.* r *is an* R*-module map such that* $r \circ u = id_{M'}$*. Then* $M \cong M' \oplus M''$*.*

Proof. We could easily construct an argument similar to that of Theorem 2.8 to prove our claim, but that's no fun. Instead, we're going to show that given a retraction of u, we can construct a section of p, and our conclusion will follow.

First, we have maps $r : M \to M'$ and $p : M \to M''$, which by the universal mapping property of products induces a unique R-module map $\varphi : M \to M' \times M''$ such that the diagram



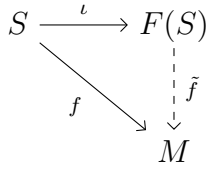
commutes. Our claim is that $p|_{\mathrm{Ker}(r)} : \mathrm{Ker}(r) \to M''$ is an isomorphism, so we need only show that it is bijective.

Let $m \in \mathrm{Ker}(p|_{\mathrm{Ker}(r)})$, and so $m \in \mathrm{Ker}(r) \cap \mathrm{Ker}(p) = \mathrm{Ker}(r) \cap \mathrm{Im}(u)$. This means there is $m' \in M'$ such that $u(m') = m$, which in turn implies $ru(m') = r(m)$. From this it follows that $m' = 0$ since r is a retraction of u, and m is in the kernel of r, hence $p|_{\mathrm{Ker}(r)}$ is injective.

Now, let $m'' \in M''$ and since p is surjective, there is $m \in M$ such that $p(m) = m''$. It is easy to show that $m - ur(m) \in \mathrm{Ker}(r)$, and so $(p|_{\mathrm{Ker}(r)})(m - ur(m)) = p(m - ur(m)) = p(m) - pur(m) = p(m) = m''$. Therefore $p|_{\mathrm{Ker}(r)}$ is bijective. This means that we can define $s = (p|_{\mathrm{Ker}(r)})^{-1} : M'' \to M$, which is clearly a section of p. Since p has a section, then $M \cong M' \oplus M''$ by Theorem 2.8. □

3. Free Modules

Definition 3.1 (Free R-modules)**.** *Let S be any set. A free R-module on S is an R-module $F(S)$ equipped with a set map $\iota : S \to F(S)$ which is universal: i.e. given any R-module M and any set map $f : S \to M$, there is a unique R-module map $\tilde{f} : F(S) \to M$ making the diagram*



commute.

Recall from our previous observations when dealing with universal mapping properties of products and coproducts that if such an object exists, it is unique up to canonical isomorphism. The next theorem will demonstrate a construction of such a free module, hence the object constructed is the *only* such object that can exist.

Theorem 3.2 (Free R-Module Construction)**.** *Let R be a ring and let S be any set, then*

$$F(S) = \coprod_{s \in S} R.$$

Proof. Let M be any R-module and let $f : S \to M$ be any set function. Define $\tilde{f} : F(S) \to M$ by $(r_s)_s \mapsto \sum_{s \in S} r_s.f(s)$. The fact that $f = \tilde{f} \circ \iota$ follows directly from our definition of $\tilde{f}$, so we must now show that it is an R-module map:

$$\begin{aligned} \tilde{f}((r_s)_s + (p_s)_s) = \tilde{f}((r_s + p_s)_s) = \sum_{s \in S} (r_s + p_s).f(s) &= \sum_{s \in S} r_s.f(s) + \sum_{s \in S} p_s.f(s) \\ &= \tilde{f}((r_s)_s) + \tilde{f}((p_s)_s) \end{aligned}$$

and

$$\tilde{f}(r.(p_s)_s) = \tilde{f}((r.p_s)_s) = \sum_{s \in S} (r.p_s).f(s) = r.\sum_{s \in S} p_s.f(s) = r.\tilde{f}((p_s)_s).$$

These properties confirm that $\tilde{f}$ is indeed an R-module map.

We will now show that $\tilde{f}$ is a unique R-module map, hence $F(S)$ with ι is universal. Let $\tilde{g} : F(S) \to M$ be an R-module map such that $f = \tilde{g} \circ \iota$. Then,

$$\begin{aligned} \tilde{g}((r_s)_s) &= \tilde{g}\left(\sum_{s \in S} r_s.\iota(s)\right) = \sum_{s \in S} \tilde{g}(r_s.\iota(s)) = \sum_{s \in S} r_s.\tilde{g}(\iota(s)) = \sum_{s \in S} r_s.f(s) \\ &= \sum_{s \in S} r_s.\tilde{f}(\iota(s)) = \sum_{s \in S} \tilde{f}(r_s.\iota(s)) = \tilde{f}\left(\sum_{s \in S} r_s.\iota(s)\right) = \tilde{f}((r_s)_s); \end{aligned}$$

therefore $\tilde{g} = \tilde{f}$, and we're done. □

Notice that we defined $F(S)$ in terms of coproducts instead of in terms of products. This means that given any element $(m_s)_s \in F(S)$, then there is a finite subset $A \subset S$ such that $m_x = 0$ if and only if $x \notin A$. In essence, this says that any element in $F(S)$ can be expressed (not necessarily uniquely) as a finite sum $\sum_{a \in A} r_a.e_a$ where $e_a := \iota(a)$.

4. $\mathbb{Z}^n = \mathbb{Z}^m$ implies $n = m$

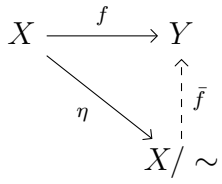
To prove the claim in the title of this section, we must first develop some additional theory. Our approach will be that of rephrasing the problem in terms of vector spaces. In addition, throughout this section, unless otherwise specified, we will assume that R is a commutative ring.

Theorem 4.1 (Correspondence Theorem for Groups)**.** *Let G be a group. If $K \lhd G$, then there is a lattice isomorphism*

$$\{H \leq G : K \subset H \subset G\} \longleftrightarrow \{H \leq G/K\}.$$

Before we prove this claim, we will consider an analogous problem in set theory. Consider a set map $f : X \to Y$ between two sets X and Y. In general, we know that $S \subset f^{-1}(f(S))$ and $f(f^{-1}(T)) \subset T$ for arbitrarily subsets $S \subset X$ and $T \subset Y$, but when do we have set equality? For starters, if f is surjective, then $f(f^{-1}(T)) = T$, so when do we have $S = f^{-1}(f(S))$?

To answer this question, recall that f induces an equivalence relation $\sim$ on X where $x_1 \sim x_2$ if and only if $f(x_1) = f(x_2)$. Let $X/\sim$ be be set of equivalence classes, and note that there is a unique map $\bar{f}$ such that the diagram



commutes where η sends each element to its respective equivalence class. We then claim that set equality holds when S is *saturated*, i.e. S is a union of equivalence classes. To prove our claim, let $s \in f^{-1}(f(S))$ where S is saturated, then $f(s) \in f(S)$ and $f^{-1}(f(s)) \subset S$. But $f^{-1}(f(s)) = [s]$ where $[s]$ denotes the equivalence class of s, so $[s] \subset S$ and it then follows that $s \in S$.

The result of these observations allows us to say that if $f : X \to Y$ is surjective, then there is a bijection between the saturated subsets of X and the subsets of Y, i.e.:

$$\{\text{saturated subsets of } X\} \longleftrightarrow \{\text{subsets of } Y\}.$$

Proof of Theorem 4.1. From the observations we just made, we note that in the context of group theory, equivalence classes are cosets of subgroups. We then take the canonical projection map $\pi : G \to G/K$ to be our surjective map, and our saturated subsets to be subgroups of G such that $K \subset H \subset G$. Applying this directly to our observations above, we have $X = G$, $Y = G/K$, and $f = \pi$. □

Theorem 4.2. *Let R be a commutative ring with an ideal I, then R/I is a field if and only if I is maximal.*

Proof. The Correspondence Theorem extends well beyond mere group theory and can be applied to the context of ring theory as well. In this sense, if we assume that R/I

is a field, then we know that it contains only two ideals: R and 0. However, the Correspondence Theorem then tells us that there can only be two ideals between R and I, namely R and I themselves, hence I is a maximal ideal. Similarly, if I is a maximal ideal, any ideal between R and I must be either R or I, hence R/I is a field. □

Example 4.3. *Let p be a prime. Then $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$, hence $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Let I be an ideal such that $p\mathbb{Z} \subset I \subset \mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, then $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. This means that $p \in n\mathbb{Z}$, hence $n|p$, but this implies that $n = 1$ or $n = p$, hence $I = p\mathbb{Z}$ or $I = \mathbb{Z}$.

Lemma 4.4. *Let M and N be R-modules, and let $M' \subset M$ and $N' \subset M$ be submodules, then*

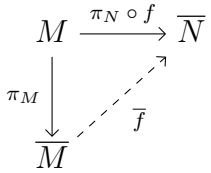
$$\frac{M \oplus N}{M' \oplus N'} \cong \frac{M}{M'} \oplus \frac{N}{N'}.$$

Proof. The canonical projections $M \to M/M'$ and $N \to N/N'$ induce a surjective map $M \oplus N \to M/M' \oplus N/N'$ given by $(m, n) \mapsto (\overline{m}, \overline{n})$. The kernel of this map is $M' \oplus N'$, hence by the First Isomorphism Theorem, our conclusion follows. □

Definition 4.5. *Let R be a ring and let $\mathfrak{m}$ be a maximal ideal in R. For any R-module M, we denote the $R/\mathfrak{m}$-module $M/(\mathfrak{m}M)$ by $\overline{M}$.*

Lemma 4.6. *Let R be a ring and let $\mathfrak{m}$ be a maximal ideal. Given an R-module map $f : M \to N$, there is a unique map $\overline{f} : \overline{M} \to \overline{N}$ such that $\pi_N \circ f = \overline{f} \circ \pi_M$, where π_M and π_N are the canonical projection maps.*

Proof. Our goal is to induce a map $\overline{f}$ which makes the diagram



commute. We will do so by showing that $\mathfrak{m}M \subset \mathrm{Ker}(\pi_N \circ f)$. Let $x.m \in \mathfrak{m}M$ and note that $f(x.m) = x.f(m) \in \mathfrak{m}N$, so $\pi_N(f(x.m)) = 0$ and so $\mathfrak{m}M \subset \mathrm{Ker}(\pi_N \circ f)$. The fundamental theorem on homomorphisms then induces the desired unique map. □

Proposition 4.7. *Let R be a ring and let $\mathfrak{m}$ be a maximal ideal in R. Let $\mathcal{C}$ be the category of R-modules and let $\mathcal{D}$ be the category of $R/\mathfrak{m}$-modules. Define $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ on objects by $M \mapsto \overline{M}$ and on arrows $f \mapsto \overline{f}$, given by Lemma 4.6. Then $\mathcal{F}$ is a functor.*

Proof. Let $f : M \to N$ and $g : N \to P$ be R-modules maps. We must show that $\mathcal{F}(g) \circ \mathcal{F}(f) = \mathcal{F}(g \circ f)$, or in other words that $\overline{g} \circ \overline{f} = \overline{g \circ f}$. This is most easily seen by the observation that

$$\overline{g \circ f} \circ \pi_M = \pi_P \circ g \circ f = \overline{g} \circ \pi_N \circ f = (\overline{g} \circ \overline{f}) \circ \pi_M.$$

Our desired identity follows by uniqueness of $\overline{g \circ f}$; it is then easy to show that $\mathcal{F}$ preserves identities. □

Lemma 4.8. *Let R be a ring and let M and N be R-modules, then $\overline{M \oplus N} \cong \overline{M} \oplus \overline{N}$.*

Proof. This follows almost immediately from Lemma 4.4, but we will make this explicit as follows:

$$\overline{M \oplus N} = \frac{M \oplus N}{\mathfrak{m}(M \oplus N)} = \frac{M \oplus N}{\mathfrak{m}M \oplus \mathfrak{m}N} \cong \frac{M}{\mathfrak{m}M} \oplus \frac{N}{\mathfrak{m}M} = \overline{M} \oplus \overline{N}.$$

□

We are now ready to prove our desired theorem, which will imply the title of this section.

Theorem 4.9. *Let R be a commutative ring. If $R^n \cong R^m$, then $n = m$.*

Proof. Let $\varphi : R^n \to R^m$ be an isomorphism of R-modules and let $\mathfrak{m}$ be a maximal ideal of R. Applying our functor from Proposition 4.7 along with Lemma 4.8, we induce a map

$$\overline{\varphi} : \overline{R}^n \to \overline{R}^m$$

which is an isomorphism of $\overline{R}$-modules. However, Theorem 4.2 says that $\overline{R}$ is a field, hence we have an isomorphism of finite-dimensional vector spaces, therefore $n = m$. □

To obtain this result, we made a key assumption that R was a commutative ring. This begs the question: can we obtain the same result if we were to omit the hypothesis that R was commutative? The answer is *yes*, provided R contains a commutative ideal I. We could then consider R/I which yields a commutative quotient and then apply Theorem 4.9 to the quotient.

5. Modules of Fractions

This section will be motivated by the construction of the rationals from the integers. We will consider a commutative ring R and let S be a multiplicatively closed subset of R which contains 1_R. Our goal will be to construct a ring, denoted by $S^{-1}R$, with a universal mapping property. The first step will be to put an equivalence relation on $R \times S$ as the next proposition will demonstrate.

Proposition 5.1. *Define a relation $(a, s) \sim (a', s')$ if and only if there exists $t \in S$ such that $tsa' = ts'a$. Then, $\sim$ defines an equivalence relation on $R \times S$.*

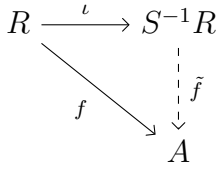
Proof. We must show reflexivity, symmetry, and transitivity of $\sim$. Reflexivity follows since $1 \in S$; likewise, symmetry follows since equality is also symmetric. Lastly, suppose $(a, s) \sim (a', s')$ and that $(a', s') \sim (a'', s'')$ and let $t, u \in S$ such that $tas' = ta's$ and $ua's'' = ua''s'$. Multiplying the first equation by us'' and the second by ts, we have

$$tuas's'' = tua'ss'' \qquad \text{and} \qquad tua'ss'' = tua''ss',$$

so it follows that $tuas's'' = tua''ss'$, and so $(tus')as'' = (tus')a''s$. Since $tus' \in S$, then this demonstrates transitivity, hence $(a, s) \sim (a'', s'')$. □

For convenience, we denote $(a, s) \in R \times S$ by $\frac{a}{s}$. We then define addition on $R \times S$ by $\frac{a}{s} + \frac{a'}{s'} = \frac{as'+a's}{ss'}$ and multiplication by $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$. Once we confirm that these operations are well-defined, we will have constructed our ring desired $S^{-1}R$.

Definition 5.2 (Ring of Fractions)**.** *Let R be a commutative ring and $S \subset R$ a multiplicatively closed set such that $1 \in S$. The ring of fractions of R with respect to S is a ring denoted $S^{-1}R$ equipped with a map $\iota : R \to S^{-1}R$ which is universal: i.e. given any commutative ring A and any ring map $f : R \to A$, there is a unique ring map $\tilde{f} : S^{-1}R \to A$ such that the diagram*



commutes.

We've already constructed $S^{-1}R$, so all that remains is to show that it satisfies the universal mapping property as described in Definition 5.2.

Theorem 5.3. *The ring $S^{-1}R$ as previous constructed satisfies the universal mapping property with $\iota : R \to S^{-1}R$ given by $\iota(r) = \frac{r}{1}$.*

Proof. Let A be any ring and let $f : R \to A$ be any ring map. Define $\tilde{f} : S^{-1}R \to A$ by $\tilde{f}(\frac{r}{s}) = f(r)f(s)^{-1}$. We must first show that this map is well-defined, so suppose $(r, s) \sim (r', s')$, so there is $t \in S$ such that $trs' = tr's$. This means that $f(t)f(r)f(s') = f(t)f(r')f(s)$, then multiply both sides by $f(t)^{-1}f(s)^{-1}f(s')^{-1}$. It then follows that $f(r)f(s)^{-1} = f(r')f(s')^{-1}$, therefore $\tilde{f}$ is well-defined. We then observe that $\tilde{f}(\iota(r)) = \tilde{f}(r/1) = f(r)f(1)^{-1} = f(r)$, hence $f = \tilde{f} \circ \iota$. Next, we will show that $\tilde{f}$ is a ring map, so we have

$$\begin{aligned} \tilde{f}\left(\frac{r}{s} + \frac{r'}{s'}\right) &= \tilde{f}\left(\frac{rs' + r's}{ss'}\right) = f(rs' + r's)f(ss')^{-1} \\ &= f(rs')f(ss')^{-1} + f(r's)f(ss')^{-1} \\ &= \tilde{f}\left(\frac{rs'}{ss'}\right) + \tilde{f}\left(\frac{r's}{ss'}\right) = \tilde{f}\left(\frac{r}{s}\right) + \tilde{f}\left(\frac{r'}{s'}\right) \end{aligned}$$

and

$$\tilde{f}\left(\frac{r}{s} \cdot \frac{r'}{s'}\right) = \tilde{f}\left(\frac{rr'}{ss'}\right) = f(rr')f(ss')^{-1} = f(r)f(s)^{-1}f(r')f(s')^{-1} = \tilde{f}\left(\frac{r}{s}\right)\tilde{f}\left(\frac{r'}{s'}\right).$$

All that remains is to show that $\tilde{f}$ is unique. Suppose there is a ring map $\tilde{g} : S^{-1}R \to A$ such that $f = \tilde{g} \circ \iota$. It then follows that

$$\tilde{g}\left(\frac{r}{s}\right) = \tilde{g}\left(\frac{r}{1}\right)\tilde{g}\left(\frac{1}{s}\right) = \tilde{g}(\iota(r))\tilde{g}(\iota(s))^{-1} = f(r)f(s)^{-1} = \tilde{f}\left(\frac{r}{s}\right),$$

therefore $\tilde{f}$ is unique. □

Lemma 5.4. *Let R be a commutative ring and let S be the set of multiplicative units of R, i.e. $S = \{s \in R : \text{ there exists } s^{-1} \in R \text{ such that } ss^{-1} = 1\}$. Then, $S^{-1}R \cong R$.*

Proof. Let $i : R \to R$ be the inclusion map. Definition 5.2 then induces a unique map $\tilde{i} : S^{-1}R \to R$ such that $\tilde{i}(\frac{r}{s}) = i(r)i(s)^{-1} = rs^{-1}$. It is clear that $\tilde{i}(\frac{r}{1}) = r$, hence $\tilde{i}$ is surjective, so it remains to show that it is likewise injective. Let $\frac{r}{s} \in \text{Ker}(\tilde{i})$, hence $rs^{-1} = 1$, therefore uniqueness of inverses implies that $r = s$, hence $\frac{r}{s} = 1$. □

Definition 5.5 (Local Ring)**.** *A commutative ring R is called a local ring if it contains a unique maximal ideal.*

Lemma 5.6. *A commutative ring R is a local ring if and only if the complement of its set of units is an ideal in R. In other words, the set of nonunits form the maximal ideal of a local ring.*

Proof. Suppose R is a local ring and denote its maximal ideal by $\mathfrak{m}$, let U denote the set of units in R. Let $x \notin \mathfrak{m}$ and suppose $x \notin U$. It then follows that (x) is an ideal and is therefore contained in some maximal ideal. However, since $x \notin \mathfrak{m}$ and $\mathfrak{m}$ is the unique maximal ideal in R, this is a contradiction, hence $x \in U$. This means that $x \notin \mathfrak{m}$ implies $x \in U$; or in other words, $x \notin U$ implies that $x \in \mathfrak{m}$. Now, let $x, y \in U^c$ and suppose $x + y \in U$. Since $x, y \notin U$, then $x, y \in \mathfrak{m}$, hence $x + y \in \mathfrak{m}$ as well; however, this implies that $x + y$ is a unit, which further implies that $\mathfrak{m} = R$, a contradiction. It then follows that U^c is closed under addition, and is therefore an ideal in R.

Conversely, suppose U^c is an ideal in R. Let I be an ideal of R such that $U^c \subset I \subset R$. If $I \neq U^c$, then there is some $i \in I$ such that $i \notin U^c$, hence i is a unit; however, this implies that $I = R$, hence U^c is a maximal ideal. Suppose there is another maximal ideal $\mathfrak{m}$ in R. Since $\mathfrak{m}$ is maximal, then it is not identically R and it cannot contain any units, hence $\mathfrak{m} \subset U^c$. Maximality of $\mathfrak{m}$ then implies that $\mathfrak{m} = U^c$, therefore R is a local ring. □

Lemma 5.7 (Localization)**.** *Let R be a commutative ring and let $S = R - \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal in R. Then, $S^{-1}R$ is a local ring; in particular, this is called the localization of R at $\mathfrak{p}$, and denoted $R_{\mathfrak{p}}$.*

Proof. Let $M = \{\frac{p}{s} \in S^{-1}R : p \in \mathfrak{p}, s \in S\}$ and let U be the set of units of $S^{-1}R$. By Lemma 5.6, it suffices to show that M is an ideal such that $M = U^c$. It is clear that M is an ideal since $\frac{r}{s} \cdot \frac{p}{s'} = \frac{rp}{ss'} \in M$ since $rp \in \mathfrak{p}$.

Let $\frac{r}{s} \in U$, hence there is $\frac{r'}{s'} \in S^{-1}R$ and $t \in S$ such that $t(rr' - ss') = 0$. Since $0 \in \mathfrak{p}$ and $t \notin \mathfrak{p}$, then $rr' - ss' \in \mathfrak{p}$. Suppose $r \in \mathfrak{p}$, then $rr' \in \mathfrak{p}$, and so $ss' \in \mathfrak{p}$, a contradiction. This means that $r \notin \mathfrak{p}$, hence $\frac{r}{s} \notin M$, which says that $M \subset U^c$. Now, let $\frac{r}{s} \notin M$ and so $r \notin \mathfrak{p}$, hence $r \in S$. It then follows that $\frac{s}{r}$ is inverse to $\frac{r}{s}$, hence $\frac{r}{s} \in U$. This means that $U^c \subset M$ and $M = U^c$, therefore $S^{-1}R$ is a local ring. □

Definition 5.8 (Reduced Rings)**.** *A ring R is said to be reduced if it contains no nonzero nilpotent elements.*

Theorem 5.9. *Let R be a ring. If $R_{\mathfrak{p}}$ is reduced for all prime ideals $\mathfrak{p}$, then R is likewise reduced.*

Proof. Let $x \in R$ such that x is nonzero and let $\text{ann}(x) = \{r \in R : rx = 0\}$. Since $0 \in \text{ann}(x)$, then $\text{ann}(x) \subset \mathfrak{m}$ for some maximal ideal in R. Furthermore, since maximal ideals are prime ideals, then $R_{\mathfrak{m}}$ is reduced. Suppose that $\frac{x}{1} = \frac{0}{1}$ in $R_{\mathfrak{m}}$, and so it follows that there is $t \notin \mathfrak{m}$ such that $t \cdot x \cdot 1 = t \cdot 1 \cdot 0 = 0$. This means that $t \in \text{ann}(x) \subset \mathfrak{m}$, but $t \in S = R - \mathfrak{m}$, a contradiction. Now, suppose x is nilpotent, so there is $n \in \mathbb{Z}^+$ such that $x^n = 0$. It then follows that since $R_{\mathfrak{m}}$ is reduced, we have $0 = \frac{x^n}{1} = (\frac{x}{1})^n \neq 0$, a contradiction. Therefore x is not nilpotent, and so we conclude that R is reduced. □

Having constructed the ring of fractions of R with respect to S and shown it satisfies the universal mapping property, we now set out to construct modules of fractions from this ring. Given an R-module M, we wish to construct $S^{-1}M$ as an $S^{-1}R$ module. But first, we prove a quick and useful lemma.

Lemma 5.10 (Pullback Module Structures)**.** *Let A and B be rings and $\varphi : A \to B$ a ring map. Then if N is a B-module, then N is also an A-module by "pullback along φ".*

Proof. Since N is a B-module, there is a ring homomorphism $\psi : B \to \text{End}(N)$. We then consider the following diagram

$$\begin{array}{ccc} B & \xrightarrow{\psi} & \text{End}(N) \\ {\scriptstyle\varphi}\uparrow & \nearrow & \\ A & & \end{array}$$

Since ψ and φ are both ring homomorphisms, then $\psi \circ \varphi : A \to \text{End}(N)$ is also a ring homomorphism. Therefore N is an A-module given by $\varphi(a).n$. □

We define an equivalence relation on $M \times S$ by $(m, s) \sim (m', s')$ if and only if there is $t \in S$ such that $t.(s.m') = t.(s'.m)$, similar to what we did previously. Likewise, denote (m, s) by $\frac{m}{s}$ for convenience, and denote $S^{-1}M$ as the collection of all such elements. Define addition and multiplication on $S^{-1}M$ by $\frac{m}{s} + \frac{m'}{s'} = \frac{s'.m+s.m'}{ss'}$ and $\frac{r}{s} \cdot \frac{m}{t} = \frac{r.m}{st}$, thereby endowing $S^{-1}M$ with a $S^{-1}R$-module structure. These operations are well-defined as they were in the case of the ring of fractions; however, we must now be a bit more careful in how we express these relationships now that we are in the context of modules.

Definition 5.11 (Modules of Fractions)**.** *Let $S^{-1}R$ be the ring of fractions of R with respect to S and let M be an R-module. The module of fractions of $S^{-1}R$ is denoted $S^{-1}M$ and is equipped with a map $\iota : M \to S^{-1}M$ which is universal: i.e. given any $S^{-1}R$-module N and any R-module map $f : M \to N$, there is a unique $S^{-1}R$-module map $\tilde{f} : S^{-1}R \to N$ such that the diagram*

$$\begin{array}{ccc} M & \xrightarrow{\iota} & S^{-1}M \\ & {\scriptstyle f}\searrow & \downarrow{\scriptstyle \tilde{f}} \\ & & N \end{array}$$

commutes.

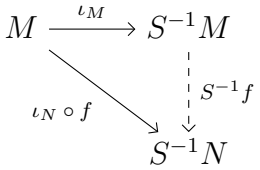
This definition may be a bit confusing, since we're mixing categories, but Lemma 5.10 remedies this confusion. Since N is an $S^{-1}R$-module and there is a ring map $\iota : R \to S^{-1}R$, then N is an R-module map by pullback.

Theorem 5.12. *The module of fractions $S^{-1}M$ as previous constructed satisfies the universal mapping property with $\iota : M \to S^{-1}M$ given by $\iota(m) = \frac{m}{1}$.*

Proof. Let N be any $S^{-1}R$-module and let $f : M \to N$ be any R-module map. Define $\tilde{f} : S^{-1}M \to N$ by $\tilde{f}\left(\frac{m}{s}\right) = \frac{f(m)}{s}$. The proof that $\tilde{f}$ is well-defined, an $S^{-1}R$-module map, and unique follows similarly to that of Theorem 5.3. □

Lemma 5.13. *Let $f : M \to N$ be an R-module map, then there is a unique $S^{-1}R$-module map $S^{-1}f : S^{-1}M \to S^{-1}N$ such that $\iota_N \circ f = S^{-1}f \circ \iota_M$.*

Proof. Invoke Definition 5.11, and let $S^{-1}f$ be the unique $S^{-1}R$-module map making the diagram



commute. □

Theorem 5.14 (Functoriality of $S^{-1}(\cdot)$)**.** *Let $S^{-1}R$ be the ring of fractions of R with respect to S. Let $\mathcal{C}$ be the category of R-modules and $\mathcal{D}$ be the category of $S^{-1}R$-modules. Define $S^{-1}(\cdot) : \mathcal{C} \to \mathcal{D}$ by $M \mapsto S^{-1}M$ on objects and $f \mapsto S^{-1}f$ on arrows. Then, $S^{-1}(\cdot)$ is a functor.*

Proof. Let $f : M \to N$ and $g : N \to P$ be R-module maps. It then follows that

$$S^{-1}(g \circ f) \circ \iota_M = \iota_P \circ g \circ f = S^{-1}g \circ \iota_N \circ f = (S^{-1}g \circ S^{-1}f) \circ \iota_M.$$

Uniqueness of $S^{-1}(g \circ f)$ implies $S^{-1}(\cdot)$ preserves composition, and preservation of identities is readily seen. □

Lemma 5.15. *If $M' \xrightarrow{f} M \xrightarrow{g} M''$ is an exact sequence of R-modules, then $S^{-1}M' \to S^{-1}M \to S^{-1}M''$ is an exact sequence of $S^{-1}R$-modules.*

Proof. Since $g \circ f = 0$ and $S^{-1}(\cdot)$ is a functor, then $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = S^{-1}(0) = 0$, so $\mathrm{Im}(S^{-1}f) \subset \mathrm{Ker}(S^{-1}g)$. Let $\frac{m}{s} \in \mathrm{Ker}(S^{-1}g)$, then $S^{-1}g(\frac{m}{s}) = 0$ and $\frac{g(m)}{s} = 0$. This says that there is $t \in S$ such that $t.1.g(m) = t.s.0$ by our equivalence relation, so $g(t.m) = 0$ and $t.m \in \mathrm{Ker}(g) = \mathrm{Im}(g)$. Then, there is then $x \in M'$ such that $f(x) = t.m$, and it follows that $S^{-1}f(\frac{x}{ts}) = \frac{f(x)}{ts} = \frac{t.m}{ts} = \frac{m}{s}$. □

Lemma 5.16. *Let M and N be R-modules, then*

$$S^{-1}(M \oplus N) \cong S^{-1}M \oplus S^{-1}N.$$

Proof. Let

$$0 \to M \xrightarrow{i} M \oplus N \xrightarrow{\pi} N \to 0$$

be an exact sequence where i and π are canonical inclusion and projection maps, respectively. There is also a retraction $r : M \oplus N \to M$ which is a canonical projection map, i.e. $r \circ i = \mathrm{id}_M$. Since $S^{-1}(\cdot)$ is exact by Lemma 5.15, then we induce an exact sequence

$$0 \to S^{-1}M \xrightarrow{S^{-1}i} S^{-1}(M \oplus N) \xrightarrow{S^{-1}\pi} S^{-1}N \to 0.$$

Functoriality of $S^{-1}(\cdot)$ then implies that $S^{-1}r \circ S^{-1}i = S^{-1}(r \circ i) = S^{-1}(\mathrm{id}_M) = \mathrm{id}_{S^{-1}M}$. This means that $S^{-1}r$ is a retraction of $S^{-1}i$, and our conclusion follows by Theorem 2.9. □

Recall the motivation question behind Theorem 4.9 which asks was whether $\mathbb{Z}^n \cong \mathbb{Z}^m$ implies $n = m$. It turned out that we could prove the result in more generality than the original question posed. In fact, after developing the theory of module of fractions, we can answer the same motivating question very easily.

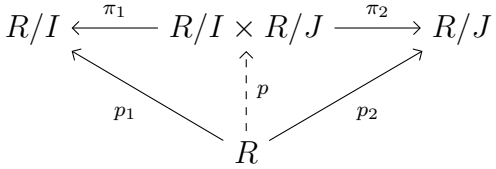
Proposition 5.17. *If $\mathbb{Z}^n \cong \mathbb{Z}^m$, then $n = m$.*

Proof. Let $S = \mathbb{Z} - \{0\}$ and note that $\mathbb{Q} = S^{-1}\mathbb{Z}$, hence exactness of $S^{-1}(\cdot)$ implies that $\mathbb{Q}^n \cong \mathbb{Q}^m$, and so $n = m$. □

6. Chinese Remainder Theorem

Theorem 6.1 (Chinese Remainder Theorem)**.** *Let R be a commutative ring with ideals $I, J \lhd R$ such that $I + J = R$, i.e. I and J are coprime ideals. Then $IJ = I \cap J$ and $R/(IJ) \cong R/I \times R/J$ as rings.*

Proof. Let $p_1 : R \to R/I$ and $p_2 : R \to R/J$ be canonical projection maps. These maps induce a unique map $p : R \to R/I \times R/J$, via the universal mapping property of products in the category of rings, hence the diagram

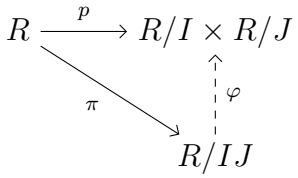


commutes. Our approach will be to show that p is surjective, that $\mathrm{Ker}(p) = I \cap J$, and lastly that $I \cap J = IJ$. First, however, since $I + J = R$, then $1 = i + j$ for some $i \in I$ and $j \in J$. It then follows that $p(i) = (\overline{i}, \overline{i}) = (0, \overline{1} - \overline{j}) = (0, \overline{1})$ and $p(j) = (\overline{j}, \overline{j}) = (\overline{1} - \overline{j}, 0) = (\overline{1}, 0)$. Let $(\overline{a}, \overline{b}) \in R/I \times R/J$, then

$$p(aj + bi) = p(aj) + p(bi) = (\overline{a}, \overline{a}) \cdot (\overline{j}, \overline{j}) + (\overline{b}, \overline{b}) \cdot (\overline{i}, \overline{i}) = (\overline{a}, 0) + (0, \overline{b}) = (\overline{a}, \overline{b}).$$

Since p was induced via canonical projection maps, then we must have that $\mathrm{Ker}(p) = I \cap J$. Next, we will show that $I \cap J = IJ$. Let $xy \in IJ$, then ideality of I imples that

$xy \in I$ and ideality of J implies that $xy \in J$, hence $xy \in I \cap J$. Now, let $x \in I \cap J$, then $x = 1x = (i+j)x = ix + jx$, then $ix \in IJ$ and $jx \in IJ$ as well, thus $x \in IJ$. The First Isomorphism Theorem then implies that the diagram



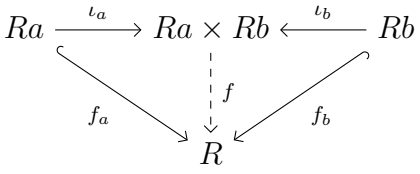
commutes where φ is an isomorphism. □

Example 6.2. *The idempotents of* $\mathbb{Z}/296\mathbb{Z}$ *are* $\overline{112}$ *and* $\overline{185}$.

Proof. We first make the observation that $296 = 8 \cdot 37$, and since $\gcd(8, 37) = 1$, then we have a Diophantine equation $1 = 8x + 37y$ for some integers x and y. It then follows by the Chinese Remainder Theorem that $\mathbb{Z}/296\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z}$ since $\operatorname{lcm}(8, 37) = 296$, hence $8\mathbb{Z} \cap 37\mathbb{Z} = 296\mathbb{Z}$. To find the idempotents of $\mathbb{Z}/296\mathbb{Z}$, we make use of the Euclidean Algorithm to show that $x = 14$ and $y = -3$ is a solution to the Diophantine equation. We then have that $8x = 112$ and $37(-3) = -111 \equiv 185 \pmod{296}$. An easy calculation (with a calculator) confirms that $(112)^2 \equiv 112 \pmod{296}$ and $(185)^2 \equiv 185 \pmod{296}$. □

Theorem 6.3 (Noncommutative Chinese Remainder Theorem)**.** *Let* R *be a ring and let* A *and* B *be coprime ideals in* R *such that* $A \cap B = 0$. *Then,* $R \cong R/A \times R/B$.

Proof. Since $R = A + B$, then there is $a \in A$ and $b \in B$ such that $a + b = 1$. Define $Ra = \{ra : r \in R\}$ and $Rb = \{rb : r \in R\}$ and define $f_a : Ra \hookrightarrow R$ and $f_b : Rb \hookrightarrow R$ by inclusion. These maps induce a unique map $\tilde{f} : Ra \times Rb \to R$ such that the diagram



commutes. Let $r \in R$, hence $ra + rb = r$, so $\tilde{f}(ra, rb) = f_a(ra) + f_b(rb) = ra + rb = r$, so $\tilde{f}$ is surjective. Now, let $(x, y) \in \operatorname{Ker}(\tilde{f})$, hence $\tilde{f}(x, y) = 0$. This means that $\tilde{f}(x, y) = f_a(x) + f_b(y) = x + y = 0$, hence $x = -y \in A \cap B$, hence $x = 0$ and $y = 0$. It then follows that $\tilde{f}$ is an isomorphism.

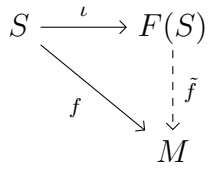
Now, since $A \cap B = 0$, then it's clear that $ab = ba = 0$. It then follows that $a = a(a + b) = a^2 + ab = a^2$ and $b = b(a + b) = ba + b^2 = b^2$, hence a and b are idempotent. Furthermore, since B is an ideal, then $rb \in B$ and $a(rb) \in B$ as well, hence $arb = 0$, and $bra = 0$ by symmetry. It then follows that $0 = arb - bra = (1-b)rb - bra = rb - brb - bra = rb - br(b + a) = rb - br$, hence $rb = br$, and $ra = ar$ by symmetry.

Define $\varphi : R \to Ra$ by $r \mapsto ra$. This is a ring homomorphism since $\varphi(r + s) = (r + s)a = ra + sa = \varphi(r) + \varphi(s)$ and $\varphi(rs) = (rs)a = (rs)a^2 = r(sa)a = r(as)a = (ra)(sa) = \varphi(r)\varphi(s)$. It then follows that $\varphi(b) = ba = 0$ for all $b \in B$, hence $B \subset \operatorname{Ker}(\varphi)$. Likewise, $\varphi(r) = 0$ implies that $0 = ra = r(1 - b) = r - rb$, so $r = rb \in B$. It then follows that $\operatorname{Ker}(\varphi) = B$, and so the First Isomorphism Theorem says that $R/B \cong Ra$. Defining a similar map $r \mapsto rb$, we conclude that $R \cong R/A \times R/B$. □

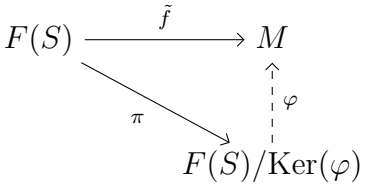
7. Finitely-Generated Modules over a PID

Lemma 7.1. *Let R be a ring, then any R-module is a quotient of a free R-module.*

Proof. Let $S = \{m_\alpha\}_\alpha$ be a generating set of M as an R-module. Definition 3.1 induces a map $\tilde{f}$ such that the diagram



commutes, where $f(m_\alpha) = m_\alpha$ for all α. Since S generates M, then $\tilde{f}$ is surjective, and the First Isomorphism Theorem induces an isomorphism φ such that the diagram



commutes. Therefore M is isomorphic to the quotient of a free module. □

Definition 7.2 (Representable Functor)**.** *Let P be an R-module. Let $\mathcal{C}$ be the category of R-modules and let $\mathcal{D}$ be the category of $\mathbb{Z}$-modules. Define $Hom_R(P, \cdot) : \mathcal{C} \to \mathcal{D}$ by $M \mapsto Hom_R(P, M)$ on objects and $(f : M \to N) \mapsto f_*$ on arrows, where $f_* : Hom_R(P, M) \to Hom_R(P, N)$ is given by $u \mapsto f \circ u$.*

With this definition, it is easy to see that $\mathrm{Hom}_R(P, \cdot)$ is a functor, since $(g \circ f)_*(u) = g \circ f \circ u = g \circ f_*(u) = g_*(f_*(u))$, so $(g \circ f)_* = g_* \circ f_*$.

Theorem 7.3 (Left Exactness of $\mathrm{Hom}_R(P, \cdot)$)**.** *If $0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$ is an exact sequence, then $0 \to Hom_R(P, M') \xrightarrow{f_*} Hom_R(P, M) \xrightarrow{g_*} Hom_R(P, M'')$ is an exact sequence.*

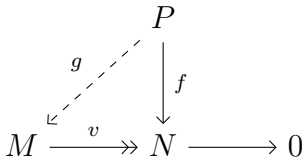
Proof. It suffices to show that f_* is injective and that $\mathrm{Ker}(g_*) = \mathrm{Im}(f_*)$, we'll first show that f_* is injective. Let $u \in \mathrm{Ker}(f_*)$, then $0 = f_*(u) = f \circ u$, thus $\mathrm{Im}(u) \subset \mathrm{Ker}(f) = 0$ since f is injective, so $\mathrm{Im}(u) = 0$ as well. It then follows that $u = 0$, so f_* is injective. Now, observe that $g_* \circ f_* = (g \circ f)_* = 0_* = 0$, so $\mathrm{Im}(f_*) \subset \mathrm{Ker}(g_*)$. Let $v \in \mathrm{Ker}(g_*)$, so $0 = g_*(v) = g \circ v$, so $\mathrm{Im}(v) \subset \mathrm{Ker}(g) = \mathrm{Im}(f)$. This means that for all $m \in M$, there is $p \in P$ and a unique $m' \in M$ (since f is injective) such that $f(m') = m = v(p)$. Define $w : P \to M'$ by $p \mapsto m'$ where $v(p) = m'$, which is easily shown to be a homomorphism. Then, $f_*(w)(p) = (f \circ w)(p) = f(w(p)) = f(m') = v(p)$, hence $f_*(w) = v$, and we're done. □

Notice that we could only conclude that $\mathrm{Hom}_R(P, \cdot)$ is left exact and not exact. We need additional hypotheses on P to conclude that $\mathrm{Hom}_R(P, \cdot)$ is exact, which will soon

be provided. First, however, we will demonstrate a counterexample to the exactness of $\mathrm{Hom}_R(P,\cdot)$ with our current hypotheses.

Consider the short exact sequence $0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$ with $P = \mathbb{Z}/2\mathbb{Z}$. It then follows that $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = 0$ and $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \{\mathrm{id}, 0\}$. This means that $(.2)_*$ is injective, but π_* is not surjective, hence the resulting sequence is not exact.

Definition 7.4 (Projective Modules)**.** *An R-module P is projective if for every R-module epimorphism $v : M \to N$ and every R-module map $f : P \to N$, there is an R-module map $g : P \to M$ (not necessarily unique) such that the diagram*



commutes.

Theorem 7.5. *The representable functor $Hom_R(P,\cdot)$ is exact if and only if P is projective.*

Proof. Suppose P is projective, then we need only show that g_* from the statement of Theorem 7.3 is surjective. Let $v : P \to M''$ be any R-module map, then since g is surjective (an epimorphism), then there is $h : P \to M$ such that $v = g \circ h = g_*(h)$, hence g_* is surjective.

Now, suppose that $\mathrm{Hom}_R(P,\cdot)$ is exact and let $v \in \mathrm{Hom}_R(M, M'')$ be an epimorphism, then we have an exact sequence $M \xrightarrow{v} M'' \to 0$. Since $\mathrm{Hom}_R(P,\cdot)$ is exact, then this induces an exact sequence $\mathrm{Hom}_R(P, M) \xrightarrow{v_*} \mathrm{Hom}_R(P, M'') \to 0$. Let $h \in \mathrm{Hom}_R(P, M'')$ and since v_* is surjective, there is $r \in \mathrm{Hom}(P, M)$ such that $v_*(r) = h$, therefore P is projective. □

Lemma 7.6. *All free modules are projective.*

Proof. By Theorem 7.5, it suffices to show for any surjection $v : M \to N$ that

$$v_* : \mathrm{Hom}_R\left(\coprod_\alpha R, M\right) \to \mathrm{Hom}_R\left(\coprod_\alpha R, N\right)$$

is likewise a surjection. For any R-module Q, we have

$$\mathrm{Hom}_R\left(\coprod_\alpha R, Q\right) \cong \prod_\alpha \mathrm{Hom}_R(R, Q) \cong \prod_\alpha Q$$

by Theorems 1.11 (only if R is commutative) and 1.20. It is then evident that for any $(n_\alpha)_\alpha \in \prod_\alpha N$, there is $(m_\alpha)_\alpha \in \prod_\alpha M$ such that $v(m_\alpha) = n_\alpha$ for all α. It therefore follows by these observations that v_* is surjective. □

Proposition 7.7. *An R-module is projective if and only if it is the direct summand of a free R-module.*

Proof. Let P be a projective R-module and let $v : M \to P$ be any R-module epimorphism, hence the sequence

$$0 \to \mathrm{Ker}(v) \to M \xrightarrow{v} P \to 0$$

is exact. Furthermore, the identity map on P yields a map $s : P \to M$ such that $\mathrm{id} = v \circ s$, hence s is a section of v, and it follows that $M \cong P \oplus \mathrm{Ker}(v)$ by Theorem 2.8.

In the other direction, let $Q \oplus P$ be a free R-module. Define $i : P \hookrightarrow Q \oplus P$ and $\pi : Q \oplus P \to P$ as the canonical inclusion and projection maps, respectively, hence $\pi \circ i = \mathrm{id}$. Let $v : M \to N$ be an epimorphism and let $f : P \to N$ be any R-module map. Since $Q \oplus P$ is a free module, hence projective by Lemma 7.6, then the map $f \circ \pi : Q \oplus P \to N$ induces an R-module map $g : Q \oplus P \to M$ such that the diagram

$$\begin{array}{ccccc} Q \oplus P & & \xrightarrow{\pi} & & P \\ & {\scriptstyle g}\swarrow & & & \downarrow{\scriptstyle f} \\ M & & \xrightarrow{v} & N & \longrightarrow 0 \end{array}$$

commutes. It then follows that $v \circ g \circ i = f \circ \pi \circ i = f \circ \mathrm{id} = f$, therefore P is projective. □

Corollary 7.8. *If $0 \to M' \xrightarrow{u} M \xrightarrow{v} P \to 0$ is exact with P projective, then $M \cong M' \oplus P$.*

Proof. Since P is projective, there is a free R-module F such that $F = P \oplus M$ by Proposition 7.7. Let $\pi : P \oplus M \to P$ be the canonical projection and note that v is surjective. This means there is an R-module map $h : F \to M$ such that $\pi = v \circ h$ by definition of P as a projective R-module. Define $s : P \to M$ by $p \mapsto h(p, 0)$, which is clearly an R-module map since h is an R-module map. It then follows that $v(s(p)) = v(h(p, 0)) = \pi(p, 0) = p$, thus s is a section of v. Our conclusion then follows by Theorem 2.8. □

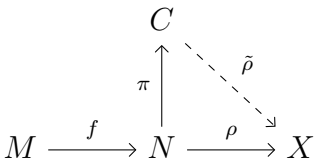
Definition 7.9 (Kernel)**.** *Let $f : M \to N$ be a map of R-modules. A kernel of f is an R-module K equipped with an R-module map $\iota : K \to M$ such that $f \circ \iota = 0$ which is universal: i.e. given any R-module X and any R-module map $\lambda : X \to M$ such that $f \circ \lambda = 0$ there exists a unique map $\tilde{\lambda} : X \to K$ such that the diagram*

$$\begin{array}{ccccc} & & X & & \\ & {\scriptstyle \tilde{\lambda}}\swarrow & \downarrow{\scriptstyle \lambda} & & \\ K & \xrightarrow{\iota} & M & \xrightarrow{f} & N \end{array}$$

commutes.

To construct the kernel of an R-module map $f : M \to N$, we let $K = \{x \in M : f(x) = 0\}$ and let $\iota : K \hookrightarrow M$ be the inclusion. Given any $\lambda : X \to M$ such that $f \circ \lambda = 0$, we define $\tilde{\lambda}(x) = \lambda(x)$. Let ψ be another map such that $\lambda = \iota \circ \psi$, then $\iota(\psi(x)) = \lambda(x) = \iota(\tilde{\lambda}(x))$. Since ι is the inclusion, it is injective, so $\psi(x) = \tilde{\lambda}(x)$.

Definition 7.10 (Cokernel)**.** *Let $f : M \to N$ be an R-module map. A cokernel of f is an R-module C equipped with a map $\pi : N \to C$ such that $\pi \circ f = 0$ which is universal: i.e. given any R-module X and any R-module map $\rho : N \to X$ such that $\rho \circ f = 0$, there is a unique $\tilde{\rho} : C \to X$ such that the diagram*



commutes.

To construct the cokernel, let $C = N/\mathrm{Im}(f)$ and let $\pi : N \to C$ be the canonical projection, so that we have $\pi \circ f = 0$. Let X be any R-module and let $\rho : N \to X$ be given such that $\rho \circ f = 0$. Since $\rho \circ f = 0$, then $\mathrm{Im}(f) \subset \mathrm{Ker}(\rho)$, so the fundamental theorem on homomorphisms induces a unique map $\tilde{\rho} : C \to X$ such that $\rho = \tilde{\rho} \circ \pi$.

Example 7.11. *The sequence $0 \to Ker(f) \to M \xrightarrow{f} N \to Coker(f) \to 0$ is exact.*

Theorem 7.12. *Let $\mathbb{Z}^n$ be a free $\mathbb{Z}$-module for some $n > 0$ and let $M \subset \mathbb{Z}^n$ be a submodule, then $M \cong \mathbb{Z}^m$ for some $m \leq n$.*

Proof. Define $i : \mathbb{Z}^{n-1} \to \mathbb{Z}^n$ by inclusion on the first $n-1$ coordinates and define $p : \mathbb{Z}^n \to \mathbb{Z}$ by projection on the n-th coordinate. It then follows that

$$0 \to \mathbb{Z}^{n-1} \xrightarrow{i} \mathbb{Z}^n \xrightarrow{p} \mathbb{Z} \to 0$$

is exact. If $n = 1$, then M is an ideal of $\mathbb{Z}$, hence $M = k\mathbb{Z}$ for some $k \geq 0$, therefore $M \cong \mathbb{Z}^m$ where $m \leq 1$. This takes care of the base case, so now suppose $n \geq 1$ and that submodules of $\mathbb{Z}^{n-1}$ are isomorphic to $\mathbb{Z}^m$ for some $m \leq n-1$. We then have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(p|_M) & \longrightarrow & M & \xrightarrow{p|_M} & p(M) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}^{n-1} & \xrightarrow{i} & \mathbb{Z}^n & \xrightarrow{p} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

and since $p(M)$ is a submodule of $\mathbb{Z}$, it must be an ideal, hence $p(M) \cong k\mathbb{Z}$ for some $k \geq 0$. Furthermore, since $\mathrm{Ker}(p|_M) \subset \mathbb{Z}^{n-1}$, then $\mathrm{Ker}(p|_M) \cong \mathbb{Z}^m$ for some $m \leq n-1$. If $k = 0$, then $p(M) = 0$, and exactness of the top row implies that $M \cong \mathrm{Ker}(p|_M) \cong \mathbb{Z}^m$ where $m \leq n-1 \leq n$. If $k \neq 0$, then $p(M) = k\mathbb{Z} \cong \mathbb{Z}$, and since $\mathbb{Z}$ is free, it is projective, and the top sequence splits by Corollary 7.8. This means that

$$M \cong \mathrm{Ker}(p|_M) \oplus p(M) \cong \mathbb{Z}^m \oplus \mathbb{Z} \cong \mathbb{Z}^{m+1}$$

where $m \leq n-1$, so $m+1 \leq n$. □

Corollary 7.13. *Any finitely-generated $\mathbb{Z}$-module M arises as a cokernel of some $\mathbb{Z}$-module map $\mathbb{Z}^m \to \mathbb{Z}^n$ with $m \leq n$.*

Proof. Let $\{x_1, \ldots, x_n\}$ be a finite generating set for M as a $\mathbb{Z}$-module. Let $\{e_i\}_{i=1}^n$ be a basis of $\mathbb{Z}^n$ where e_i has 1 in the i-th coordinate and zeros elsewhere. Define $\pi : \mathbb{Z}^n \to M$ by $\pi(e_i) = x_i$ for all $i \in \{1, \ldots, n\}$, which is clearly a surjection since it maps to all of the generators of M. This means that $\mathrm{Ker}(\pi)$ is a submodule of $\mathbb{Z}^n$, and it follows by Theorem 7.12 that $\mathrm{Ker}(\pi) \cong \mathbb{Z}^m$ with $m \leq n$. Let $\varphi : \mathbb{Z}^m \cong \mathrm{Ker}(\pi) \hookrightarrow \mathbb{Z}^n$ be the inclusion map, then $\mathrm{Coker}(\varphi) = \mathbb{Z}^n/\mathrm{Im}(\varphi) \cong \mathbb{Z}^n/\mathrm{Ker}(\pi) \cong M$, where the last isomorphism follows from the First Isomorphism Theorem on π. We therefore have that $M \cong \mathrm{Coker}(\mathbb{Z}^m \xrightarrow{\varphi} \mathbb{Z}^n)$. □

Theorem 7.14 (Smith Normal Form)**.** *Let $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ be any $\mathbb{Z}$-module map. Then, there exists a basis $\mathcal{B}$ of $\mathbb{Z}^m$ and $\mathcal{B}'$ of $\mathbb{Z}^n$ such that $[\varphi]_{\mathcal{B}'}^{\mathcal{B}}$ is diagonal with entries $d_1|d_2|\cdots|d_m$.*

Note that the representing matrix of φ will not necessarily be a square matrix. Instead, when we say that it will be diagonal, it means that the only non-zero entries in the matrix occur in positions where the row and column index agree.

Proof. Let $\mathcal{E}$ be the standard basis of $\mathbb{Z}^m$ and $\mathcal{E}'$ be the standard basis of $\mathbb{Z}^n$. Let $A = [\varphi]_{\mathcal{E}'}^{\mathcal{E}}$. Note that for any basis $\mathcal{B}$ of $\mathbb{Z}^m$ and any basis $\mathcal{B}'$ of $\mathbb{Z}^n$, we have that

$$[\varphi]_{\mathcal{B}'}^{\mathcal{B}} = [\mathrm{id} \circ \varphi \circ \mathrm{id}]_{\mathcal{B}'}^{\mathcal{B}} = [\mathrm{id}]_{\mathcal{B}'}^{\mathcal{E}'} \cdot [\varphi]_{\mathcal{E}'}^{\mathcal{E}} \cdot [\mathrm{id}]_{\mathcal{E}}^{\mathcal{B}}.$$

Our goal will be to construct the change-of-base matrices which flank A in the above equality. To show that such matrices can be constructed, we will show that elementary row and column operations can reduce A to the desired form. In this way, one would need only keep track of the elementary row and column operations to recover the change-of-base matrices. What are the elementary row and column operations though? They must be operations which can be undone through some inverse operation. Consistent with standard linear algebra, there are only three operations: row/column swap, adding a multiple of a row/column to another row/column, and scaling a row/column by a unit (in this context, scaling by ± 1).

Step 1: If $A = 0$, we're done, so we'll assume that $A \neq 0$, hence there is at least one non-zero entry in A. We can then perform a row and column swap to move this element to the upper-left corner of A.

Step 2: If the left-most entry of the first row is the only non-zero element, go to Step 3. Otherwise, swap columns to place one such entry to the immediate right of the upper-left corner. Denote the value of the number in upper-left corner with x and the value to its right by a. We can then write $a = xq + r$ for some q and some $0 \leq r < x$, and perform a column operation by subtracting q times the first column from the second column. This places a value of r to the immediate right of x; swap the first and second row and continue this process until we get a zero at the top of the second column. We continue this process for all non-zero values in the first row until the first column is the only column with a non-zero element in the first row.

Step 3: Repeat the process described in Step 2 for clearing the first row, but instead with the first column. Explicitly, all column operations described in Step 2 are replaced by row operations.

Step 4: At this point (and this needs to be spelled out more explicitly), we arrange so that the entry in the upper-left corner of the matrix divides all other entries in the matrix.

Step 5: Induct this process on the submatrix consisting of all but the first row and first column. □

Definition 7.15 (Torsion)**.** *Let R be any ring, and let M be an R-module. We say that $x \in M$ is torsion if there is $r \in R - \{0\}$ such that $r.x = 0$. Let $Tor(M) = \{x \in M : x \text{ is torsion}\}$.*

Lemma 7.16 (Torsion Submodule)**.** *Let R be a domain and let M be an R-module, then $Tor(M)$ is a submodule of M.*

Proof. Since M is an abelian group, there is $0 \in M$ which is clearly torsion, so $\mathrm{Tor}(M)$ is nonempty. Let $x, y \in \mathrm{Tor}(M)$, let $r \in R$, and let $a, b \in R$ be elements such that $a.x = b.y = 0$. Then, $(ab).(x + r.y) = (ab).x + (ab).(r.y) = (ba).x + a.(br).y = b.(a.x) + a.(rb).y = b.0 + (ar).(b.y) = (ar).0 = 0$. This means that $x + r.y \in \mathrm{Tor}(M)$, and so $\mathrm{Tor}(M)$ is an R-submodule of M by Lemma 1.5. □

Corollary 7.17. *Any finitely-generated $\mathbb{Z}$-module M has a decomposition $M \cong T \oplus F$ where T is finitely-generated torsion and F is free of finite rank.*

Proof. Since M is a finitely-generated $\mathbb{Z}$-module, then by Corollary 7.13, we know that $M \cong \mathrm{Coker}(\varphi) = \mathbb{Z}^n/\mathrm{Im}(\varphi)$ where $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ with $m \leq n$. We know that $\mathrm{Im}(\varphi)$ is a submodule of $\mathbb{Z}^n$, hence $\mathrm{Im}(\varphi) \cong \mathbb{Z}^k$ with $k \leq m$ by Theorem 7.12. It then follows by Lemma 4.4 that

$$M \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_k\mathbb{Z}} \oplus \mathbb{Z}^r$$

where $r = n - k$ and d_i's are nonzero. Let $T = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}$ and $F = \mathbb{Z}^r$. □

Lemma 7.18. *Let T be a torsion $\mathbb{Z}$-module and let $S = \mathbb{Z} - \{0\}$, then $S^{-1}T = 0$.*

Proof. It suffices to show that $t/s = 0$ for all $t \in T$ and all $s \in S$. To do so, we need to produce an $r \in \mathbb{Z} - \{0\} = S$ such that $r.(1.t) = r.(0.s)$, but the fact that T is a torsion $\mathbb{Z}$-module produces such an element. □

As a consequence of Lemma 7.18, the torsion part of a finitely-generated $\mathbb{Z}$-module vanishes whenever we consider its module of fractions. This means that if $M \cong T \oplus \mathbb{Z}^r$ for some $r \geq 0$ and T torsion, then $S^{-1}M = \mathbb{Q}^r$, hence $S^{-1}M$ becomes an r-dimensional $\mathbb{Q}$-vector space.

Definition 7.19 (Noetherian Module)**.** *Let R be a ring. A Noetherian module is an R-module M which satisfies the ascending chain condition on submodules: any sequence $M_1 \subset M_2 \subset \cdots$ of R-submodules of M stabilizes, i.e. there is an integer n such that $M_n = M_{n+1} = \cdots$.*

Theorem 7.20. *An R-module is Noetherian if and only if all of its submodules are finitely-generated.*

Proof. Let M be a Noetherian module and suppose that M is not finitely-generated. Let $a_1 \in M$ and let $M_1 = (a_1)$. Let $a_2 \in M - M_1$ and let $M_2 = (a_1, a_2)$. Continue in this way inductively, hence $M_1 \subsetneq M_2 \subsetneq \cdots$. Since M is Noetherian, there is n such that $M_n = M_{n+1}$; however, this contradicts our construction, therefore M is finitely-generated.

In the other direction, suppose all submodules of M are finitely-generated, and let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules. It then follows that $M' = \bigcup_{i=1}^{\infty} M_i$ is a submodule of M, hence finitely-generated. Let M' be generated by $\{a_1, \ldots, a_m\}$ and let k_i be any index of any submodule such that $a_i \in M_{k_i}$. Let $n = \max\{k_1, \ldots, k_m\}$, then it follows that $M_n = M'$, and subsequently that $M' = M_n = M_{n+1} = \cdots$, therefore M is Noetherian. □

8. Decompositions

Definition 8.1 (Cyclic Module)**.** *An R-module M is called cyclic if it is generated by one element, i.e. $M = R.x = \langle x \rangle$ for some $x \in M$.*

Definition 8.2 (Annihilator)**.** *Let M be an R-module and let $x \in M$. The annihilator of x is given by $ann(x) = \{r \in R : r.x = 0\}$. The annihilator of M is given by $ann(M) = \{r \in R : r.x = 0$ for all $x \in M\} = \bigcap_{x \in M} ann(x)$.*

Definition 8.3 (Invariant Factor Decomposition)**.** *Let T be a finitely-generated torsion abelian group (i.e. $\mathbb{Z}$-module), an invariant factor decomposition is a sequence of integers $1 \neq d_1 | d_2 | \cdots | d_s \neq 0$ such that*

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

Definition 8.4 (Elementary Divisor Decomposition)**.** *Let T be a finitely-generated torsion $\mathbb{Z}$-module, an elementary divisor decomposition is given by*

$$T \cong \bigoplus_p \bigoplus_k (\mathbb{Z}/p^k\mathbb{Z})^{r_{p,k}}$$

for some integers $r_{p,k}$.

Our goal in this section will be to show that not only does an elementary divisor decomposition determine an invariant factor decomposition, but the converse is also true. To this end, we will not prove these results in great generality, but give an example to highlight the methodology behind such a proof. The statement in Definition 8.4 may seem a bit confusing, but it is much easier to understand through an example. To demystify its statement, we consider the following elementary divisor decomposition:

Example 8.5 (Elementary Divisor Decomposition)**.**

$$\left(\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{5\mathbb{Z}} \oplus \frac{\mathbb{Z}}{125\mathbb{Z}}\right).$$

In this case, we would have $r_{2,1} = 1$; $r_{2,2} = 1$; $r_{3,1} = 1$; $r_{3,2} = 2$; $r_{5,1} = 1$; $r_{5,3} = 1$; and $r_{p,k} = 0$ for all other p and k.

Using this example, along with commutativity of direct sums, we can rearrange the summands however we please. We will choose the highest order elementary divisor from each prime grouping and utilize the Chinese Remainder Theorem to collapse them into a single module representative. We demonstrate this via Example 8.5:

$$\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{5\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{125\mathbb{Z}}\right) \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{90\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4500\mathbb{Z}}.$$

It is easy to see that this satisfies the definition of an invariant factor decomposition, since $3|90|4500$. In fact, this will be true for any combination by virtue of how we grouped the elementary divisors. As a consequence, elementary divisor decompositions determine invariant factor decompositions.

Our next goal will be to show the converse; in order to do this, we will need to make use of the following lemma.

Lemma 8.6. *Let $m, n \in \mathbb{Z}$, then $\frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{(mn)\mathbb{Z}}$ if and only if $\gcd(m, n) = 1$.*

Proof. First, we note that if $\gcd(m, n) = 1$, we can apply the Chinese Remainder Theorem (Theorem 6.1), since $m\mathbb{Z}$ and $n\mathbb{Z}$ are coprime ideals. Now, suppose $\frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{(mn)\mathbb{Z}}$. Recall that $\operatorname{lcm}(m, n)\gcd(m, n) = mn$, hence $\gcd(m, n) = 1$ if and only if $\operatorname{lcm}(m, n) = mn$. It therefore suffices to show that $mn(a, b) = 0$ for arbitrary $(a, b) \in \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}$; this, however, is evident. □

This lemma allows us to say that $\mathbb{Z}/p^k\mathbb{Z}$ is indecomposable for p prime and $k \geq 1$. To be precise, this says that $\mathbb{Z}/p^k\mathbb{Z}$ cannot be written as $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ for any such $m, n \geq 2$. The importance of this is that we can take invariant factor decompositions, and by repeatedly using the Chinese Remainder Theorem break cyclic modules apart into sums of the form $\mathbb{Z}/p^k\mathbb{Z}$. Hence, invariant factor decompositions determine elementary divisor decompositions.

A natural question at this point would be to ask whether or not these decompositions are unique. As it will turn out, they are; however, we will need to develop some additional theory along the way to prove it. In fact, we will only need to prove uniqueness for one such flavor of decompositions, since uniqueness of the other will follow immediately.

Definition 8.7 (p-Primary Module)**.** *We say that a $\mathbb{Z}$-module M is p-primary for p prime, if there are integers $r_1, \ldots, r_k$ such that*

$$M \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{r_1} \oplus \cdots \oplus \left(\frac{\mathbb{Z}}{p^k\mathbb{Z}}\right)^{r_k}.$$

This definition in mind, we state the following useful theorem without proof.

Theorem 8.8 (Primary Decomposition Theorem)**.** *Let R be a principal ideal domain and let M be a torsion R-module with a nonzero annihilator a. Suppose that $a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ and let $N_i = \{x \in M : p_i^{\alpha_i}.x = 0\}$ for all $i = 1, \ldots, n$. Then N_i is a submodule of M with annihilator $p_i^{\alpha_i}$ and is the submodule of M of all elements annihilated by some power of p_i. We have*

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_n.$$

If M is finitely generated then each N_i is the direct sum of finitely many cyclic modules whose annihilators are divisors of $p_i^{\alpha_i}$.

In order to show that elementary divisor decompositions are unique, we will simplify matters by showing that for any p-primary module, the exponents provided by the definition are unique.

Before we continue, however, note that Definition 8.5 can now be reformulated as follows:

Definition 8.9 (Elementary Divisor Decomposition)**.** *Let T be a finitely-generated torsion $\mathbb{Z}$-module, an elementary divisor decomposition of T is given by*

$$T \cong T_{p_1} \oplus \cdots \oplus T_{p_n}$$

where each T_{p_k} is p_k-primary.

As stated, we will need to develop some further theory in order to prove uniqueness of elementary divisor decompositions...

9. Filtration

Definition 9.1 (Filtered Module)**.** *A filtered module is a module with a nested sequence of submodules:*

$$M = F_0M \supset F_1M \supset F_2M \supset \cdots \supset F_{n-1}M \supset F_nM = 0.$$

Note that F_*M merely denotes the position of the submodule in the filtration sequence of M.

Definition 9.2 (Associated Graded Module)**.** *Let M be a filtered module and define $G_jM = F_{j-1}M/F_jM$ for all $j \in \{1, \ldots, n\}$. An associated graded module is a module*

$$G_*(M) = \coprod_{j \in \mathbb{Z}} G_jM.$$

These definitions don't yield much intuition on the outset, so we will consider a few examples to illuminate the topic.

Definition 9.3 (Filtration-Preserving Module Map)**.** *Let M and N be filtered modules, a filtration-preserving map is a module map $f : M \to N$ such that $f(F_jM) \subset F_jN$ for all j.*

Lemma 9.4. *Let M and N be filtered modules and let $f : M \to N$ be a filtration-preserving module map, then there is a module map $\overline{f_j} : G_jM \to G_jN$.*

Proof. We wish to induce a map $\overline{f_j}$ such that the diagram

$$\begin{array}{ccc} F_{j-1}M & \xrightarrow{f} & F_{j-1}N \\ {\scriptstyle \pi_j^M}\downarrow & & \downarrow{\scriptstyle \pi_j^N} \\ G_jM & \xrightarrow{\overline{f_j}} & G_jN \end{array}$$

commutes. We will show that $F_jM \subset \mathrm{Ker}(\pi_j^N \circ f)$, thereby inducing the desired map by the fundamental theorem on homomorphisms. Our assumption on f tells us that $f(F_jM) \subset F_jN$, hence $(\pi_j^N \circ f)(F_jM) = 0$, since $G_jN = F_{j-1}N/F_jN$. We then induce a unique map $\overline{f_j} : G_jM \to G_jN$ such that $\pi_j^N \circ f = \overline{f_j} \circ \pi_j^M$. □

Theorem 9.5. *Let $\mathcal{C}$ be the category of filtered modules and let $\mathcal{D}$ be the category of associated graded modules. Define $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ on objects by $F_*M \mapsto G_*M$, and on arrows by $f \mapsto \overline{f} := \coprod_j \overline{f_j}$ where each $\overline{f_j}$ is given by Lemma 9.4. Then, $\mathcal{F}$ defines a functor.*

Proof. Let $f : M \to N$ and $g : N \to P$ be filtration-preserving module maps. We must show that $\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$. The maps f and g individually induce a commuting diagram

$$\begin{array}{ccccc} F_{j-1}M & \xrightarrow{f} & F_{j-1}N & \xrightarrow{g} & F_{j-1}P \\ \downarrow{\scriptstyle \pi_j^M} & & \downarrow{\scriptstyle \pi_j^N} & & \downarrow{\scriptstyle \pi_j^P} \\ G_jM & \xrightarrow{\overline{f_j}} & G_jN & \xrightarrow{\overline{g_j}} & G_jP \end{array}$$

for each $j \geq 1$. We then consider the analogous diagram induced by the map $g \circ f$ and observe that

$$\overline{(g \circ f)_j} \circ \pi_j^M = \pi_j^P \circ (g \circ f) = \overline{g_j} \circ \pi_j^N \circ f = \overline{g_j} \circ \overline{f_j} \circ \pi_j^M,$$

hence $\overline{(g \circ f)_j} = \overline{g_j} \circ \overline{f_j}$ by uniqueness, and functoriality follows since j was arbitrary. □

Notice that the functor in Theorem 9.5 was defined in terms of a coproduct. This means that all but finitely many of the $\overline{f_j}$'s that define $\overline{f}$ must be zero maps.

Lemma 9.6 (Five Lemma)**.** *If the diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \end{array}$$

commutes such that each row is exact, and f' and f'' are isomorphisms, then f is an isomorphism as well.

Proof. This is a standard diagram chasing proof.

To prove surjectivity of f, we let $n \in N$ and choose $m'' \in M''$ such that $f''(m'') = v'(n)$. We then let $m \in M$ such that $v(m) = m''$, and so it follows that $v'(n) = f''(m'') = f''(v(m)) = v'(f(m))$, hence $v'(n - f(m)) = 0$. Since $n - f(m) \in \mathrm{Ker}(v')$, it is in the image of u', and so there is $n' \in N'$ such that $u'(n') = n - f(m)$. Now, let $m' \in M'$ be such that $f'(m') = n'$, and we have $n - f(m) = u'(n') = u'(f'(m')) = f(u(m'))$, hence $f(u(m') + m) = n$.

Let $m \in \mathrm{Ker}(f)$ and so $f(m) = 0$, hence $0 = v'(f(m)) = f''(v(m))$ and so $v(m) = 0$ since f'' is an isomorphism. Then, there is $m' \in M'$ such that $u(m') = m$ and so $0 = f(m) = f(u(m')) = u'(f'(m))$, so $m = 0$ since $u' \circ f'$ is injective. □

We will use this lemma for the following theorem.

Theorem 9.7. *Let M and N be filtered modules and let $f : M \to N$ be a filtration-preserving module map. Then, f is an isomorphism if and only if $\overline{f} : G_*M \to G_*N$*

Proof. Add this later... □

Theorem 9.8 (p-Primary Dimension)**.** *Let M be a p-primary module and let $M \supset pM \supset p^2M \supset \cdots \supset p^nM = 0$ be a filtration. Let $G_*M = \coprod_j G_jM$ be its associated graded module, then each G_jM is a $\mathbb{Z}_p$-vector space with dimension $r_j + \cdots + r_n$. We define this dimension by $d_j(M) := \dim_{\mathbb{Z}_p}(G_jM)$.*

Proof. First we note that by $p^jM := (p^j\mathbb{Z})M$, and that the first j terms of M vanish via p^jM, hence

$$p^jM = \left(\frac{p^j\mathbb{Z}}{p^{j+1}\mathbb{Z}}\right)^{r_{j+1}} \oplus \cdots \oplus \left(\frac{p^j\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r_n}.$$

It then follows that

$$\begin{aligned} G_jM = \frac{F_{j-1}M}{F_jM} &= \frac{\left(\frac{p^{j-1}\mathbb{Z}}{p^j\mathbb{Z}}\right)^{r_j} \oplus \left(\frac{p^{j-1}\mathbb{Z}}{p^{j+1}\mathbb{Z}}\right)^{r_{j+1}} \oplus \cdots \oplus \left(\frac{p^{j-1}\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r_n}}{\left(\frac{p^j\mathbb{Z}}{p^{j+1}\mathbb{Z}}\right)^{r_{j+1}} \oplus \cdots \oplus \left(\frac{p^j\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r_n}} \\ &\cong \left(\frac{p^{j-1}\mathbb{Z}}{p^j\mathbb{Z}}\right)^{r_j} \oplus \left(\frac{p^{j-1}\mathbb{Z}/p^{j+1}\mathbb{Z}}{p^j\mathbb{Z}/p^{j+1}\mathbb{Z}}\right)^{r_{j+1}} \oplus \cdots \oplus \left(\frac{p^j\mathbb{Z}/p^n\mathbb{Z}}{p^{j-1}\mathbb{Z}/p^n\mathbb{Z}}\right)^{r_n}. \end{aligned}$$

The Third Isomorphism Theorem tells us that $\frac{p^{j-1}\mathbb{Z}/p^k\mathbb{Z}}{p^j\mathbb{Z}/p^k\mathbb{Z}} \cong \frac{p^{j-1}\mathbb{Z}}{p^j\mathbb{Z}} \cong \mathbb{Z}_p$ for all $k \geq j$. It then immediately follows that $G_jM \cong (\mathbb{Z}_p)^{r_j+\cdots+r_n}$. □

Theorem 9.8 is now enough to prove that elementary divisor decompositions are unique, but how? First, let M be a p-primary module and let $d_j := d_j(G_jM)$ be clear from context. We then observe that $d_1 = r_1 + r_2 + \cdots + r_n$, $d_2 = r_2 + r_3 + \cdots + r_n$, and so forth. In fact, what this says is that $r_1 = d_1 - d_2$, that $r_2 = d_2 - d_3$, and so forth, hence $r_j = d_j - d_{j+1}$. Why does this say that each r_j is unique though? Well, note that each d_j is defined without reference to any decomposition of M; in fact, the associated graded module doesn't actually "see" any specific decomposition of M. This tells us that the d_j's are an intrinsic property of the original module, regardless of the choice of decomposition, hence unique. Furthermore, since we can then deduce the r_j's from the d_j's, then it follows that the r_j's are unique as well. We then conclude that elementary divisor decompositions are unique, hence invariant factor decompositions are likewise unique. All of this yields the following structure theorem on finitely-generated $\mathbb{Z}$-modules (i.e. abelian groups)

Theorem 9.9 ($\mathbb{Z}$-Module Structure Theorem)**.** *Let M be a finitely-generated $\mathbb{Z}$-module, then there is a unique invariant factor decomposition given by*

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \oplus \mathbb{Z}^r$$

where $1 \neq d_1|d_2|\cdots|d_s \neq 0$ are positive integers such that $r, s, d_1, \ldots, d_s$ are uniquely determined.

Proof. We just did it. □

10. Rational Canonical Form

Okay, so we've proven–more or less–this Structure Theorem and it seems really, really important, but what exactly does it tell us? What exactly does it allow us to do? To answer this question, we turn toward the world of Linear Algebra!

Let V be a finite-dimensional k-vector space and let $T \in \mathrm{End}_k(V)$, hence T is a linear transformation. It's easy to see that the polynomials of one variable over the field k, denoted $k[X]$, is a free k-module. We then define a set map taking $X \mapsto T$, and induce (by Definition 3.1) a k-module map $k[X] \to \mathrm{End}_k(V)$. Theorem 1.3 then implies that V can be viewed as a $k[X]$-module induced via T.

Definition 10.1 (Vector Spaces as $k[X]$-Modules)**.** *Let V be a finite-dimensional vector space and let $T : V \to V$ be a linear transformation. We say that V is a $k[X]$-module via T where the $k[X]$-module structure is given by the mapping $k[X] \times V \to V$ such that $(f, v) \mapsto f.v := f(T)(v)$.*

Let V be a finite-dimensional k-vector space such that $V = W_1 \oplus W_2 \oplus \cdots \oplus W_s$ as a $k[X]$-module via T. Then each W_j is a $k[X]$-submodule via T; in linear algebra terms, we consider them T-invariant subspaces of V represented by a basis $\mathcal{B}_j$. We could then let $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_s$ be a k-basis of V. Then, the representing matrix of T would be given by

$$[T]^{\mathcal{B}}_{\mathcal{B}} = \begin{bmatrix} [T|_{W_1}]^{\mathcal{B}_1}_{\mathcal{B}_1} & & & 0 \\ & [T|_{W_2}]^{\mathcal{B}_2}_{\mathcal{B}_2} & & \\ & & \ddots & \\ 0 & & & [T|_{W_s}]^{\mathcal{B}_s}_{\mathcal{B}_s} \end{bmatrix}.$$

Big deal, right? Well, as it turns out the Structure Theorem allows us to view V as a $k[X]$-module

$$V \cong \frac{k[X]}{(f_1)} \oplus \cdots \oplus \frac{k[X]}{(f_s)} \oplus k[X]^r,$$

such that $k[X] \supsetneq (f_1) \supset (f_2) \supset \cdots \supset (f_s) \neq 0$ such that $f_1 | f_2 | \cdots | f_s \neq 0$. In fact, when the f_j's are taken to be monic, then they are likewise unique. Now, since we're assuming that V is finite-dimensional, then it is therefore finitely-generated, hence $r = 0$ and so we have $W_j = \frac{k[X]}{(f_j)}$ for all j. This means that V as a $k[X]$-module is the direct sum of cyclic $k[X]$-submodules.

Definition 10.2 (Minimal Polynomial)**.** *Let V be a $k[X]$-module via T as just described. The minimal polynomial of T, denoted μ_T, is the unique monic polynomial which generates $ann(V)$ in $k[X]$.*

As a quick aside, it is pretty easy to see that f_s generates the annihilator of V in $k[X]$ given an invariant factor decomposition. In this way, the invariant factor decomposition of V as a $k[X]-$module affords us a quick and easy way of identifying the minimal polynomial of T: we simply look at the right-most term.

Our goal now will be to construct a representing matrix $[T]$ for some basis given only the polynomials of the invariant factor decomposition of V as a $k[X]$-module. To do this, we will restrict our attention to a single block $[T|_{W_j}]^{\mathcal{B}_j}_{\mathcal{B}_j}$ in the above matrix.

Proposition 10.3. *Let $V \cong k[X]/(f)$ as a $k[X]$-module, then $\beta = \{\overline{1}, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1}\}$ is a $k[X]$-basis of V where $d = \deg(f)$.*

Proof. We must show that the given basis spans V, as well as that it is linearly independent. Let $\overline{h} \in k[X]/(f)$, hence $h \in k[X]$ and $h = f \cdot q + r$ where $\deg(r) < \deg(f)$ by the Division Algorithm. Then, $\overline{h} = \overline{f}\overline{q} + \overline{r} = \overline{r}$ since $\overline{f}$ vanishes in $k[X]/(f)$. Since $r = c_0 + c_1X + \cdots + c_{d-1}X^{d-1}$ for some coefficients in k, then it follows that β spans $k[X]/(f)$.

Now, suppose $c_0.\overline{1} + c_1.\overline{X} + \cdots + c_{d-1}.\overline{X}^{d-1} = \overline{0}$ for some coefficients $c_0, \ldots, c_{d-1} \in k$. Consolidating these into a single quotient, it follows that $\overline{c_0 + c_1X + \cdots + c_{d-1}X^{d-1}} = \overline{0}$. However, this says that f divides $c_0 + c_1X + \cdots + c_{d-1}X^{d-1}$, hence $c_0 = c_1 = \cdots = c_{d-1} = 0$, and so β is linearly independent. □

We now have a basis β for $k[X]/(f)$, and so we quickly remind ourselves exactly how to construct a representing matrix given a transformation and a basis. We are taught in Linear Algebra that to construct such a matrix, we transform each basis vector via T and place the resultant vector in the column corresponding to that basis vector. For example, given a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$, we would have

$$[T]_{\mathcal{B}}^{\mathcal{B}} = [T(v_1) \quad T(v_2) \quad \cdots \quad T(v_n)],$$

which is consistent with what we found in Theorem 1.22. The same rule applies here, except that we need to take pause and remind ourselves exactly what is being transformed. Since we are working in $k[X]/(f)$ and not k^n, we need to be careful about exactly what action is taking the place of transformation via T as in the k^n case. Well, in this instance, it's relatively easy to see that T corresponds to action by X, hence our module structure tells us that $(X, v) \mapsto X.v = T(v)$. We therefore need only consider how X acts on the basis β, and so we observe that

$$\begin{array}{rcl} \overline{1} & \overset{X}{\mapsto} & \overline{X} \\ \overline{X} & \mapsto & \overline{X}^2 \\ \overline{X}^2 & \mapsto & \overline{X}^3 \\ & \vdots & \\ \overline{X}^{d-2} & \mapsto & \overline{X}^{d-1} \\ \overline{X}^{d-1} & \mapsto & \overline{X}^d. \end{array}$$

The first $d-1$ actions are perfectly fine, since we are basically mapping each basis element to the next one in line. However, we now need to consider how to handle the last action $\overline{X}^{d-1} \mapsto \overline{X}^d$, since $\overline{X}^d$ isn't a basis element; in other words, we need to write $\overline{X}^d$ as a linear combination of basis elements.

To do this, we make the observation that f is monic and $\deg(f) = n$, hence $f = X^d + c_{d-1}X^{d-1} + \cdots + c_1X + c_0$ in $k[X]$. Furthermore, we note that $\overline{f} = \overline{0}$ in $k[X]/(f)$, and so $\overline{X}^d = -c_{d-1}.\overline{X}^{d-1} - \cdots - c_1.\overline{X} - c_0.\overline{1}$. We now know exactly how to construct

our representing matrix in $k[X]/(f)$:

$$[T]^{\beta}_{\beta} = \begin{bmatrix} 0 & 0 & 0 & \cdots & \cdots & -c_0 \\ 1 & 0 & 0 & \cdots & \cdots & -c_1 \\ 0 & 1 & 0 & \cdots & \cdots & -c_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -c_{d-1} \end{bmatrix}.$$

Definition 10.4 (Companion Matrix)**.** *Let V be a finite-dimensional k-vector space, and let $T : V \to V$ be a linear transformation. Suppose that $V \cong k[X]/(f)$ for some polynomial $f \in k[X]$ such that $\deg(f) = d$, we then call the matrix above the companion matrix of f. We will denote the companion matrix of f by $\mathcal{C}(f)$.*

Definition 10.5 (Rational Canonical Form)**.** *Let $V \cong k[X]/(f_1) \oplus \cdots \oplus k[X]/(f_s)$ as a $k[X]$-module via T. The rational canonical form of the representing matrix of T is given by the block matrix*

$$R_{[T]} = \begin{bmatrix} \mathcal{C}(f_1) & & & 0 \\ & \mathcal{C}(f_2) & & \\ & & \ddots & \\ 0 & & & \mathcal{C}(f_s) \end{bmatrix}.$$

This is a good point to put things into perspective by considering an example.

Example 10.6. *Let V be a finite-dimensional k-vector space and let $T : V \to V$ be such that $T^2 = T$. Furthermore, assume that $T \neq 0$ and $T \neq I$. What are the possible rational canonical forms of T?*

Solution. First, we observe that $T^2 - T = 0$, and so we might guess that $\mu_T = X^2 - X$ since this polynomial clearly annihilates V. To prove this is the case, suppose there is some other polynomial f which annihilates V, then we must have that $f|X(X-1)$ and so $f = X$ or $f = X - 1$. If $f = X$, then we have $f.v = 0$ for all $v \in V$, but this means that $0 = X.v = T(v)$, hence $T = 0$. If $f = X-1$, then $0 = (X-1).v = (T-I)(v) = T(v)-v$, hence $T(v) = v$, and so $T = I$. Since we assumed that $T \neq I$ and $T \neq 0$, then we conclude that $\mu_T = X^2 - X$ as desired.

We then must ask ourselves what are the possible invariant factor decompositions? In this instance, there are two possibilities

$$V \cong \left(\frac{k[X]}{(X)}\right)^{s_1} \oplus \left(\frac{k[X]}{(X(X-1))}\right)^{s_2}$$

or

$$V \cong \left(\frac{k[X]}{(X-1)}\right)^{s_1} \oplus \left(\frac{k[X]}{(X(X-1))}\right)^{s_2}.$$

Suppose the former, hence we need only compute the companion matrices $\mathcal{C}(X)$ and $\mathcal{C}(X(X-1))$. It's clear that $\mathcal{C}(X) = 0$, the 1×1 zero matrix, since the polynomial

X has no constant coefficient. Furthermore, $X(X-1) = X^2 - X$, hence $c_0 = 0$ and $c_1 = -1$, and so

$$\mathcal{C}(X^2 - X) = \begin{bmatrix} 0 & -c_0 \\ 1 & -c_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

Can we simplify $\mathcal{C}(X(X-1))$? Yes. Let $\{e_1, e_2\}$ be the basis on which this matrix is defined, hence $e_1 \mapsto e_2$ and $e_2 \mapsto e_2$. Define a new basis $\{u_1 = e_2, u_2 = e_1 - e_2\}$, and note that $u_1 \mapsto e_2 = u_1$ and $u_2 \mapsto e_2 - e_2 = 0$. This means that we can perform a change of basis operation in such a way that

$$A = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = B$$

where $\sim$ denotes matrix similarity, i.e. there is $P \in \mathrm{GL}_2(k)$ such that $A = PBP^{-1}$. This tells us that we can construct the following rational canonical form of $[T]$:

$$R_{[T]} = \left[\begin{array}{ccc|ccccc} 0 & & & & & & & \\ & \ddots & & & & & & \\ & & 0 & & & & & \\ \hline & & & 1 & 0 & & & \\ & & & 0 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & 0 \\ & & & & & & 0 & 0 \end{array}\right] \sim \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$$

where I is the $s_2 \times s_2$ identity matrix.

Lastly, suppose the latter, hence we need only compute $\mathcal{C}(X-1)$, however, this is easily seen to be the 1×1 identity matrix. Coupled with our observations about $\mathcal{C}(X(X-1))$ in the previous paragraph, it then follows that

$$R_{[T]} = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$$

where I is the $(s_1 + s_2) \times (s_1 + s_2)$ identity matrix in this instance. □

Up to this point, we've shown that given an invariant factor decomposition, we can construct the rational canonical form $R_{[T]}$. This begs the question: given a linear transformation $T : V \to V$, how do we arrive at the invariant factor decomposition of V as a $k[X]$-module via T?

Let V be an n-dimensional k-vector space, let $T : V \to V$ be a linear transformation, and let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a k-basis. For convenience's sake, define $[T]^{\mathcal{B}}_{\mathcal{B}} =: A = [a_{ij}]_{ij}$, hence $T(v_j) = \sum_{i=1}^{n} a_{ij} v_i$. Let $k[X]^n$ be a free $k[X]$-module of rank n and let $\mathcal{E} = \{\epsilon_1, \ldots, \epsilon_n\}$ be its generating set. Define a map $\pi : k[X]^n \to V$ such that $\epsilon_j \mapsto v_j$ for all $j = 1, \ldots, n$. Our goal will be to determine $\mathrm{Ker}(\pi)$.

Define $\xi_j = X.\epsilon_j - \sum_i a_{ij}\epsilon_i$, and observe that

$$\begin{aligned}\pi(\xi_j) &= \pi(X.\epsilon_j) - \pi\left(\sum_i a_{ij}\epsilon_i\right)\\ &= X.\pi(\epsilon_j) - \sum_i a_{ij}\pi(\epsilon_i)\\ &= X.v_j - \sum_i a_{ij}v_i\\ &= T(v_j) - T(v_j) = 0,\end{aligned}$$

hence $\xi_j \in \mathrm{Ker}(\pi)$ for all $j = 1, \ldots, n$. Rewriting our definition of ξ_j, we have that $X.\epsilon_j = \xi_j + \sum_i a_{ij}\epsilon_i$, and so we want to consider what happens to $X^2.\epsilon_j$. We observe the following:

$$\begin{aligned}X^2.\epsilon_j = X.(X.\epsilon_j) &= X.\left(\xi_j + \sum_i a_{ij}\epsilon_i\right)\\ &= X.\xi_j + \sum_i a_{ij}X.\epsilon_i\\ &= X.\xi_j + \sum_i a_{ij}\left(\xi_i + \sum_r a_{ri}\epsilon_r\right)\\ &= \sum_\alpha h_\alpha(X).\xi_\alpha + \sum_\alpha b_\alpha\epsilon_\alpha\end{aligned}$$

for some $h_\alpha \in k[X]^2$ and some $b_\alpha \in k$. In this case, the α indices ranges over all possible combinations of integer pairs which make sense in context and are merely there as convenient shorthand, since the explicit details are not important. By induction, it then follows that

$$X^r.\epsilon_j = \sum_\alpha h_\alpha(X).\xi_j + \sum_\alpha b_\alpha\epsilon_\alpha$$

for some $h_\alpha \in k[X]^r$ and $b_\alpha \in k$. This means that we can choose any $g \in k[X]$ and write

$$g(X).\epsilon_j = \sum_\alpha h_\alpha(X).\xi_j + \sum_\alpha b_\alpha\epsilon_\alpha.$$

Now, choose an arbitrary element $\eta \in k[X]^n$, hence

$$\eta = \sum_j g_j(X).\epsilon_j = \sum_\alpha h_\alpha(X).\xi_\alpha + \sum_\alpha b_\alpha\epsilon_\alpha,$$

for some $h_\alpha \in k[X]^n$, $b_\alpha \in k$. Assuming that $\eta \in \mathrm{Ker}(\pi)$, it immediately follows that $\sum_\alpha b_\alpha\epsilon_\alpha \in \mathrm{Ker}(\pi)$. However, $\sum_\alpha b_\alpha\epsilon_\alpha$ is just some coefficient in k, and so must be equal to zero. It then follows that η is a sum of ξ_j's, hence $\{\xi_j\}_j$ generates $\mathrm{Ker}(\pi)$ With this in mind, we define a map $\partial : k[X]^n \to k[X]^n$ given by $\epsilon_j \mapsto \xi_j$, hence ∂ maps surjectively to $\mathrm{Ker}(\pi)$. This means that $\pi \circ \partial = 0$ and $\mathrm{Im}(\partial) = \mathrm{Ker}(\pi)$, and so V is the cokernel of ∂. We say that V as a $k[X]$-module via T has a *presentation* given by

$$k[X]^n \xrightarrow{\partial} k[X]^n \xrightarrow{\pi} V \to 0.$$

Now, for all j, we then have

$$\partial(\epsilon_j) = \xi_j = X.\epsilon_j - \sum_i a_{ij}\epsilon_i = \sum_i (X\delta_{ij} - a_{ij})\epsilon_i = \sum_i (XI - A)_{ij}\epsilon_i,$$

hence $[\partial]_{\mathcal{E}}^{\mathcal{E}} = XI - A$.

Having done all of this, what exactly does this tell us? Well, it tells us that we need only perform elementary row and column operations on $XI - A$ over $k[X]$ to obtain a diagonal matrix of the form

$$R_{[T]} = \begin{bmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1 & & \\ & & & & \ddots & \\ 0 & & & & & f_s \end{bmatrix}$$

such that $1 \neq f_1 | f_2 | \cdots | f_s \neq 0$, each f_i monic; this determines the invariant factor decomposition of V as a $k[X]$-module via T. We are allowed to do this for the same reason Smith's Normal Form allowed us to determine an invariant factorization of an arbitrary matrix over the integers. Furthermore, taking a closer look at $XI - A$, we can easily recognize this as the form of a matrix whose determinant yields the characteristic polynomial of A. We then make the following definition:

Definition 10.7 (Characteristic Polynomial)**.** *Let V be a finite-dimensional k-vector space and let $T : V \to V$ be a linear transformation. Define $A := [T]_{\mathcal{B}}^{\mathcal{B}}$ to be the representing matrix of T for some basis $\mathcal{B}$. The characteristic polynomial of A, denoted χ_A, is given by* $\det(XI - A)$.

It turns out that the characteristic polynomial is the product $f_1 f_2 \cdots f_s$ for the given invariant factorization. In fact, the condition that $f_i | f_s$ for all $i = 1, \ldots, s$ tells us that the roots of the characteristic polynomial are also the roots of the minimal polynomial as well.

Example 10.8. *Find the rational canonical form of*

$$A = \begin{bmatrix} 3 & 1 & 0 \\ 1 & 4 & 1 \\ 3 & -2 & 5 \end{bmatrix}$$

and determine the matrix which conjugates it into its rational canonical form.

Solution. Our approach will be to consider the matrix $XI - A$ in $\mathbb{R}[X]$, reduce it into its invariant factor decomposition, and use this to tell us the rational canonical form, R_A. In doing so, we will keep track of the row operations and use these to reconstruct the matrix $P \in GL_3(\mathbb{R})$ such that $A = P^{-1} R_A P$. We need only keep track of the row operations, since row operations act on the left of the matrix in which we operate; column operations act on the right. Of course, we could just as easily keep track of the column operations and use these to construct the inverse of the conjugating matrix.

We begin with $XI - A$:

$$\begin{bmatrix} X-3 & -1 & 0 \\ -1 & X-4 & -1 \\ -3 & 2 & X-5 \end{bmatrix} \begin{matrix} e_1 \\ e_2 \\ e_3 \end{matrix} \xrightarrow{C_1 \leftrightarrow C_2, -C_1}$$

$$\begin{bmatrix} 1 & X-3 & 0 \\ -X+4 & -1 & -1 \\ -2 & -3 & X-5 \end{bmatrix} \begin{matrix} e_1 \\ e_2 \\ e_3 \end{matrix} \xrightarrow{C_2-(X-3)C_1 \to C_2}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ -X+4 & X^2-7X+11 & -1 \\ -2 & 2X-9 & X-5 \end{bmatrix} \begin{matrix} e_1 \\ e_2 \\ e_3 \end{matrix} \xrightarrow{R_2+(X-4)R_1 \to R_2}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & X^2-7X+11 & -1 \\ -2 & 2X-9 & X-5 \end{bmatrix} \begin{matrix} e_1-(X-4)e_2 \\ e_2 \\ e_3 \end{matrix} \xrightarrow{R_3+2R_1 \to R_3}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & X^2-7X+11 & -1 \\ 0 & 2X-9 & X-5 \end{bmatrix} \begin{matrix} e_1-(X-4)e_2-2e_3 \\ e_2 \\ e_3 \end{matrix} \xrightarrow{C_3 \leftrightarrow C_2, -C_2}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & X^2-7X+11 \\ 0 & -X+5 & 2X-9 \end{bmatrix} \begin{matrix} e_1-(X-4)e_2-2e_3 \\ e_2 \\ e_3 \end{matrix} \xrightarrow{R_3+(X-5)R_2 \to R_3}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & X^2-7X+11 \\ 0 & 0 & (X-4)^3 \end{bmatrix} \begin{matrix} e_1-(X-4)e_2-2e_3 \\ e_2-(X-5)e_3 \\ e_3 \end{matrix} \longrightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X-4)^3 \end{bmatrix} \begin{matrix} e_1-(X-4)e_2-2e_3 \\ e_2-(X-5)e_3 \\ e_3 \end{matrix}$$

Since $(X-4)^3 = X^3 - 12X^2 + 48X - 64$, then this tells us that

$$R_A = \begin{bmatrix} 0 & 0 & 64 \\ 1 & 0 & -48 \\ 0 & 1 & 12 \end{bmatrix}.$$

Our original basis was $\{e_1, e_2, e_3\}$ and the form of A tells us that $Xe_1 = 3e_1 + e_2 + 3e_3$, $Xe_2 = e_1 + 4e_2 - 2e_3$, and $Xe_3 = e_2 + 5e_3$. Having kept track of how the rows affect our basis, we can easily see that $e_1 - (X-4)e_2 - 2e_3 = 0$ and $e_2 - (X-5)e_3 = 0$. This means that 0, 0 and e_3 are the generators of V as a cyclic $\mathbb{R}[X]$-module, hence $V \cong \mathbb{R}[X]/(e_3)$ in its invariant factor decomposition as an $\mathbb{R}[X]$-module. We can then recover the conjugating matrix

$$P = [\overline{1}.e_3 \quad \overline{X}.e_3 \quad \overline{X}^2.e_3] = [e_3 \quad T(e_3) \quad T^2(e_3)] = \begin{bmatrix} 1 & 3 & 10 \\ 0 & 1 & 10 \\ 0 & 3 & 22 \end{bmatrix}.$$

It can be easily checked that $R_A = P^{-1}AP$, and so P conjugates A into its rational canonical form. $\square$

Example 10.9. *Find the rational canonical form of*

$$B = \begin{bmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{bmatrix}$$

and find the matrix which conjugates it into its rational canonical form.

Proposition 10.10. *If A and B are similar matrices, i.e. there is $P \in GL_n(k)$ such that $PAP^{-1} = B$, then $\chi_A = \chi_B$.*

Proof. Let P be such that $B = PAP^{-1}$, and so it follows that $XI - B = XI - PAP^{-1}$. This means that $\det(XI - B) = \det(XI - PAP^{-1}) = \det(PXIP^{-1} - PAP^{-1}) = \det(P)\det(XI - A)\det(P^{-1})$. It follows that

$$\begin{aligned} \chi_B = \det(XI - B) &= \det(P^{-1}XIP - P^{-1}BP) = \det(P^{-1}(XI - B)P) \\ &= \det(P^{-1})\det(XI - B)\det(P) = \det(XI - A) = \chi_A. \end{aligned}$$

□

This says that the characteristic polynomial of a matrix is determined by it's similarity class. However, this *does not* say that the characteristic polynomial determines the similarity class of a matrix. In effect, this means that knowing the characteristic polynomial is not enough to determine its similarity class; however, the similarity class is enough to determine it's characteristic polynomial. This observation makes similarity classes incredibly powerful in terms of characteristic polynomials. Given a matrix, we can effectively "replace" it by a similar matrix which may be more computationally tractable, using it to determine the original matrix's characteristic polynomial. This is incredibly useful since the characteristic polynomial holds the key to unlocking the eigenvalues and eigenvectors of the matrix.

Theorem 10.11 (Cayley-Hamilton Theorem)**.** *Let $T : V \to V$ be a linear transformation of a finite-dimensional k-vector space V. If V is cyclic as a $k[X]$-module, then $\mu_T | \chi_T$, i.e. the minimal polynomial divides the characteristic polynomial.*

Proof. This follows immediately from the observation that χ_T is a product of the invariant factors, of which μ_T is one such factor. □

While this theorem is a straightforward consequence, this has a couple profound consequences. First, this means that any matrix $A \in M_n(k)$ satisfies its own characteristic polynomial. Secondly, the minimal polynomial has degree at most n.

Definition 10.12 (Diagonalizable)**.** *Let V be a finite-dimensional k-vector space and let $T : V \to V$; we say that T is diagonalizable if there is some basis $\mathcal{B}$ such that $[T]^{\mathcal{B}}_{\mathcal{B}} = diag(\lambda_1, \lambda_2, \ldots, \lambda_s)$. Note that we make no assumption that the λ_i are distinct.*

Definition 10.13 (λ-Eigenspace)**.** *Let V be a finite-dimensional k-vector space and $T : V \to V$ a linear transformation. The λ-eigenspace of V with respect to T is given by ${}_{(X-\lambda)}V = \{v \in V : (X - \lambda).v = 0\} = \{v \in V : T(v) = \lambda v\}$.*

Proposition 10.14. *Let $T : V \to V$ be a linear transformation of a finite-dimensional k-vector space, then T is diagonalizable if and only if μ_T is a product of distinct linear polynomials in $k[X]$.*

Proof. We will prove the forward direction first, so suppose T is diagonalizable, hence there is a k-basis $\mathcal{B}$ such that $A = [T]^{\mathcal{B}}_{\mathcal{B}}$ is diagonal. Without loss of generality, assume that elements along the diagonal are ordered according to their multiplicity, i.e. $A = \operatorname{diag}(\lambda_1, \ldots, \lambda_1, \ldots, \lambda_s, \ldots, \lambda_s)$. Let $L_i(X) = X - \lambda_i$ be a linear polynomial in $k[X]$, hence

$$\begin{aligned} L_1(A) &= \operatorname{diag}(0, \ldots, 0, \lambda_2 - \lambda_1, \ldots, \lambda_2 - \lambda_1, \ldots, \lambda_s - \lambda_1, \ldots, \lambda_s - \lambda_1) \\ L_2(A) &= \operatorname{diag}(\lambda_1 - \lambda_2, \ldots, \lambda_1 - \lambda_2, 0, \ldots, 0, \ldots, \lambda_s - \lambda_2, \ldots, \lambda_s - \lambda_2) \\ &\vdots \end{aligned}$$

Define $f(X) = L_1(X)L_2(X)\cdots L_s(X)$. We then observe that $f(A)$ is the product of s matrices, each of which contains a block of zeros of dimension equal to the multiplicity of λ_i. This product is then equal to zero, hence $f \in \operatorname{ann}(V)$, but $\operatorname{ann}(V)$ is generated by the minimal polynomial, hence μ_T divides f, and so μ_T has distinct linear factors.

Now, suppose μ_T is a product of distinct linear polynomials, hence

$$\mu_T = (X - \lambda_1)(X - \lambda_2)\cdots(X - \lambda_s)$$

for distinct λ_i's in k. Since each λ_i is distinct, then each $k[X]/(X - \lambda_i)$ is coprime. It then follows by the Primary Decomposition Theorem (Theorem 8.8) that

$$V \cong {}_{(X-\lambda_1)}V \oplus \cdots \oplus {}_{(X-\lambda_s)}V$$

as a $k[X]$-module. □

11. Jordan Canonical Form

Definition 11.1 (Algebraic Closure)**.** *We say that a field k is algebraically closed if the roots of any polynomial $f \in k[X]$ are elements in k.*

For example, the complex numbers are algebraically closed; however, the real numbers are not.

Recall the definition of a p-primary module (Definition 8.7) which described $\mathbb{Z}$-modules of the form

$$\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{r_1} \oplus \cdots \oplus \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r_n}.$$

Throughout this section, we will consider the analogous $k[X]$-modules, appropriately named $(X - \lambda)$-primary modules, of the form

$$\left(\frac{k[X]}{(X-\lambda)}\right)^{r_1} \oplus \cdots \oplus \left(\frac{k[X]}{(X-\lambda)^n}\right)^{r_n}.$$

In fact, we will even further simplify our discussion by considering only a single summand, $k[X]/((X - \lambda)^d)$ for some nonzero power d.

Definition 11.2 (k-Algebra)**.** *Let k be a commutative ring and let A be a k-module. We say that A is a k-algebra if A has a ring structure compatible with scalar multiplication. This means that for all $\lambda \in k$, and for all $a, b \in A$, we have $(\lambda.a).b = a.(\lambda.b) = \lambda.(ab)$.*

Recall Proposition 10.3 in which we showed that $\{\overline{1}, \overline{X}, \ldots, \overline{X}^{d-1}\}$ is a $k[X]$-basis of $k[X]/(f)$ where $\deg(f) = d$. Furthermore, recall that $k[X]$ is a k-module with a ring structure, and therefore a k-algebra by the definition we just stated. In fact, there is a k-algebra isomorphism $\varphi : k[X] \to k[X]$ given by $X \mapsto X - \lambda$, wherein the reverse direction is given by $Y \mapsto Y + \lambda$. This means that there is a k-basis of $\frac{k[X]}{(X-\lambda)^d}$ given by $\{\overline{1}, \overline{Y}, \ldots, \overline{Y}^{d-1}\} = \{\overline{1}, \overline{X-\lambda}, \ldots, \overline{(X-\lambda)}^{d-1}\}$.

Similar to what we did in the case of the rational canonical form, let

$$\beta = \{v_1, v_2, \ldots, v_d\} \quad \text{where} \quad v_i = \overline{X-\lambda}^{d-i}.$$

Our goal will be to determine the form of the matrix

$$\left[T|_{\frac{k[X]}{(X-\lambda)^d}}\right]_\beta^\beta.$$

To do this, we need only consider how X acts on the basis elements of β. We consider $X.v_i$:

$$\begin{aligned} X.v_i \quad = \quad X.\overline{(X-\lambda)}^{d-i} &= (X-\lambda+\lambda).\overline{(X-\lambda)}^{d-1} \\ &= \overline{(X-\lambda)}^{d-i+1} + \lambda\overline{(X-\lambda)}^{d-i} \\ &= \overline{(X-\lambda)}^{d-i+1} + \lambda v_i. \end{aligned}$$

For all $i = 2, \ldots, d$, this means that $X.v_i = v_{i-1} + \lambda v_i$; however, for $i = 1$, $\overline{(X-\lambda)}^d = \overline{0}$, hence $X.v_1 = \lambda v_1$. From these observations, we have

$$\left[T|_{\frac{k[X]}{(X-\lambda)^d}}\right]_\beta^\beta = \begin{bmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ 0 & & & & \lambda \end{bmatrix}.$$

Theorem 11.3 (Jordan Canonical Form)**.** *Let k be algebraically closed, then every $A \in M_n(k)$ is similar to a matrix in block diagonal form, where each diagonal block is of the form as depicted above. We call each block a Jordan block with eigenvalue λ and dimension r, denoted $T(\lambda, r)$.*

Proof. Let $T : V \to V$ be a linear operator whose representing matrix is A, and let V be a $k[X]$-module via T. Express V as a $k[X]$-module in its elementary divisor decomposition. Since k is algebraically closed, then V is isomorphic to a direct sum of $(X-\lambda)$-primary modules. For each $(X-\lambda)$-primary module, determine the corresponding Jordan block for each multiplicity of $(X-\lambda)$ and use these to construct the block diagonal matrix

$$J_A = \begin{bmatrix} T(\lambda_1, r_1) & & & 0 \\ & T(\lambda_2, r_2) & & \\ & & \ddots & \\ 0 & & & T(\lambda_n, r_n) \end{bmatrix}.$$

where each (λ_i, r_i) pair is distinct. By our construction of each block, this says that there is a change-of-basis matrix $P \in GL_n(k)$ such that $A = PJ_AP^{-1}$, hence $A \sim J_A$. □

This is a good time to consider an example.

Example 11.4. *How many similarity classes in $M_4(\mathbb{C})$ have characteristic polynomial $\chi_T = (X-2)^4$?*

Solution. To answer this question, we need to consider all possible minimal polynomials. Recall that the Cayley-Hamilton Theorem tells us that μ_T divides χ_T, hence there are only four possibilities for μ_T, we will consider each. The four cases are $X-2$, $(X-2)^2$, $(X-2)^3$, and $(X-2)^4$. If $\mu_T = X-2$, then M_1's invariant decomposition must be $f_1 = f_2 = f_3 = f_4 = X-2$. If $\mu_T = (X-2)^2$, there are two possible invariant decompositions. Let M_2 have decomposition $f_1 = f_2 = 1$ and $f_3 = f_4 = (X-2)^2$; let M_3 have decomposition $f_1 = 1$, $f_2 = f_3 = X_2$, and $f_4 = (X-2)^2$. If $\mu_T = (X-3)^2$, then M_4 must have invariant decomposition $f_1 = f_2 = 1$, $f_3 = X-2$, and $f_4 = (X-2)^4$. Lastly, if $\mu_T = (X-2)^4$, then M_5 must have invariant decomposition $f_1 = f_2 = f_3 = 1$ and $f_4 = (X-4)^4$. These decompositions yield the following Jordan Canonical forms:

$$M_1 = \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & 2 & \\ & & & 2 \end{bmatrix} \quad M_2 = \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & 2 & 1 \\ & & 0 & 2 \end{bmatrix} \quad M_3 = \begin{bmatrix} 2 & 1 & & \\ 0 & 2 & & \\ & & 2 & 1 \\ & & 0 & 2 \end{bmatrix} \quad M_4 = \begin{bmatrix} 2 & & & \\ & 2 & 1 & 0 \\ & 0 & 2 & 1 \\ & 0 & 0 & 2 \end{bmatrix} \quad M_5 = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

□

Definition 11.5 (Field Extension)**.** *Let k be a field, then we say that K is a field extension of k, denoted K/k (K over k), if K is a field and $k \subset K$.*

A common example of this would be $\mathbb{C}/\mathbb{R}$, since $\mathbb{R} \subset \mathbb{C}$; with this in mind, we state the following theorem:

Theorem 11.6. *Let K/k be a field extension. Let $A, B \in M_n(k) \subset M_n(K)$ and suppose $A \sim_K B$, i.e. there is $P \in M_n(K)$ such that $A = PBP^{-1}$. Then, $A \sim_k B$, i.e. there is $Q \in M_n(k)$ such that $A = QBQ^{-1}$.*

Proof. Let $f_1^A | f_2^A | \cdots | f_s^A$ be the invariant decomposition of A in $k[X]$, and similarly let $f_1^B | f_2^B | \cdots | f_t^B$ be the invariant decomposition of B in $k[X]$. Let $F_1^A | F_2^A | \cdots | F_P^A$ be the invariant decomposition of A in $K[X]$, and let $F_1^B | F_2^B | \cdots | F_q^B$ be the invariant decomposition of B in $K[X]$.

Since $A \sim_K B$, then $p = q$ and $F_i^A = F_i^B$ for all $i = 1, \ldots, p$ by uniqueness of invariant decompositions. Note that $f_j^A \in k[X] \subset K[X]$ satisfies the condition of an invariant decomposition, and so $s = p$ and $f_j^A = F_j^A$ for all $j = 1, \ldots, p$. Similarly, $f_j^B \in k[X] \subset K[X]$ satisfies the condition of an invariant decomposition, and so $t = p$ and $f_j^B = F_j^B$ for all j. It then follows that $f_j^A = F_j^A = F_j^B = f_j^B$, hence $A \sim_k B$ as desired. □

This theorem tells us that if we can show that two matrices are similar in a field extension, then they are similar in the base field. For example, if $A, B \in M_n(\mathbb{R})$, then we need only show that $A \sim_{\mathbb{C}} B$ to conclude that $A \sim_{\mathbb{R}} B$.

12. Dual Spaces

Lemma 12.1. *Let k be a field and let V be a k-vector space, not necessarily finite-dimensional, then $Hom_k(k, V) \cong V$.*

Proof. This follows immediately from Theorem 1.11 since k is a field hence commutative, and k-vector spaces are precisely k-modules. □

Definition 12.2 (Dual Space)**.** *Let V be a k-vector space for some field k, then we say that $V^* := Hom_k(V, k)$ is the dual space of V.*

This definition is fairly simple and innocent, but it will prove to be incredibly powerful in practice. Furthermore, if V has a basis $\mathcal{B} = \{e_i\}_i$, then we define $e^i \in V^*$ such that

$$e^i(e_j) = \delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

Lemma 12.3 (Dual Basis Expansion)**.** *Let V be a finite-dimensional k-vector space. Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of V, and let $\mathcal{B}^* = \{e^1, \ldots, e^n\}$ be a collection such that $e^i(e_j) = \delta_{ij}$. Then, (1) $\mathcal{B}^*$ is a basis of V^*; (2) For all $v \in V$, $v = \sum_{i=1}^n e^i(v)e_i$; and (3) For all $\varphi \in V^*$, $\varphi = \sum_{i=1}^n \varphi(e_i)e^i$.*

Proof. We'll first prove (2), so let $v = \sum_i a_i e_i$ for some a_i since $\mathcal{B}$ is a basis for V. It then follows that

$$e^j(v) = e^j\left(\sum_i a_i e_i\right) = \sum_i a_i e^j(e_i) = \sum_i a_i \delta_{ij} = a_j,$$

and so $v = \sum_i a_i e_i = \sum_i e^i(v)e_i$.

Now for (3), we can't yet assume that $\mathcal{B}^*$ is a basis for V^*, we must show that the equation in (3) holds for all $v \in V$. Let $\varphi \in V^*$, and consider the following:

$$\left(\sum_i \varphi(e_i)e^i\right)(e_j) = \sum_i \varphi(e_i)e^i(e_j) = \sum_i \varphi(e_i)\delta_{ij} = \varphi(e_j),$$

and so (3) holds.

Lastly, we note that (2) says that $\mathcal{B}^*$ spans V^*, and so we need only show linear independence of $\mathcal{B}^*$. Suppose $0 = \sum_i a_i e^i$ for some coefficients $a_i \in k$, and so

$$0 = \left(\sum_i a_i e^i\right)(e_j) = \sum_i a_i e^i(e_j) = \sum_i a_i \delta_{ij} = a_j,$$

hence $a_i = 0$ for all $i = 1, \ldots, n$, therefore (1) holds. □

Definition 12.4 (Bilinear Form)**.** *Let V and W be k-vector spaces for some field k. A bilinear form is a function $B : V \times W \to k$ such that for all $v \in V$, $B(v, \cdot) : W \to k$ is linear and for all $w \in W$, $B(\cdot, w) : V \to k$ is linear. We will, on occasion, denote $B(\cdot, \cdot)$ by $\langle \cdot, \cdot \rangle$. We will denote the collection of all such bilinear forms by $Bilin(V \times W, k)$.*

Definition 12.5 ("Musical Maps")**.** *Note that the maps $B(\cdot, w)$ and $B(v, \cdot)$ from the definition of Bilinear Forms are homomorphisms in V^* and W^*. This means that we have maps, which are whimsically called "musical maps" given by $B^\flat : V \to W^*$ by $v \mapsto B(v, \cdot)$ and ${}^\flat B : W \to V^*$ by $w \mapsto B(\cdot, w)$.*

We will be mostly interested in instances where $V = W$ such that either $B(v, w) = B(w, v)$ or $B(v, w) = -B(w, v)$. These cases are important enough to warrant actual definitions.

Definition 12.6 (Symmetric and Skew-Symmetric)**.** *Let $B : V \times V \to k$ be a bilinear form for a k-vector space V. If B is such that $B(v, w) = B(w, v)$, then B is said to be symmetric. Similarly, if B is such that $B(v, w) = -B(w, v)$, then B is said to be skew-symmetric.*

In the case that B is symmetric, it follows that ${}^\flat B = B^\flat$; and in the case that B is skew-symmetric, it follows that ${}^\flat B = -B^\flat$.

Definition 12.7 (Nondegenerate and Nonsingular)**.** *Let $B : V \times V \to k$ be a symmetric or skew-symmetric bilinear form, then B is said to be nondegenerate if $V \xrightarrow{\flat} V^*$ is injective. Likewise, B is said to be nonsingular if $V \xrightarrow{\flat} V^*$ is surjective.*

Corollary 12.8. *In light of Definition 12.7, if V is a finite-dimensional k-vector space, then B is nondegenerate if and only if B is nonsingular if and only if $V \xrightarrow{\flat} V^*$ is an isomorphism.*

Proof. This is a consequence of the Dual Basis Expansion (Lemma 12.3). □

Definition 12.9 (Gram Matrix)**.** *Let $B : V \times W \to k$ be a bilinear form for k-vector spaces V and W. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis for V and let $\mathcal{C} = \{w_1, \ldots, w_m\}$ be a basis for W. The Gram Matrix of B is then given by*

$$ {}^{\mathcal{B}}[B]^{\mathcal{C}} = [\langle v_i, w_j \rangle]_{ij} = \begin{bmatrix} \langle v_1, w_1 \rangle & \cdots & \langle v_1, w_m \rangle \\ \vdots & \ddots & \vdots \\ \langle v_n, w_1 \rangle & \cdots & \langle v_n, w_m \rangle \end{bmatrix} $$

for all $i = 1, \ldots, n$ and all $j = 1, \ldots, m$.

Lemma 12.10. *Let V and W be finite-dimensional k-vector spaces with basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_m\}$, respectively. Then, for all $v \in V$ and all $w \in W$, we have*

$$ \langle v, w \rangle = {}^t[v]_{\mathcal{B}} \cdot {}^{\mathcal{B}}[B]^{\mathcal{C}} \cdot [w]_{\mathcal{C}}. $$

Proof. Let $v \in V$ and $w \in W$, hence $v = \sum_{i=1}^n a_i v_i$ and $w = \sum_{j=1}^m b_j w_j$. It then follows that

$$ \begin{aligned} \langle v, w \rangle &= \left\langle \sum_{i=1}^n a_i v_i, \sum_{j=1}^m b_j w_j \right\rangle \\ &= \sum_{i=1}^n a_i \left\langle v_i, \sum_{j=1}^m b_j w_j \right\rangle \\ &= \sum_{i=1}^n \sum_{j=1}^m a_i b_j \langle v_i, w_j \rangle, \end{aligned} $$

and this is precisely ${}^t[v]_{\mathcal{B}} \cdot {}^{\mathcal{B}}[B]^{\mathcal{C}} \cdot [w]_{\mathcal{C}}$. □

Definition 12.11 (Cogredient/Congruent)**.** *Let k be a field, we say that $A, B \in M_n(k)$ are cogredient/congruent if there is $P \in GL_n(k)$ such that $B = {}^tPAP$.*

Lemma 12.12. *Let $B : V \times V \to k$ be a bilinear form in V for some basis $\mathcal{B}$, and let $\mathcal{C}$ be another basis of V. Then, ${}^{\mathcal{B}}[B]^{\mathcal{B}}$ and ${}^{\mathcal{C}}[B]^{\mathcal{C}}$ are cogredient.*

Proof. Let $v, w \in V$, then

$$\begin{aligned} {}^t[v]_{\mathcal{C}} \cdot {}^{\mathcal{C}}[B]^{\mathcal{C}} \cdot [w]_{\mathcal{C}} = \langle v, w \rangle &= {}^t[v]_{\mathcal{B}} \cdot {}^{\mathcal{B}}[B]^{\mathcal{B}} \cdot [w]_{\mathcal{B}} \\ &= {}^t([\mathrm{id}]^{\mathcal{C}}_{\mathcal{B}} \cdot [v]_{\mathcal{C}}) \cdot {}^{\mathcal{B}}[B]^{\mathcal{B}} \cdot [\mathrm{id}]^{\mathcal{C}}_{\mathcal{B}} \cdot [w]_{\mathcal{C}} \\ &= {}^t[v]_{\mathcal{C}} \cdot \left({}^t[\mathrm{id}]^{\mathcal{C}}_{\mathcal{B}} \cdot {}^{\mathcal{B}}[B]^{\mathcal{B}} \cdot [\mathrm{id}]^{\mathcal{C}}_{\mathcal{B}}\right) \cdot [w]_{\mathcal{C}}, \end{aligned}$$

and so ${}^{\mathcal{C}}[B]^{\mathcal{C}} = {}^t[\mathrm{id}]^{\mathcal{C}}_{\mathcal{B}} \cdot {}^{\mathcal{B}}[B]^{\mathcal{B}} \cdot [\mathrm{id}]^{\mathcal{C}}_{\mathcal{B}}$. □

Proposition 12.13. *Let $B : V \times V \to k$ be a symmetric bilinear form on a finite-dimensional k-vector space V. Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of V and let $\mathcal{B}^* = \{e^1, \ldots, e^n\}$ be the dual basis of V^*. Then,*

$$[B^\flat]^{\mathcal{B}}_{\mathcal{B}^*} = {}^{\mathcal{B}}[B]^{\mathcal{B}}.$$

Proof. Let $A = [B^\flat]^{\mathcal{B}}_{\mathcal{B}^*} = [a_{ij}]_{ij}$, hence $B^\flat(e_j) = \sum_i a_{ij} e^i$. By Lemma 12.3, it follows that

$$\sum_i a_{ij} e^i = B^\flat(e_j) = \sum_i (B^\flat(e_j))(e_i) e^i = \sum_i B(e_j, e_i) e^i.$$

This means that $\sum_i (a_{ij} - B(e_j, e_i)) e^i = 0$, and since $\mathcal{B}^*$ is a basis of V^*, then $a_{ij} = B(e_j, e_i) = B(e_i, e_j)$, and our conclusion follows. □

Lemma 12.14. *Let k be a field. Let $\mathcal{C}$ be the category of k-vector spaces and let $\mathcal{D}$ be the category of k-dual spaces. Let V and W be k-vector spaces and let $T : V \to W$ be a linear transformation. Define $T^* : W^* \to V^*$ by $\psi \mapsto \psi \circ T$. Define $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ on objects by $V \mapsto V^*$ and and arrows by $T \mapsto T^*$. Then, $\mathcal{F}$ is a contravariant functor.*

Proof. Let V, W, U be k-vector spaces and let $T : V \to W$ and $R : W \to U$ be linear transformations. For all $\psi \in U^*$, we have

$$(R \circ T)^*(\psi) = \psi \circ R \circ T = R^*(\psi) \circ T = (T^* \circ R^*)(\psi),$$

hence $\mathcal{F}(R \circ T) = \mathcal{F}(T) \circ \mathcal{F}(R)$. Lastly, $\mathcal{F}(\mathrm{id}_V) = \mathrm{id}^*_V = \mathrm{id}_{V^*} = \mathrm{id}_{\mathcal{F}(V)}$, and so $\mathcal{F}$ is a contravariant functor. □

Proposition 12.15. *Let $T : V \to W$ be a linear transformation of k-vector spaces, and let $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_m\}$ bases of V and W, respectively. Then $[T^*]^{\mathcal{C}^*}_{\mathcal{B}^*} = {}^t[T]^{\mathcal{B}}_{\mathcal{C}}$.*

Proof. Let $A = [T]_{\mathcal{C}}^{\mathcal{B}} = [a_{ij}]_{ij}$ and let $B = [T^*]_{\mathcal{B}^*}^{\mathcal{C}^*} = [b_{ij}]_{ij}$. Then, $T(v_s) = \sum_r a_{rs} w_r$ and $T^*(w^j) = \sum_i b_{ij} v^i$. We also have

$$\begin{aligned} T^*(w^j) &= \sum_i (T^*(w^j))(v_i)v^i = \sum_i (w^j \circ T)(v_i)v^i = \sum_i w^j(T(v_i))v^i \\ &= \sum_i w^j \left(\sum_r a_{ri} w_r \right) v^i = \sum_i \sum_r a_{ri} w^j(w_r) v^i = \sum_i \sum_r a_{ri} \delta_{rj} v^i \\ &= \sum_i a_{ji} v^i. \end{aligned}$$

This implies that $b_{ij} = a_{ji}$, hence $B = {}^tA$, so $[T^*]_{\mathcal{B}^*}^{\mathcal{C}^*} = {}^t[T]_{\mathcal{C}}^{\mathcal{B}}$. □

Definition 12.16 (Quadratic Space)**.** *A quadratic space is a vector space equipped with a bilinear form, i.e.* (V, B) *where* $B : V \times V \to k$.

Definition 12.17 (Orthogonal Sum)**.** *Let* (V, B_V) *and* (W, B_W) *be two quadratic spaces, then* $V \boxplus W$ *is called an orthogonal sum.*

It turns out that $V \boxplus W = V \oplus W$ as vector spaces, hence the Gram Matrix for $V \boxplus W$ is block diagonal, of the form

$$\begin{bmatrix} {}^{\mathcal{B}}[B]^{\mathcal{B}} & 0 \\ 0 & {}^{\mathcal{C}}[B]^{\mathcal{C}} \end{bmatrix}$$

where $\mathcal{B}$ and $\mathcal{C}$ are bases of V and W, respectively.

13. Quadratic Forms

Definition 13.1 (Quadratic Form)**.** *Let* V *be a finite-dimensional* k*-vector space and let* $B : V \times V \to k$ *be a symmetric bilinear form. The associated quadratic form is the function* $Q : V \to k$ *given by* $Q(v) = \langle v, v \rangle$.

It follows immediately from this definition that if Q is a quadratic form, then $Q(av) = \langle av, av \rangle = a^2 \langle v, v \rangle = a^2 Q(v)$.

Lemma 13.2 (Polarization)**.** *Let* k *be a field such that* $char(k) \neq 2$. *Let* $Q : V \to k$ *be a quadratic form on* V. *Then we can recover the bilinear form* $B = \langle \cdot, \cdot \rangle : V \times V \to k$.

Proof. Let $v, w \in V$ and consider

$$\begin{aligned} \frac{1}{2}\big(Q(v+w) - Q(v) - Q(w)\big) &= \frac{1}{2}\big(\langle v+w, v+w \rangle - \langle v, v \rangle - \langle w, w \rangle\big) \\ &= \frac{1}{2}\big(\langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle - \langle v, v \rangle - \langle w, w \rangle\big) \\ &= \langle v, w \rangle. \end{aligned}$$

□

We now look at two different approaches to diagonalize a quadratic form.

Theorem 13.3. *Let $\langle \cdot, \cdot \rangle$ be a symmetric bilinear form on a finite-dimensional k-vector space V such that $\text{char}(k) \neq 2$. Then, there exists a basis $\mathcal{B}$ of V such that ${}^{\mathcal{B}}[\langle \cdot, \cdot \rangle]^{\mathcal{B}}$ is diagonal, i.e. $\mathcal{B}$ is an orthogonal basis.*

Proof. If the associated quadratic form $Q(v) = \langle v, v \rangle = 0$ for all $v \in V$, then we're done by Lemma 13.2. Otherwise, choose $v_1 \in V$ such that $Q(v_1) = \langle v_1, v_1 \rangle \neq 0$. Let $W = \text{span}\{v_1\}$ and let $W^\perp = \{w \in V : \langle w, v_1 \rangle = 0\}$. We claim that $V = W \boxplus W^\perp$, and so we must show that $V = W + W^\perp$ and $W \cap W^\perp = 0$. First, let $v \in W \cap W^\perp$, then $v = \lambda v_1$ for some $\lambda \in k$ and $\langle v, v_1 \rangle = 0$. This means that $0 = \langle v, v_1 \rangle = \langle \lambda v_1, v_1 \rangle = \lambda \langle v_1, v_1 \rangle = \lambda Q(v_1)$, but since $Q(v_1) \neq 0$, then $\lambda = 0$, and so $v = 0$. Let $v \in V$ and let $\lambda = \frac{\langle v_1, v \rangle}{\langle v_1, v_1 \rangle}$. We then have that $\langle v_1, v - \lambda v_1 \rangle = \langle v_1, v \rangle - \lambda \langle v_1, v_1 \rangle = 0$, and so $v - \lambda v_1 \in W^\perp$. It then follows that $v = \lambda v_1 + (v - \lambda v_1) \in W + W^\perp$.

Now, suppose $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a linearly independent set such that $\langle v_i, v_j \rangle = 0$ whenever $i \neq j$. Let $W = \text{span}(\mathcal{B})$ and choose some $v_{n+1} \in W^\perp = \{w \in V : \langle w, v_i \rangle \text{ for all } i = 1, \ldots, n\}$ such that $Q(v_{n+1}) \neq 0$. If no such element exists, we're done. Otherwise, let $\mathcal{B}' = \mathcal{B} \cup \{v_{n+1}\}$, let $W' = \text{span}\{\mathcal{B}'\}$, and let $W'^\perp = \{w \in V : \langle w, v_i \rangle = 0 \text{ for all } i = 1, \ldots, n+1\}$. Again, we want to show that $V = W' \boxplus W'^\perp$, and so let $v \in W' \boxplus W'^\perp$, hence

$$v = \sum_{i=1}^{n+1} \lambda_i v_i \quad \text{and} \quad \langle v, v_j \rangle = 0 \text{ for all } j = 1, \ldots, n+1.$$

It then follows for arbitrary j that

$$0 = \langle v, v_j \rangle = \left\langle \sum_{i=1}^{n+1} \lambda_i v_i, v_j \right\rangle = \sum_{i=1}^{n+1} \lambda_i \langle v_i, v_j \rangle = \begin{cases} \lambda_j Q(v_j), & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases},$$

and so $\lambda_j = 0$ and $v = 0$. Lastly, let $v \in V$ and let $\lambda_i = \frac{\langle v_i, v \rangle}{\langle v_i, v_i \rangle}$ for all $i = 1, \ldots, n+1$. We then have that

$$\left\langle v_j, v - \sum_{i=1}^{n+1} \lambda_i v_i \right\rangle = \langle v_j, v \rangle - \sum_{i=1}^{n+1} \lambda_i \langle v_j, v_i \rangle = \langle v_j, v \rangle - \lambda_j \langle v_j, v_j \rangle = 0,$$

and so

$$v - \sum_{i=1}^{n+1} \lambda_i v_i \in W'^\perp.$$

It then follows that $v \in W' + W'^\perp$, completing the proof. □

This approach is very similar to that of the Gram-Schmidt process, with the exception that we cannot yet require the basis to be normalized. However, this is incredibly important, as it says that we can find an orthogonal basis for any symmetric bilinear form over any field of characteristic other than 2.

We now consider a similar theorem from a bit more of an abstract viewpoint.

Theorem 13.4. *Let $\langle \cdot, \cdot \rangle : V \times V \to k$ be a symmetric bilinear form on a finite-dimensional k-vector space V with $\text{char}(k) \neq 2$. Let $W \subset V$ be a nondegenerate subspace, i.e. $\langle \cdot, \cdot \rangle|_W : W \times W \to k$ is nondegenerate. Then,*

(1) $\dim(W) + \dim(W^\perp) = \dim(V)$*;*

(2) $V \cong W \boxplus W^\perp$*; and*

(3) if V *itself was nondegenerate, then* $W^\perp$ *is also nondegenerate.*

Proof. Consider the exact sequence

$$0 \to W^\perp \hookrightarrow V \xrightarrow{\beta} W^* \to 0$$

where β is given by $v \mapsto \langle v, \cdot\rangle|_W$. This sequence has a section since we can define a map $s : W^* \to V$ by $e^i \mapsto e_i$ where $\{e_1, \dots, e_m\}$ is a basis for W. By Theorem 2.8, this means that $V \cong W^\perp \oplus W^*$, hence $\dim(V) = \dim(W^\perp) + \dim(W^*)$. Since W is nondegenerate, then $W \cong W^*$ by Corollary 12.8, and so $\dim(W^*) = \dim(W)$. It then follows that $\dim(V) = \dim(W) + \dim(W^\perp)$ and so (1) holds. Furthermore, since W is nondegenerate, then $W \cap W^\perp = 0$, hence $\dim(W \cap W^\perp) = 0$. Then, $\dim(W + W^\perp) = \dim(W) + \dim(W^\perp) - \dim(W^\perp \cap W) = \dim(W) + \dim(W^\perp) = \dim(V)$, and so (2) follows. Part (3) isn't exactly clear in my notes, so I'll fill this in later. □

Definition 13.5 (Inner Product)**.** *For* V *a real vector space, a symmetric bilinear form* $\langle\cdot,\cdot\rangle$ *on* V *is an inner product if it is positive definite, i.e. for all* $v \in V$*,* $\langle v, v\rangle \geq 0$ *with equality if and only if* $v = 0$*.*

Corollary 13.6 (Orthonormalization)**.** *Let* $\langle\cdot,\cdot\rangle$ *be a symmetric bilinear form on an* n*-dimensional* $\mathbb{R}$*-vector space. Then there exists a basis* $\mathcal{E}$ *of* V *such that the Gram Matrix has the form*

$$^{\mathcal{E}}[\langle\cdot,\cdot\rangle]^{\mathcal{E}} = \mathit{diag}(1, \dots, 1, -1, \dots, -1, 0, \dots, 0)$$

where there are t *ones,* s *negative ones, and* $n - s - t$ *zeros.*

Proof. Theorem 13.3 tells us that there is a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V such that

$$^{\mathcal{B}}[\langle\cdot,\cdot\rangle]^{\mathcal{B}} = \operatorname{diag}(a_1, \dots, a_r, 0, \dots, 0)$$

where $a_i \neq 0$. We then define a new basis $\mathcal{E} = \{e_1, \dots, e_n\}$ such that

$$e_j = \begin{cases} \frac{1}{\sqrt{|\langle v_j, v_j\rangle|}} v_j, & \text{if } j \leq r \\ v_j, & \text{if } j > r \end{cases}.$$

When $j > r$, then $Q(e_j) = \langle v_j, v_j\rangle = 0$; however, when $j \leq r$, then

$$Q(e_j) = Q\left(\frac{1}{\sqrt{|\langle v_j, v_j\rangle|}} v_j\right) = \frac{1}{|\langle v_j, v_j\rangle|} Q(v_j) = \frac{a_j}{|a_j|} = \pm 1.$$

□

Definition 13.7 (Rank/Signature)**.** *In light of Corollary 13.6, the rank of* V *is given by the value* r*; and the signature of* V *is given by the value of* s*.*

14. More Linear Algebra!

14.1 Adjoint Transformations

For a given linear transformation $T : V \to W$ where V and W are nondegenerate k-vector spaces, we know by contravariant functoriality of dual spaces that T induces a map $T^* : W^* \to V^*$. This requires us to work in dual spaces, which may not always be desirable, so can we induce a similar map $W \to V$? To answer this question, we consider the following diagram:

$$\begin{array}{ccc} W^* & \xrightarrow{T^*} & V^* \\ {\scriptstyle \flat_W}\uparrow & & \uparrow{\scriptstyle \flat_V} \\ W & & V \end{array}$$

and our definition then follows.

Definition 14.1 (Adjoint Transformation)**.** *Let V and W be nondegenerate finite-dimensional k-vector spaces with associated symmetric bilinear forms, and let $T : V \to W$ be a linear transformation. The map ${}^tT : W \to V$ given by ${}^tT = \flat_V^{-1} \circ T^* \circ \flat_W$ is called the adjoint transformation of T where $\flat$ is given by Definition 12.5.*

Note that we are only allowed to make this definition if V and W are nondegenerate and finite-dimensional, hence $\flat_V$ and $\flat_W$ define isomorphisms between duals.

Definition 14.2 (Symmetric Transformation)**.** *Given a linear transformation $T : V \to V$, we say that T is symmetric if ${}^tT = T$.*

Corollary 14.3. *Let V and W be as described above with $T : V \to W$ and ${}^tT : W \to V$ as defined. Then,*

$$\langle \cdot, {}^tT(w) \rangle_V = \langle T(\cdot), w \rangle_W.$$

Proof. Note that as an immediate consequence of the above definition, we have that

$$\flat_V \circ {}^tT = T^* \circ \flat_W$$

as maps $W \to V^*$. Let $w \in W$ and note that

$$(\flat_V \circ {}^tT)(w) = \flat_V({}^tT(w)) = \langle \cdot, {}^tT(w) \rangle_V$$

and

$$(T^* \circ \flat_W)(w) = T^*(\flat_W(w)) = T^*(\langle \cdot, w \rangle_W) = \langle \cdot, w \rangle_W \circ T = \langle T(\cdot), w \rangle_W.$$

The conclusion follows immediately. □

Corollary 14.4. *Let $\mathcal{B}$ and $\mathcal{C}$ be bases of V and W, respectively, where the conditions on V and W are given by the previous corollary. Then,*

$$[{}^tT]_{\mathcal{B}}^{\mathcal{C}} = G_V^{-1} \cdot {}^t[T]_{\mathcal{C}}^{\mathcal{B}} \cdot G_W$$

where G_V and G_W denote the associated Gram matrices. In particular, if $\mathcal{B}$ and $\mathcal{C}$ are orthonormal bases, then $[{}^tT]_{\mathcal{B}}^{\mathcal{C}} = {}^t[T]_{\mathcal{C}}^{\mathcal{B}}$.

Proof.

$$\begin{aligned}
[{}^tT]_{\mathcal{B}}^{\mathcal{C}} &= [\flat_V^{-1} \circ T^* \circ \flat_W]_{\mathcal{B}}^{\mathcal{C}} \\
&= [\flat_V^{-1}]_{\mathcal{B}}^{\mathcal{B}^*} \cdot [T^*]_{\mathcal{B}^*}^{\mathcal{C}^*} \cdot [\flat_W]_{\mathcal{C}^*}^{\mathcal{C}} \\
&= G_V^{-1} \cdot [T^*]_{\mathcal{B}^*}^{\mathcal{C}^*} \cdot G_W \quad \text{(Proposition 12.13)} \\
&= G_V^{-1} \cdot {}^t[T]_{\mathcal{C}}^{\mathcal{B}} \cdot G_W \quad \text{(Proposition 12.15).}
\end{aligned}$$

If $\mathcal{B}$ and $\mathcal{C}$ are orthonormal, then G_W and G_V are both identity matrices. □

14.2 Sesequilinear Forms and Hermitian Inner Products

Our goal now will be to define an inner product on $\mathbb{C}$-vector spaces. We might naively try to define one such inner product by

$$\left\langle \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}, \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \right\rangle = z_1 w_1 + \cdots + z_n w_n,$$

but we would quickly find this not to be a positive definite bilinear form, e.g.

$$\langle (i,0), (i,0) \rangle = i^2 = -1.$$

Fortunately, this is easily repaired by defining $\langle \cdot, \cdot \rangle : \mathbb{C}^n \to \mathbb{C}^n \to \mathbb{C}$ by

$$\left\langle \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}, \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \right\rangle = \overline{z_1} w_1 + \cdots + \overline{z_n} w_n,$$

where $\overline{z}$ is the complex conjugate of z. In particular, when $z_i = w_i$, then the inner product just defined yields

$$\overline{z_1} z_1 + \cdots + \overline{z_n} z_n = |z_1|^2 + \cdots + |z_n|^2 \geq 0$$

and this therefore positive definite.

We also note that this inner product ceases to be a bilinear form, since we are only linear in the second variable. In the first variable, we are *semilinear*, since we must conjugate any scalar we wish to "pull out" of the inner product. This is called semilinear, since if the scalar is real-valued, then this acts exactly as it would if the first variable were linear, which is clearly not the case for scalars with nonzero imaginary parts. A form of this type is said to be a *sesquilinear form.*

Definition 14.5 (Hermitian Inner Product)**.** *A Hermitian inner product on a $\mathbb{C}$-vector space V is a sesquilinear form $V \times V \to \mathbb{C}$ which is conjugate symmetric, i.e. $\langle w, v \rangle = \langle v, \overline{w} \rangle$, and positive definite.*

Definition 14.6 (Hermitian Transpose)**.** *Let $A \in M_n(\mathbb{C})$ and define the Hermitian transpose of A to be the conjugate transpose of A, denoted ${}^H A = \overline{{}^t A}$.*

Lemma 14.7. *Let V be a finite-dimensional $\mathbb{C}$-vector space, then for all $v, w \in V$, we have*

$$\langle v, w\rangle = {}^{H}[v]_{\mathcal{B}} \cdot {}^{\mathcal{B}}[B]^{\mathcal{C}} \cdot [w]_{\mathcal{C}}.$$

Proof. Following the proof of Lemma 12.10, we have

$$\langle v, w\rangle = \overline{{}^{t}[v]_{\mathcal{B}}} \cdot {}^{\mathcal{B}}[B]^{\mathcal{B}} \cdot [w]_{\mathcal{B}},$$

but since ${}^{H}A = \overline{{}^{t}A}$, then our conclusion follows. □

Recall Definition 14.1, which gave us a way to define an adjoint transformation given a linear transformation. In particular, we considered the diagram

$$\begin{array}{ccc} W^* & \xrightarrow{T^*} & V^* \\ {\scriptstyle \flat_W}\uparrow & & \uparrow{\scriptstyle \flat_V} \\ W & & V \end{array}$$

where $\flat_V$ and $\flat_W$ linear. In the context of sesequilinear forms, however, these are maps both semilinear when V and W are $\mathbb{C}$-vector spaces with Hermitian inner products. We can likewise induce a similar map, which we now define.

Definition 14.8 (Hermitian Adjoint)**.** *Let V and W be $\mathbb{C}$-vector spaces with Hermitian inner products and let $T : V \to W$ be a linear transformation. We then define ${}^{H}T = \flat_V^{-1} \circ T^* \circ \flat_W : W \to V$, called the Hermitian adjoint of T.*

As it turns out, since we are factoring elements in W through $\flat_W$ and $\flat_V^{-1}$, then ${}^{H}T$ becomes a linear transformation (since $\overline{\overline{z}} = z$). We also obtain results similar to those found in Corollaries 14.3 and 14.4, namely that

$$\langle T(v), w\rangle_W = \langle v, {}^{H}T(w)\rangle_V$$

and

$$[{}^{H}T]_{\mathcal{B}}^{\mathcal{C}} = {}^{H}[T]_{\mathcal{C}}^{\mathcal{B}} \text{ when } \mathcal{B} \text{ and } \mathcal{C} \text{ are orthonormal bases.}$$

Definition 14.9 (Self-Adjoint/Hermitian Transformation)**.** *Let $T : V \to W$ be a linear transformation of $\mathbb{C}$-vector spaces with Hermitian inner products. We say that T is self-adjoint (or Hermitian) if ${}^{H}T = T$. In particular, if $\mathcal{B}$ and $\mathcal{C}$ are orthonormal bases, respectively, then T is self-adjoint if and only if $A := [T]_{\mathcal{C}}^{\mathcal{B}}$ satisfies ${}^{H}A = A$, i.e. A is its own conjugate transpose.*

Definition 14.10 (Unity Transformation)**.** *Let V be a finite-dimensional $\mathbb{C}$-vector space with Hermitian inner product. A linear transformation $T : V \to V$ is unitary if for all $v, w \in V$, we have $\langle T(v), T(w)\rangle = \langle v, w\rangle$.*

15. Spectral Theorem

Our goal in section will be to prove the Spectral Theorem for two classes of transformations. This will provide us with criteria in which these classes can be diagonalized.

Lemma 15.1. *Let V be a finite-dimensional $\mathbb{C}$-vector space and let $T : V \to V$ be a linear transformation. Then, T has a nonzero eigenvector.*

Proof. Recall that eigenvalues of T are the roots of the characteristic polynomial $\chi_T \in \mathbb{C}[X]$. Since $\mathbb{C}$ is algebraically closed, then χ_T has a root, i.e. T has an eigenvalue, hence a nonzero eigenvector. □

Lemma 15.2. *Let $T : V \to V$ be a Hermitian linear transformation on a Hermitian vector space V. Then, (1) all eigenvalues of T are real; and (2) if v is a λ-eigenvector of T, and w is a μ-eigenvector of T such that $\lambda \neq \mu$, then $\langle v, w\rangle = 0$.*

Proof. Since T is Hermitian, then ${}^H T = T$ by Definition 14.9. Furthermore, Lemma 15.1 provides the existence of a nonzero eigenvector, so let $v \in V$ be one such eigenvector with associated eigenvalue λ. Note that $\langle v, v\rangle > 0$ and consider

$$\lambda\langle v, v\rangle = \langle v, \lambda v\rangle = \langle v, T(v)\rangle = \langle v, {}^H T(v)\rangle = \langle T(v), v\rangle = \langle \lambda v, v\rangle = \overline{\lambda}\langle v, v\rangle.$$

This means that $\lambda = \overline{\lambda}$, hence $\lambda \in \mathbb{R}$, and so (1) follows.

Next, let v and w be as in (2), and then

$$\mu\langle v, w\rangle = \langle v, \mu w\rangle = \langle v, Tw\rangle = \langle v, {}^H Tw\rangle = \langle Tv, w\rangle = \langle \lambda v, w\rangle = \lambda\langle v, w\rangle.$$

This means that $(\mu - \lambda)\langle v, w\rangle = 0$, and since $\lambda \neq \mu$, then $\langle v, w\rangle = 0$, so (2) holds. □

Lemma 15.3. *Let V be a finite-dimensional Hermitian inner product space, and let $T : V \to V$ be a linear transformation. Suppose $W \subset V$ is a T-invariant subspace, i.e. $Im(T|_W) = W$, then $W^\perp$ is an ${}^H T$-invariant subspace.*

Proof. Let $x \in W^\perp$, we must show that ${}^H T(x) \in W^\perp$. So, let $w \in W$ and consider $\langle w, {}^H T(x)\rangle = \langle T(w), x\rangle$. Since W is T-invariant, then $\langle T(w), x\rangle = 0$, and so $W^\perp$ is ${}^H T$-invariant as desired. □

These three lemmas then allow us to prove the following theorem.

Theorem 15.4 (Unitary Triangulability)**.** *Let V be a finite-dimensional Hermitian inner product space with $T : V \to V$ a linear transformation. Then, there exists an orthonormal basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}}^{\mathcal{B}}$ is upper triangular.*

Proof. Consider ${}^H T : V \to V$. Lemma 15.1 provides us a nonzero eigenvector v, which we can further assume to be normalized, i.e. $\langle v, v\rangle = 1$. Let $W = \text{span}\{v\}$, and so W is ${}^H T$-invariant. Lemma 15.3 then tells us that $W^\perp$ is ${}^{HH}T$-invariant, but ${}^{HH}T = T$, hence $W^\perp$ is T-invariant. By induction, there exists an orthonormal basis $\{v_1, \ldots, v_{n-1}\}$ of $W^\perp$. Then, $\mathcal{B} = \{v_1, \ldots, v_{n-1}, v\}$ is an orthonormal basis of V, and $[T]_{\mathcal{B}}^{\mathcal{B}}$ is upper triangular. Need to fill in the details... □

Theorem 15.5 (Spectral Theorem for Self-Adjoint Operators)**.** *Let V be a finite-dimensional Hermitian inner product space and let $T : V \to V$ be self-adjoint. Then, there is an orthonormal basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}}^{\mathcal{B}}$ is diagonal. Furthermore, if $A \in M_n(\mathbb{C})$ such that ${}^H A = A$, then there exists a unitary matrix P such that PAP^{-1} is diagonal.*

Proof. Theorem 15.4 provides us an orthonormal basis $\mathcal{B}$ such that $[T]_{\mathcal{B}}^{\mathcal{B}}$ is upper triangular. Since T is self-adjoint, then ${}^H T = T$, and since $\mathcal{B}$ is orthonomal, then ${}^H A = A$ by Definition 14.9. We then have

$$ {}^H A = \begin{bmatrix} \overline{a_{11}} & & 0 \\ & \ddots & \\ * & & \overline{a_{nn}} \end{bmatrix} = \begin{bmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{bmatrix} = A, $$

hence $* = 0$, and $a_{ii} = \overline{a_{ii}}$. This means that

$$ A = \begin{bmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{bmatrix}, $$

where $a_{ii} \in \mathbb{R}$. □

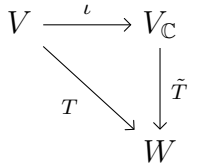
Lastly, as a corollary to the Spectral Theorem for Self-Adjoint Operators, we state the following theorem without proof.

Theorem 15.6 (Spectral Theorem for Symmetric Transformations)**.** *Let V be a finite-dimensional real inner product space with $T : V \to V$ a symmetric linear transformation. Then, there is an orthonormal basis $\mathcal{B}$ of V such that $[T]_{\mathcal{B}}^{\mathcal{B}}$ is diagonal. Furthermore, if $A \in M_n(\mathbb{R})$ such that ${}^t A = A$, then there is an orthogonal $P \in GL_n(\mathbb{R})$, i.e. ${}^t P = P^{-1}$, such that PAP^{-1} is diagonal.*

Lemma 15.7. *There is an isomorphism $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$.*

Proof. Let $\varphi : \{X\} \to \mathbb{C}$ be a set map given by $X \mapsto i$. This map induces $\tilde{\varphi} : \mathbb{R}[X] \to \mathbb{C}$ such that $\tilde{\varphi}(X) = i$. Let $g \in \mathrm{Ker}(\tilde{\varphi})$ and let $g = q(X^2+1)+r$ by the division algorithm, such that $\deg(r) < 2$. Then $0 = \tilde{\varphi}(g) = \tilde{\varphi}(q \cdot (X^2+1) + r) = \tilde{\varphi}(q)\tilde{\varphi}(X^2+1) + \tilde{\varphi}(r) = \tilde{\varphi}(q)(i^2+1)+\tilde{\varphi}(r) = \tilde{\varphi}(r)$. Since $\deg(r) < 2$, then $r = r_0 + r_1 X$, hence $0 = \tilde{\varphi}(r) = r_0 + r_1 i$, so $r = 0$. It then follows that $\mathrm{Ker}(\tilde{\varphi})$ is a principal ideal generated by X^2+1. By the First Isomorphism Theorem, this implies that $\mathbb{C} \cong \frac{\mathbb{R}[X]}{(X^2+1)}$. □

Definition 15.8 (Complexification)**.** *Let V be a finite-dimensional $\mathbb{R}$-vector space. The complexification of V is a $\mathbb{C}$-vector space $V_{\mathbb{C}}$ equipped with an $\mathbb{R}$-linear map $\iota : V \to V_{\mathbb{C}}$ which is universal: i.e. for all $\mathbb{C}$-vector spaces W and all $\mathbb{R}$-linear maps $T : V \to W$, there is a unique $\mathbb{C}$-linear map $\tilde{T} : V_{\mathbb{C}} \to W$ such that the diagram*



commutes.

As with all universal mapping properties, we need only construct such an object and uniqueness follows immediately. To construct such an object, define a map $J : V \oplus V \to V \oplus V$ by $(v, w) \mapsto (-w, v)$, and define $\epsilon_J : \mathbb{R}[X] \to \text{End}(V \oplus V)$ by $X \mapsto J$. It then follows that $\epsilon_J(X^2) = J(-w, v) = (-v, -w)$, hence $\epsilon_J(X^2 + 1) = 0$, and so $(X^2 + 1) \subset \text{Ker}(\epsilon_J)$. The fundamental theorem on homomorphisms then induces a unique map $\mathbb{R}[X]/(X^2+1) \to \text{End}(V \oplus V)$. Lemma 15.7 then implies that $V \oplus V$ can be viewed as a $\mathbb{C}$-module, and so we define $V_{\mathbb{C}} = V \oplus V$. This means that $V_{\mathbb{C}}$ is a $\mathbb{C}$-module (i.e. $\mathbb{C}$-vector space) with the following module structure:

$$\mathbb{C} \times V_{\mathbb{C}} \to V_{\mathbb{C}} \quad \text{given by} \quad (a + bi, (v, w)) \mapsto (av - bw, aw + bv).$$

Lemma 15.9. *Let V be a finite-dimensional $\mathbb{R}$-vector space, then the complexification of V is given by the $\mathbb{C}$-vector space $V_{\mathbb{C}}$ just constructed with universal $\mathbb{R}$-linear map $\iota : V \to V_{\mathbb{C}}$ given by $v \mapsto (v, 0)$.*

Proof. Let W be a $\mathbb{C}$-vector space and let $T : V \to W$ be $\mathbb{R}$-linear. We then define $\tilde{T} : V_{\mathbb{C}} \to W$ by $(v, w) \mapsto T(v) + iT(w)$, and so $\tilde{T}\iota(v) = \tilde{T}(v, 0) = T(v)$ as desired. It is clear that $\tilde{T}(v_1 + v_2, w_1 + w_2) = \tilde{T}(v_1, w_1) + \tilde{T}(v_2, w_2)$ is evident. Furthermore, we have

$$\begin{aligned} \tilde{T}\big((a + bi).(v, w)\big) &= \tilde{T}(av - bw, aw + bv) = T(av - bw) + iT(aw + bv) \\ &= a(T(v) + iT(w)) + b(iT(v) - T(w)) \\ &= a\tilde{T}(v, w) + bi(T(v) + iT(w)) \\ &= (a + bi)\tilde{T}(v, w), \end{aligned}$$

and so $\tilde{T}$ is $\mathbb{C}$-linear. Lastly, suppose there is $\hat{T} : V_{\mathbb{C}} \to W$ such that $T = \hat{T} \circ \iota$. Then, we observe that

$$\hat{T}(v, w) = \hat{T}(v, 0) + i\hat{T}(w, 0) = \tilde{T}(v, 0) + i\tilde{T}(w, 0) = \tilde{T}(v, w),$$

hence $\tilde{T}$ is unique. □

16. Group Actions

Definition 16.1 (G-Sets #1)**.** *Let G be a group. A G-set is a set X equipped with a scalar multiplication $G \times X \to X$ satisfying the axioms (1) $g.(h.x) = (gh).x$ for all $g, h \in G$ and all $x \in X$; and $1.x = x$ for all $x \in X$. Alternatively, we can view a*

Definition 16.2 (G-Sets #2)**.** *A G-set is a set X equipped with a group homomorphism $\varphi : G \to S(X)$ where $S(X)$ is the set of permutations of X.*

Theorem 16.3. *Definition 16.1 and Definition 16.2 are equivalent.*

Proof. Given a group homomorphism $\varphi : G \to S(X)$, we simply define $G \times X \to X$ by $(g, x) \mapsto \varphi(g)(x)$. The two axioms hold by virtue of the way permutation composition is defined in addition to the fact that the identity in G must map to the identity permutation in $S(X)$, hence Definition 16.2 implies 16.1.

On the other hand, suppose we have $G \times X \to X$ such that the two axioms are satisfied. We then define $\varphi : G \to S(X)$ by $\big(\varphi(g)\big)(x) = g.x$. We must verify that

$\varphi(g) \in S(X)$ as well as that φ defines a group homomorphism. First, we need to show that $\varphi(g) \circ \varphi(g^{-1}) = \mathrm{id} = \varphi(g^{-1}) \circ \varphi(g)$. Let $x \in X$ and consider

$$\varphi(g)\big(\varphi(g^{-1})(x)\big) = \varphi(g)\big(g^{-1}.x\big) = g.(g^{-1}.x) = (gg^{-1}).x = 1.x = x,$$

hence $\varphi(g) \circ \varphi(g^{-1}) = \mathrm{id}$ and the opposite composition holds as well. This means that $\varphi(g) \in S(X)$. Lastly, let $g, h \in G$ and $x \in X$, we then have

$$\varphi(gh)(x) = (gh).x = g.(h.x) = g.\varphi(h)(x) = (\varphi(g) \circ \varphi(h))(x),$$

and so φ is a group homomorphism. □

We now have two separate ways to think of G-sets, either as a scalar multiplication or as a group homomophism into the group of permutations on X. If X is a finite set and $n = |X|$ is the number of elements of X, then our second definition tells us that we are effectively mapping G into S_n, the symmetric group on n elements. This can tell us a lot about the structure of certain groups as the following example will demonstrate.

Proposition 16.4. *Denote the field of p elements by $\mathbb{F}_p$, and denote the sets of invertible $n \times n$ matrices over $\mathbb{F}_p$ by $GL_n(\mathbb{F}_p)$. In particular, when $n = 2$ and $p = 2$, then $GL_2(\mathbb{F}_p) \cong S_3$.*

Proof. Let X be the set of non-zero vectors in $\mathbb{F}_2^2$ and define a group action $\mathrm{GL}_2(\mathbb{F}_2) \times X \to X$ by $(A, x) \mapsto Ax$. This means that there is a group homomorphism $\varphi : \mathrm{GL}_2(\mathbb{F}_2) \to S(X) \cong S_3$ given by $(\varphi(A))(x) = Ax$. Suppose $\varphi(A) = \varphi(B)$, then $Ax = Bx$ for all $x \in X$, and so $B^{-1}Ax = x$. Since this equality is true for $x = 0$ as well, then it follows that $B^{-1}A = I$, therefore $A = B$ and φ is injective. Lastly, it is easily seen that $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$ and so φ is surjective, hence $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ as desired. □

Definition 16.5 (Stabilizer/Isotropy Subroup)**.** *Let G be a group and let X be a G-set. Fix $x \in X$. We define the stabilizer (or isotropy subgroup) of x by $G_x = \{g \in G : g.x = x\}$.*

We provided an alternative name for the stabilizer of an element $x \in G$, called the isotropy subgroup of x, so it would be appropriate to actually prove this is a subgroup of G.

Proposition 16.6. *Let X be a G-set and let $x \in X$, then $G_x \leq G$.*

Proof. Let $g, h \in G_x$, and note that $h.x = x$, hence $h^{-1}.x = h^{-1}.(h.x) = (h^{-1}h).x = 1.x = x$, and so $h^{-1} \in G_x$. We then have $(gh^{-1}).x = g.(h^{-1}.x) = g.x = x$, and so $gh^{-1} \in G_x$, so G_x is a subgroup of G. □

There are some canonical examples that will be important to consider in the coming pages, which we will now describe.

Example 16.7 (Left-Translation)**.** *When $X = G$, we say that G acts by left-translation, i.e. $G \times G \to G$ given by $(g, x) \mapsto g.x = gx$.*

Example 16.8 (Coset Action)**.** *Let H be a subgroup of G and let $X = G/H$. We then define a left-translation action $G \times G/H \to G/H$ given by $(g, xH) \mapsto g.xH = gxH$.*

We must verify that this action is well-defined. Suppose $xH = yH$, hence $y^{-1}xH = H$, and so $y^{-1}x \in H$. Then, $y^{-1}x = y^{-1}g^{-1}gx = (gy)^{-1}gx \in H$, hence $gxH = gyH$, so our group action is well-defined.

Moreover, let $xH \in X$ and let $g \in G_{xH}$, so that $gxH = g.xH = xH$, hence $x^{-1}gx \in H$, so $g \in xHx^{-1}$. Since the reverse direction follows in the same manner, we conclude that $G_{xH} = gHg^{-1}$.

Example 16.9 (Action by Conjugation)**.** *Let $X = G$ and define the group action $G \times G \to G$ by $(g, x) \mapsto g.x = gxg^{-1}$.*

For a fixed $g \in G$, we can vary $x \in G$, which in turn defines an inner automorphism. This means that we are mapping G into the set of automorphisms on G, hence $\varphi : G \to \mathrm{Aut}(G) \subset S(G)$. In fact, for a fixed $x \in X$, it is easily seen that $G_x = \{g \in G : g.x = gxg^{-1} = x\} = C_G(x)$, the centralizer of x in G.

Example 16.10 (Action on Subgroups)**.** *Let X be the set of subgroups of G, we then define an action $G \times X \to X$ by conjugation, i.e. $(g, H) \mapsto gHg^{-1}$.*

For a fixed subgroup $H \leq G$, the stabilizer of H is the set of all $g \in G$ such that $gHg^{-1} = H$, hence $G_H = N_G(H)$, the normalizer of H in G.

Theorem 16.11. *Let X be a G-set defined by translation, i.e. $G \times X \to X$ given by $(g, x) \mapsto g.x$. Then, the group homomorphism $\varphi : G \to S(X)$ is such that*

$$Ker(\varphi) = \bigcap_{x \in X} G_x.$$

Proof. Fix $h \in \mathrm{Ker}(\varphi)$, and so $\varphi(h)$ is the identity permutation. This means that $(\varphi(h))(x) = h.x = x$ for all $x \in X$, which says that $h \in G_x$ for all $x \in X$. It then follows that

$$\mathrm{Ker}(\varphi) \subset \bigcap_{x \in X} G_x,$$

and the converse is easily seen to hold by reversing the same process. □

Theorem 16.12. *Let G be a finite group with $H \leq G$ a subgroup such that $|G| \nmid [G : H]!$. Then, there exists a normal subgroup $K \lhd G$ such that $1 \neq K \subset H$.*

Proof. By Example 16.8, there is a group action on G/H defined by $(g, xH) \mapsto gxH$. This in turn defines a homomorphism $\varphi : G \to S(G/H)$, but $|S(G/H)| = [G : H]!$. However, since $|G| \nmid [G : H]!$, then φ cannot be an injection by Lagrange's Theorem. This means that $\mathrm{Ker}(\varphi) \neq 1$, and so there must be a normal subgroup $K = \mathrm{Ker}(\varphi) \neq 1$. Since the given group action is given by translation, then Lemma 16.11 and our observation after Example 16.8 tell us that

$$K = \bigcap_{xH \in G/H} G_{xH} = \bigcap_{xH \in G/H} xHx^{-1} \subset H.$$

□

Theorem 16.13. *Let G be a finite group and let $1 \neq H \leq G$ be a subgroup such that $[G : H] = p$ where p is the smallest prime dividing $|G|$, then $H \lhd G$.*

Proof. Let $G \times G/H \to G/H$ be given by left translation, so there is a homomorphism $\varphi : G \to S(G/H)$. Theorem 16.11 tells us that $\mathrm{Ker}(\varphi)$ is the intersection of isotropy subgroups G_{xH} for all $xH \in G/H$. This means that $\mathrm{Ker}(\varphi) \subset G_{1H} = H$, hence $|\mathrm{Ker}(\varphi)| \leq |H|$. We know that $|G| = |\mathrm{Im}(\varphi)| \cdot |\mathrm{Ker}(\varphi)|$, and so $|\mathrm{Im}(\varphi)|$ must divide $|G|$. Moreover, we know that $|\mathrm{Im}(\varphi)|$ divides $p!$ since $\mathrm{Im}(\varphi) \leq S_p$, and so either $|\mathrm{Im}(\varphi)| = p$ or φ is the trivial homomorphism. In the latter case, we have that $\mathrm{Ker}(\varphi) = G$, but $\mathrm{Ker}(\varphi) \subset H$, so $G = H$, hence $[G : H] = 1$, a contradiction. This means that $|\mathrm{Im}(\varphi)| = p$, and so $|\mathrm{Ker}(\varphi)| = |G|/p = |H|$. Since $\mathrm{Ker}(\varphi) \subset H$ and they have the same order, then $H = \mathrm{Ker}(\varphi) \lhd G$, as desired. □

Proposition 16.14 (Equivalence Relation on G-Sets)**.** *Let X be a G-set, we then define $\sim$ such that $x \sim y$ if there exists $g \in G$ such that $g.x = y$. Then, $\sim$ is an equivalence relation.*

Proof. Reflexivity follows by the second axiom of G-sets. Now, let $x \sim y$, so there is $g \in G$ such that $g.x = y$, then $g^{-1}.y = g^{-1}.(g.x) = (g^{-1}g).x = 1.x = x$, and so $y \sim x$. Lastly, suppose $x \sim y$ and $y \sim z$, so there is $g, h \in G$ such that $g.x = y$ and $h.y = z$. It then follows that $(hg).x = h.(g.x) = h.y = z$, hence $x \sim z$. □

Definition 16.15 (Orbit)**.** *Let $\sim$ be the equivalence relation just defined, the equivalence classes induced by $\sim$ are then called orbits. We denote the orbit of $x \in X$ by*

$$\mathcal{O}_x = \{g.x : g \in G\}.$$

It is easily seen by this definition that $x \sim y$ if and only if $\mathcal{O}_x = \mathcal{O}_y$.

Definition 16.16 (Transitive Class)**.** *Let X be a G-set, we say that X is transitive if there is only one orbit, i.e. $\mathcal{O}_x = X$ for any $x \in X$. In particular, individual orbits are transitive G-sets.*

Recall Example 16.7, in which G acted on itself by left-translation. Let $x, y \in G$, then $(yx^{-1})x = y(x^{-1}x) = y$, and so this group action is transitive.

Furthermore, consider Example 16.8, where we acted upon cosets of G/H for some subgroup $H \leq G$. Let $xH, yH \in G/H$, then $(yx^{-1}).xH = y.(x^{-1}xH) = yH$, hence this group action is also transitive.

Lastly, consider Example 16.10. An orbit in this case is given by $\mathcal{O}_x = \{g.x = gxg^{-1} : g \in G\}$ where $x \in G$, and so the orbits via this group action provide us with the conjugacy class containing $x \in G$.

Definition 16.17 (G-Set Maps)**.** *Let X and Y be G-sets. A G-set map $f : X \to Y$ is a function satisfying $f(g.x) = g.f(x)$ for all $x, y \in X$, $g \in G$. In particular, if f is a bijection, then f is said to be a G-set isomorphism.*

Theorem 16.18 (Structure Theorem for G-Sets)**.** *(1) Any G-set X is a disjoint union of transitive G-sets, and (2) any transitive G-set is isomorphic to G/H as a G-set for some $H \leq G$.*

Proof. Let X be a G-set, then the equivalence relation partitions X into disjoint orbits, which are transitive by definition, and so (1) holds. Now, suppose X is a transitive G-set and let $x \in X$, hence $H = G_x$ by definition of transitivity. Our claim is that $X \cong G/H$ as G-sets. Define a map $f : G/H \to X$ by $f(gH) = g.x$, we must show that this is well-defined and that it is a G-set isomorphism. First, suppose $g_1H = g_2H$, then $g_2^{-1}g_1H = H$, so $g_2^{-1}g_1 \in H = G_x$. This means that $(g_2^{-1}g_1).x = x$, hence $g_1.x = g_2.x$, and so f is well-defined. We then consider $f(k.gH) = f(kgH) = (kg).x = k.(g.x) = k.f(gH)$, so f is a G-set map. Suppose $f(g_1H) = f(g_2H)$, then $g_1.x = g_2.x$, so $g_2^{-1}g_1.x = x$, hence $g_2^{-1}g_1 \in G_x = H$ and it follows that $g_2H = g_1H$. Lastly, since X is assumed to be transitive, then f is surjective, and therefore $X \cong G/H$ as G-sets. □

Corollary 16.19. *Let X be a G-set with G finite, and let $\mathcal{O}_x$ be the orbit of $x \in X$. Then, $|G| = |\mathcal{O}_x| \cdot |G_x|$.*

Proof. Since $\mathcal{O}_x$ is a transitive G-set, then $\mathcal{O}_x \cong G/H$ where we can take $H = G_x$ by the proof of Theorem 16.18. Given that G is finite, this means that $|\mathcal{O}_x| = |G|/|G_x|$, and so $|G| = |\mathcal{O}_x| \cdot |G_x|$ as claimed. □

Theorem 16.20 (Cauchy)**.** *Let G be a finite group and let p divide $|G|$ where p is prime, then there is an element in G with order p.*

Proof. Let $C = \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$ be the cyclic group of order p. Let

$$X = \{(g_1, \ldots, g_p) \in G \times \cdots \times G : g_1 \cdots g_p = 1\}$$

be a C-set where $C \times X \to X$ is given by $(\sigma, x) = \sigma.x = \sigma.(g_1, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$. This action is well-defined, since $g_1 \cdots g_p = 1$ implies that $g_2 \cdots g_p = g_1^{-1}$, and so $g_2 \cdots g_p g_1 = 1$. Theorem 16.18 says that transitive sets are isomorphic to C/H for some $H \leq C$, and since C is cyclic order p, then the only possible transitive C-sets are $C/1$ and C/C; the former has order p and the latter has order 1. In particular, this says that

$$X = \mathcal{O}_1 \sqcup \cdots \sqcup \mathcal{O}_r \sqcup \mathcal{O}'_1 \sqcup \cdots \sqcup \mathcal{O}'_s$$

where $|\mathcal{O}_i| = 1$ and $|\mathcal{O}'_j| = p$ for appropriate values of i and j. Since the orbits are disjoint (hence the usage of $\sqcup$), this says that $|X| = r + ps \equiv r \pmod{p}$. Furthermore, by the way X was defined, we have $p - 1$ degrees of freedom, i.e. we are free to choose any of the $|G|$ elements to fill the first $p - 1$ entries in X; however, we are forced to make the last choice by the relation $g_1 \cdots g_p = 1$. This means that $|X| = |G|^{p-1}$ and since p divides $|G|$, then $|X| \equiv 0 \pmod{p}$. It then follows that $r \equiv 0 \pmod{p}$, and so we must show that $r \neq 0$ by providing the existence of a singleton orbit, i.e. $(x, \ldots, x)$ such that $x^p = 1$. Clearly $(1, \ldots, 1)$ is a singleton orbit, and so it follows that $r \neq 0$, hence $r \geq p \geq 2$, and so there must be some other element in G with order p. □

Definition 16.21 (p-Groups)**.** *Let G be a group such that all $g \in G$ have order p^k for some $k \geq 0$; we then say that G is a p-group.*

Definition 16.22 (Fixed-Point Set)**.** *Let X be a G-set, then the fixed-point set of X with respect to G is denoted $X^G = \{x \in X : g.x = x \text{ for all } g \in G\}$.*

Theorem 16.23 (Class Equation)**.** *Let G be a finite p-group and let X be a G-set. Then $|X^G| \equiv |X| \pmod{p}$.*

Proof. A transitive set must be isomorphic to G/H as a G-set where $H \leq G$ such that $|G/H| = [G : H] = p^k$ for some $k \geq 0$. It then follows that

$$X = \mathcal{O}_1 \sqcup \cdots \sqcup \mathcal{O}_r \sqcup \mathcal{O}'_1 \sqcup \cdots \sqcup \mathcal{O}'_s$$

where $|\mathcal{O}_i| = 1$, and p divides $|\mathcal{O}'_j|$. Let $x \in X^G$, hence $g.x = x$ for all $g \in G$, and so $\mathcal{O}_x = \{g.x : g \in G\} = \{x\}$. This means that the elements of X^G are exactly those which constitute the singleton orbits of X, and so $|X^G| = r$. It then follows that $|X^G| \equiv |X| \pmod{p}$ since all larger orbits have cardinality divisible p. □

Corollary 16.24. *Let G be a finite p-group, then $Z(G)$, the center of G, is non-trivial.*

Proof. Let G act on itself by conjugation, i.e. $g.x = gxg^{-1}$, then Theorem 16.23 tells us that $|G^G| \equiv |G| \pmod{p}$. We then observe that

$$\begin{aligned} G^G &= \{x \in G : g.x = x \text{ for all } g \in G\} \\ &= \{x \in G : gxg^{-1} = x \text{ for all } g \in G\} \\ &= \{x \in G : gx = xg \text{ for all } g \in G\} = Z(G). \end{aligned}$$

We then note that $|G| = p^k$ for some $k \geq 1$, hence $|G| \equiv 0 \pmod{p}$, and so $|Z(G)| \equiv 0 \pmod{p}$. However, $1 \in Z(G)$, so $|Z(G)| \geq p$, therefore $Z(G)$ is non-trivial. □

Lemma 16.25. *Let G be a finite group, then $G/Z(G)$ cannot be a non-trivial cyclic group.*

Proof. Let $Z = Z(G)$ and suppose G/Z is cyclic, and so $G/Z = \{Z, gZ, g^2Z, \ldots, g^{n-1}Z\}$ for some $g \in G$. Moreover, this means that any element in G is of the form $g^k z$ for some $z \in Z$. It then follows that $(g^k z)(g^q z') = g^k(zg^q)z' = g^k(g^q z)z' = (g^k g^q)(zz') = (g^q g^k)(z'z) = g^q(g^k z')z = g^q(z'g^k)z = (g^q z')(g^k z)$, and so G is abelian. It then follows that $Z = G$, hence $G/Z = 1$. □

This lemma says that if G is a finite group such that $G/Z(G)$ is cyclic, then G must be an abelian group.

Corollary 16.26. *Any group of order p^2 with p prime is abelian.*

Proof. Let G have order p^2 and note that G is a p-group, hence $Z(G)$ is non-trivial by Corollary 16.24. If $|Z(G)| = p$, then $|G/Z(G)| = p$ and must therefore by cyclic order p; however, this contradicts Lemma 16.25. We must therefore have that $|Z(G)| = p^2$, hence $Z(G) = G$ and so G is abelian. □

Corollary 16.27. *Let G be a p-group, then there is $K \lhd G$ such that $|K| = p$.*

Proof. Since G is a p-group, it has non-trivial center, and so there is some $z \in Z(G)$ such that $z \neq 1$ where $z^p = 1$. Let $K = \langle z \rangle$; it then follows that $K \lhd G$ since $z \in Z(G)$. □

Corollary 16.28. *Let G be a p-group, i.e. $|G| = p^n$, and let $m \leq n$. Then, there is $K \lhd G$ such that $|K| = p^m$.*

Proof. Lemma 16.27 tells us that there is some $K' \lhd G$ such that $|K'| = p$. Define $\pi : G \to G/K'$ as the canonical projection map, hence $|G/K'| = p^{n-1}$, and so G/K' is a p-group as well. By induction on Corollary 16.27 it follows that there is some $\overline{K} \lhd G/K'$ such that $|\overline{K}| = p^{m-1}$. Now, let $K = \pi^{-1}(\overline{K})$, and since $\overline{K} \lhd G/K'$ and π is a homomorphism, then $K \lhd G$; furthermore, $|K| = p^m$. □

Lemma 16.29. *Let G be a group and let $H \leq G$ and $K \leq G$. Define $HK = \{hk : h \in H, k \in K\}$ and suppose that $HK = KH$, then $HK \leq G$.*

Proof. A subgroup must contain the identity of G, must be closed under operation and under inverse. Clearly, $1 \in HK$, and we then observe that $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$. Similarly, $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$, and therefore $HK \leq G$. □

Theorem 16.30 (Second Isomorphism Theorem)**.** *Let G be a group, let $H \leq G$ and $K \lhd G$. Then, (1) $HK \leq G$; (2) $H \cap K \lhd G$; and (3)*

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

Proof. First, we observe that

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$$

and so Lemma 16.29 tells us that (1) holds. Now, define $\pi : G \to G/K$ as the canonical projection map, and so the following diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/K \\ \uparrow & & \uparrow \\ H & \xrightarrow{\pi|_H} & \pi(H) \end{array}$$

commutes. Note that the canonical projection map acts by $g \mapsto gK$, hence $\pi|_H$ maps $h \mapsto hK$. This means that $\pi(H) = \{hK : h \in H\} = \{hkK : h \in H, k \in K\} = HK/K$. We further observe that for an element to be in $\mathrm{Ker}(\pi|_H)$, it must be in the intersection of H and K, hence $\mathrm{Ker}(\pi|_H) = H \cap K$, and so $H \cap K \lhd G$. Lastly, The First Isomorphism Theorem then tells us that

$$\frac{H}{\mathrm{Ker}(\pi|_H)} = \frac{H}{H \cap K} \cong \frac{HK}{K}.$$

□

17. Sylow Theorem

Definition 17.1 (p-Sylow)**.** *Let G be a group, a p-Sylow subgroup $P \leq G$ is a p-group such that $|P|$ completely divides $|G|$, i.e. $|P| = p^k$ is the largest power of p dividing $|G|$.*

Before we continue, we quickly revisit the Correspondence Theorem (Theorem 4.1). Given a normal subgroup $K \lhd G$, there is a bijection between the sets

$$\{H \leq G : K \subset H \subset G\} \longleftrightarrow \{H \leq G/K\}.$$

The bijection can be given explicitly by $H \leftrightarrow H/K$. This observation then says that every subgroup of G/K is of the form H/K for a unique subgroup such that $K \leq H \leq G$. Similarly, this also says that $H \lhd G$ if and only if $H/K \lhd G/K$.

Lemma 17.2. *Let G be a finite group with $P \leq G$ a p-Sylow subgroup and let $H \leq N_G(P)$ be a p-group, then $H \subset P$.*

Proof. Let k be such that $|P| = p^k$. Now, since $H \leq N_G(P)$, then $H \lhd P$, which means that $HP = PH$ and so $HP \leq G$ by Lemma 16.29. The Second Isomorphism Theorem for $N_G(P)$ (with $P \lhd N_G(P)$ and $H \leq P$) tells us that $\frac{H}{H \cap P} \cong \frac{HP}{P}$. Suppose p divides HP/P, then Theorem 16.20 tells us there is an element $aP \in HP/P$ with order p. Since $\langle aP \rangle \leq HP/P$, then the Correspondence Theorem tells us that $S^* := \langle aP \rangle = S/P$ such that $P \leq S \leq HP$. It then follows that $|S^*| = |S|/|P|$, hence $|S| = |S^*| \cdot |P| = p^{k+1}$, but this contradicts the fact that P is a p-Sylow subgroup. It must then be the case that $p \nmid [HP : P]$. However, since $\frac{H}{H \cap P}$ is a p-group and $[H : H \cap P] = [HP : P]$, then $\frac{H}{H \cap P} = 1$, so $H = (H \cap P) \subset P$. □

Theorem 17.3 (Sylow Theorem)**.** *Let G be a finite group, let p be prime, and define $\mathcal{S}_p = \{p\text{-Sylow subgroups of } G\}$. Then, (1) G has a p-Sylow subgroup, i.e. $\mathcal{S}_p \neq \emptyset$; (2) All p-Sylow subgroups are conjugate, i.e. $\mathcal{S}_p$ is a transitive G-set; (3) for all $P \in \mathcal{S}_p$, then $n_p := |\mathcal{S}_p| = [G : N_G(P)]$; and (4) $n_p \equiv 1 \pmod{p}$.*

Proof. Let $|G| = p^k m$ such that $p \nmid m$, i.e. p^k completely divides $|G|$, and let G act on itself by conjugation. We then have

$$G = Z \sqcup \mathcal{O}_{x_1} \sqcup \cdots \sqcup \mathcal{O}_{x_s}$$

where Z is the union of singleton orbits and $\mathcal{O}_{x_i}$ denotes the non-singleton orbits of G.

Suppose $p \nmid |Z|$, then since p divides $|G|$ there must be some j such that $p \nmid |\mathcal{O}_{x_j}|$. Corollary 16.19 tells us that $|G| = |\mathcal{O}_{x_j}| \cdot |G_{x_j}|$, and so p^k divides $|G_{x_j}|$. Since p divides $|G_{x_j}|$ there is an element $q \in G_{x_j}$ with order p, and since $G_{x_j} = C_G(x_j)$ by our observations about G acting by conjugation, this means that $\langle q \rangle \lhd G_{x_j}$. By induction, we can therefore produce a subgroup $P \leq G_{x_j} \leq G$ such that $|P| = p^k$, hence P is a p-Sylow subgroup of G.

Suppose p divides $|Z|$, and since Z is the center of G, then by Cauchy, there is $z \in Z$ such that z has order p. It then follows that $P := \langle z \rangle \lhd Z$ since z is central, and so $|G/P| = p^{k-1}m$. By induction, there is $\overline{P} \leq G$ such that $\overline{P} = p^k$, and so $\overline{P}$ is a p-Sylow subgroup of G, hence (1) holds.

Now, let G act on $\mathcal{S}_p$ by conjugation, hence $G \times \mathcal{S}_p \to \mathcal{S}_p$ given by $(g, P) \mapsto g.P = gPg^{-1}$. Let $\mathcal{O}$ be a G-orbit in the decomposition of $\mathcal{S}_p$ and let $P \in \mathcal{O}$. Define a group action $P \times \mathcal{O} \to \mathcal{O}$ by $(p, A) \mapsto p.A = pAp^{-1}$. Clearly $\{P\}$ is a singleton P-orbit for this group action, we will show that it is the only one. Let $Q \in \mathcal{O}$ such that $\{Q\}$ is a singleton P-orbit, and so $P \in N_P(Q)$. Lemma 17.2 then says that $P \subset Q$, and since

they are both p-Sylow subgroups then they have the same cardinality, so $P = Q$, and $\{P\}$ is the only singleton P-orbit. Decomposing $\mathcal{O}$ into P-orbits, we have

$$\mathcal{O} = \{P\} \sqcup \mathcal{O}'_1 \sqcup \cdots \sqcup \mathcal{O}'_s$$

where p divides $|\mathcal{O}'_j|$ for all j, and so $|\mathcal{O}| \equiv 1 \pmod{p}$.

Now, let $P' \in \mathcal{S}_p - \mathcal{O}$ and define a group action $P' \times \mathcal{O} \to \mathcal{O}$ by conjugation and decompose $\mathcal{O}$ into P'-orbits. Let $\{Q\}$ be a singleton P'-orbit, and so by the same reasoning as in the previous paragraph, it follows that $P' \leq N_{P'}(Q)$, hence $P' = Q$; however, $P' \notin \mathcal{O}$ and $Q \in \mathcal{O}$, a contradiction. This means there are no singleton P'-orbits, hence $|\mathcal{O}| \equiv 0 \pmod{p}$, a contradiction. We therefore conclude that $\mathcal{S}_p - \mathcal{O} = \emptyset$, hence $\mathcal{S}_p$ is transitive and $n_p = |\mathcal{S}_p| = |\mathcal{O}| \equiv 1 \pmod{p}$, so (2) and (4) hold.

Lastly, recall that G_P, the stabilizer of $P \leq G$, for a group action defined by conjugation on subsets is given by $N_G(P)$. Corollary 16.19 then tells us that $|G| = |\mathcal{O}| \cdot |G_P| = |\mathcal{S}_p| \cdot |N_G(P)|$. It then immediately follows that $n_p = |\mathcal{S}_p| = [G : N_G(P)]$, and so (3) holds. □

Corollary 17.4. *Let G be a finite group such that p divides $|G|$. If $n_p = 1$, then $P \lhd G$ where P is p-Sylow.*

Proof. Since $n_p = 1$, then there is a unique p-Sylow subgroup of G, let P be this subgroup. Furthermore, since $1 = n_p = [G : N_G(P)] = |G|/|N_G(P)|$, then $|N_G(P)| = |G|$, hence $N_G(P) = G$ and so $P \lhd G$. □

Proposition 17.5. *There are no simple groups of order 12.*

Proof. Let G be a group such that $|G| = 12 = 2^2 \cdot 3$, and suppose that G is simple. Since 2 and 3 are the only prime divisors of $|G|$ and G is simple, then $n_2 \neq 1$ and $n_3 \neq 1$. Let P_2 and P_3 be 2- and 3-Sylow subgroups, respectively, hence $|P_2| = 4$ and $|P_3| = 3$. Furthermore, since $n_p = [G : N_G(P_p)] = |G|/|N_G(P_p)|$, then n_p divides $|G|$. This means that $n_2 = 3$ and $n_3 = 4$. Since there are four distinct 3-Sylow subgroups, then these groups contribute $(3-1) \times 4 = 8$ non-identity elements to G. Moreover, since $|P_2| = 4$, then $P_2 \cong \mathbb{Z}_4$ or $P_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. If $P_2 \cong \mathbb{Z}_4$, then the 2-Sylow subgroups contribute an additional $1 + (4-1) \times 3 = 10$ elements, but then $|G| = 18$, a contradiction. If $P_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then there are at least five distinct elements amongst the four 2-Sylow groups, hence $|G| \geq 13$. Since both cases lead to contradictions, we conclude that there are no simple groups of order 12. □

18. Solvable Groups

This is a very brief section that does not contain many deep results. I added this section simply as a potluck of definitions and simple lemmas regarding the basic theory of solvability.

Definition 18.1 (Commutator Subgroup)**.** *Let G be a group and let $[G, G]$ be the subgroup generated by all elements of the form $[a, b] := aba^{-1}b^{-1}$. This subgroup, as you might have guessed, is called the commutator subgroup of G.*

This definition yields some immediate trivial consequences. Namely, it is evident that $[a,b]=1$ if and only if a commutes with b. Furthermore, $[a,b]^{-1}=[b,a]$.

Definition 18.2 (Characteristic Subgroups)**.** *A subgroup $K\leq G$ is said to be characteristic if it is invariant under all automorphisms of G. This means that for $\varphi:G\to G$ an automorphism, $\varphi(K)=K$.*

In particular, if K is a characteristic subgroup of G, then K is normal, since normality follows from invariance via inner automorphisms.

Lemma 18.3. *The commutator subgroup $[G,G]$ is characteristic in G, hence $[G,G]\lhd G$.*

Proof. Let $\varphi:G\to G$ be an automorphism, and let $[a,b]$ be a generator of $[G,G]$. It then follows that $\varphi([a,b])=\varphi(aba^{-1}b^{-1})=\varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}=[\varphi(a),\varphi(b)]$, hence $\varphi([G,G])\subset[G,G]$. In the other direction, since φ is an automorphism, we identify $x,y\in G$ such that $\varphi(x)=a$ and $\varphi(y)=b$, hence $\varphi([x,y])=[a,b]$. It then follows that $\varphi([G,G])=[G,G]$, therefore $[G,G]$ is characteristic in G. □

Lemma 18.4. *A group G is abelian if and only if $[G,G]=1$.*

Proof. If G is abelian, then $ab=ba$, hence $[a,b]=1$ for all $a,b\in G$, so $[G,G]$ is generated by 1. On the other hand, suppose $[G,G]=1$ and let $a,b\in G$. Since $[a,b]$ is a generator of $[G,G]$, then $1=[a,b]=aba^{-1}b^{-1}$, hence $ab=ba$, therefore G is abelian. □

Definition 18.5 (Abelianization)**.** *The quotient $G/[G,G]$ is said to be the abelianization of G; it is denoted G_{ab}.*

Lemma 18.6. *If G is nonabelian and simple, then $[G,G]=G$, hence $G_{ab}=1$.*

Proof. Since $[G,G]\lhd G$ by Lemma 18.3 and G is simple, it must follow that $[G,G]=G$ or $[G,G]=1$; however, since G is nonabelian, then $[G,G]=G$. □

Definition 18.7 (Derived Subgroups)**.** *For $i\geq 0$, define $G^{(i)}$ inductively by $G^{(0)}=G$ and $G^{(i)}=[G^{(i-1)},G^{(i-1)}]$ for $i\geq 1$. We call $G^{(i)}$ the i-th derived subgroup of G, hence $G^{(1)}=[G,G]$, the commutator of G.*

Definition 18.8 (Solvable Groups)**.** *A group G is said to be solvable if $G^{(k)}=1$ for some $k\geq 0$.*

Lemma 18.9. *Every abelian group is solvable. Furthermore, simple groups are solvable if and only if they are abelian.*

Proof. Lemma 18.4 immediately implies that all abelian groups are solvable. If G is simple, then $[G,G]=G$ or $[G,G]=1$; however, since G is solvable, it must follow that $[G,G]=1$, hence G is abelian. □

19. Semidirect Products

We will motivate this section by considering the group of rigid motions in $\mathbb{R}^n$, which we now define.

Definition 19.1 (Rigid Motion)**.** *A rigid motion is any map $A : \mathbb{R}^n \to \mathbb{R}^n$ which preserves distances, i.e. for all $x, y \in \mathbb{R}^n$, dist$(Ax, Ay) =$ dist(x, y). We denote the set of these actions by $E(n)$; this set defines a group with composition as its group operation.*

Lemma 19.2. *Any origin preserving rigid motion is an orthogonal transformation, i.e. if $A \in E(n)$ such that $A(0) = 0$, then A is linear, hence $A \in O(n)$.*

Proof. Let A be one such rigid motion and note that in $\mathbb{R}^n$ with the Euclidean inner product, $||x||$, the norm of x, is given by $||x|| = \text{dist}(x, 0)$; furthermore, $\text{dist}(x, y) = \text{dist}(x - y, 0)$. It then follows that $||Ax|| = \text{dist}(Ax, 0) = \text{dist}(x, 0) = ||x||$, hence A preserves norms. Next, we observe that $||A(x - y)|| = ||x - y|| = \text{dist}(x - y, 0) = \text{dist}(x, y) = \text{dist}(Ax, Ay) = \text{dist}(Ax - Ay, 0) = ||Ax - Ay||$, and so A is "linear in norm". It then follows that

$$\langle Ax - Ay, Ax - Ay\rangle = ||Ax - Ay||^2 = ||A(x - y)||^2 = ||x - y||^2 = \langle x - y, x - y\rangle,$$

and so we

$$\langle Ax, Ax\rangle - 2\langle Ax, Ay\rangle + \langle Ay, Ay\rangle = \langle x, x\rangle - 2\langle x, y\rangle + \langle y, y\rangle.$$

Since $\langle Ax, Ax\rangle = ||Ax||^2 = ||x||^2 = \langle x, x\rangle$, then this implies that $\langle Ax, Ay\rangle = \langle x, y\rangle$, and so A preserves inner products.

Lastly, let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{R}^n$ and note that since A preserves inner products, then $\langle Ae_i, Ae_j\rangle = \langle e_i, e_j\rangle = \delta_{ij}$. This means that $\{Ae_1, \ldots, Ae_n\}$ forms a basis of A as well. Let $v, w \in \mathbb{R}^n$ and then

$$\begin{aligned} A(av + bw) &= \sum_{i=1}^{n} \langle A(av + bw), Ae_i\rangle Ae_i = \sum_{i=1}^{n} \langle av + bw, e_i\rangle Ae_i \\ &= a \cdot \sum_{i=1}^{n} \langle v, e_i\rangle Ae_i + b \cdot \sum_{j=1}^{n} \langle w, e_j\rangle Ae_j \\ &= a \cdot \sum_{i=1}^{n} \langle Av, Ae_i\rangle Ae_i + b \cdot \sum_{j=1}^{n} \langle Aw, Ae_j\rangle Ae_j \\ &= aAv + bAw, \end{aligned}$$

and so A is linear, hence A is an orthogonal transformation. □

Corollary 19.3. *Any $A \in E(n)$ can be written uniquely as $A = T_a \circ S$ for some $a \in \mathbb{R}^n$ and some $S \in O(n)$ where T_a is defined by $v \mapsto v + a$.*

Proof. Let $S = T_{-A(0)} \circ A$, hence $S(0) = 0$, and so $S \in O(n)$; it is easily seen that $T_{A(0)} \circ S = A$. Now, suppose there is some other $a' \in \mathbb{R}^n$ and $S' \in O(n)$ such that $T_{A(0)} \circ S = T_{a'} \circ S'$. It then follows that $S' \circ S^{-1} = T_{-a'} \circ T_{A(0)} = T_{-a'+A(0)}$. However, $(S' \circ S^{-1})(0) = 0$, and so $T_{-a'+A(0)}(0) = 0$, hence $A(0) = a'$. This means that $S' \circ S^{-1} = \text{id}$, so $S' = S$. □

The uniqueness criterion of the previous corollary immediately implies that there is a set bijection $E(n) \longleftrightarrow \mathbb{R}^n \times O(n)$ given by $T_a \circ S \longleftrightarrow (a, S)$.

Corollary 19.4. *Let $(a, S), (a', S') \in \mathbb{R}^n \times O(n)$, then $(a, S) \circ (a', S') = (a + S(a'), S \circ S')$.*

Proof. This is a straightforward calculation:

$$\begin{aligned}\big((a, S) \circ (a', S')\big)(v) &= (T_a \circ S \circ T_{a'} \circ S')(v) \\ &= (T_a \circ S \circ T_{a'})(S'(v)) \\ &= a + S(a' + S'(v)) \\ &= a + S(a') + (S \circ S')(v) \\ &= T_{a+S(a')} \circ (S \circ S')(v),\end{aligned}$$

and so $(a, S) \circ (a', S') = (a + S(a'), S \circ S')$. □

We stated on the outset that rigid motion would be the model for which we develop the concept of semidirect products, and so we now make some observations regarding these groups.

Denote the set of translations by $T = \{T_a \in E(n) : a \in \mathbb{R}\}$. It then follows that $T \lhd E(n)$, since for $A \in E(n)$ and $T_a \in T$, it is easily seen that $A \circ T_a \circ A^{-1} = T_{S(a)}$ where $A = T_{a'} \circ S$. Furthermore, $O(n)$ is clearly a subgroup of $E(n)$; the intersection of $O(n)$ and T is the identity; and $E(n) = T \cdot O(n)$.

Lemma 19.5. *Let G be any group, and let $K \lhd G$ and $H \leq G$ such that $HK = G$ and $H \cap K = 1$. Then $g \in G$ can be written uniquely as $g = kh$ for $k \in K$ and $h \in H$. Furthermore, there is a set bijection $G \longleftrightarrow K \times H$ given by $g \leftrightarrow (k, h)$, and the group operation in G is given by $(k, h) \cdot (k', h') = (k \cdot {}^h k', h \cdot h')$ where ${}^h k = hkh^{-1}$.*

Proof. Let $g \in G$, then since $G = HK$, there are $h \in H$ and $k \in K$ such that $g = hk$. Suppose there are $h_1 \in H$ and $k_1 \in K$ such that $h_1 k_1 = g = hk$, then $h^{-1}h_1 = kk_1^{-1} \in H \cap K = 1$. Therefore $h = h_1$ and $k = k_1$, hence uniqueness, and so the claimed set bijection immediately follows. We then observe that

$$(k, h) \cdot (k', h') = khk'h' = khk'(h^{-1}h)h' = k({}^h k')hh' = (k \cdot {}^h k', h \cdot h').$$

This follows based on the assumption that $K \lhd G$, hence ${}^h k \in K$. □

The key observation to make in the above lemma is that we end up defining the group operation in G in terms of an action by H on K. Namely, H acts on K by inner automorphism. Explicity, there is a group action $H \times K \to K$ given by $(h, k) \mapsto h.k = hkh^{-1}$; this group action yields a group homomorphism $\varphi : H \to \mathrm{Aut}(K) \subset S(K)$. We can then generalize this action by considering the group of automorphisms on K, instead of limiting ourselves to the inner automorphisms.

Definition 19.6 (Semidirect Product)**.** *Let K and H be groups and let $\alpha : H \to Aut(K)$ be an action of H on K by automorphism. Then the semidirect product of K and H is denoted by $K \rtimes_\alpha H$ such that $K \rtimes_\alpha H = K \times H$ as sets. Furthermore, multiplication in $K \rtimes_\alpha H$ is given by $(k, h) \cdot (k', h') = (k \cdot {}^h k, h \cdot h')$ where ${}^h k = (\alpha(h))(k')$.*

Proposition 19.7. *A semidirect product is a group.*

Proof. It is easy to show that $(1,1)$ is the identity of $K \rtimes_\alpha H$ for K and H groups and $\alpha : H \to \mathrm{Aut}(K)$.

Next, let $(k,h) \in K \rtimes_\alpha H$ and let $k' \in K$ be the unique element such that $k^{-1} = (\alpha(h))(k')$. Then, $(k,h)\cdot(k',h^{-1}) = (k \cdot {}^h k', hh^{-1}) = (k \cdot (\alpha(h))(k'), 1) = (kk^{-1}, 1) = (1,1)$. Now, let $\varphi = \alpha(h)$, and so $\varphi(k') = k^{-1}$, hence $\varphi^{-1}(k^{-1}) = k'$. This means that $(\varphi^{-1}(k))^{-1} = k'$, which implies that $(\alpha(h))^{-1}(k) = (k')^{-1}$. Furthermore, since $1 = \alpha(hh^{-1}) = \alpha(h) \circ \alpha(h^{-1})$, so $(\alpha(h))^{-1} = \alpha(h^{-1})$. We have that $(\alpha(h^{-1}))(k) = (k')^{-1}$. It then follows that $(k',h^{-1})\cdot(k,h) = (k'\cdot^{h^{-1}} k, hh^{-1}) = (k'\cdot(\alpha(h^{-1}))(k), 1) = (k'(k')^{-1}, 1) = (1,1)$, and so (k,h) has an inverse.

Lastly, associativity is left as an easy, yet tedious, exercise. □

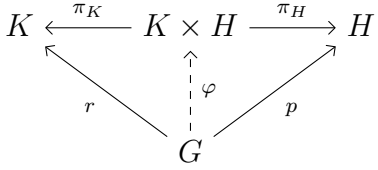
Corollary 19.8. *If $K \rtimes_\alpha H$ is a semidirect product and α is the trivial action, then $K \rtimes_\alpha H \cong K \times H$.*

Proof. To say that α is the trivial action is to say that α maps to the identity automorphism, hence $(\alpha(h))(k) = k$ for all $h \in H$ and all $k \in K$. We then observe that $(k,h)\cdot(k',h') = (k \cdot {}^h k', hh') = (k \cdot (\alpha(h))(k'), hh') = (kk', hh')$, therefore our conclusion follows. □

Before we continue, we quickly verify that the inclusion maps $K \hookrightarrow K \rtimes_\alpha H \hookleftarrow H$ are actually group homomorphisms; this will allow us to begin talking about exact sequences. It suffices to see that $(1,h)\cdot(1,h') = (1 \cdot {}^h 1, h \cdot h') = (1 \cdot (\alpha(h))(1), hh') = (1, hh')$, and $(k,1)\cdot(k',1) = (k \cdot {}^1 k', 1) = (k \cdot (\alpha(1))(k'), 1) = (kk', 1)$.

Lemma 19.9. *Let $1 \to K \xrightarrow{i} G \xrightarrow{p} H \to 1$ be an exact sequence of groups such that i has a retraction r, then $G \cong K \times H$.*

Proof. We will use the universal property of products to induce a map $\varphi : G \to K \times H$ such that the diagram



commutes, and show that φ is an isomorphism. Let $g \in \mathrm{Ker}(\varphi)$, hence $\varphi(g) = (1,1) = (r(g), p(g))$, so $r(g) = 1$ and $p(g) = 1$. This means that $g \in \mathrm{Ker}(p) = \mathrm{Im}(i)$, and so there is $k \in K$ such that $i(k) = g$. Since r is a retraction, then $1 = r(g) = ri(k) = k$, and since i is an injection, it follows that $g = 1$.

Next, let $(k,h) \in K \times H$ and since p is surjective, there is $x \in G$ such that $p(x) = h$. To determine the element which maps onto (k,h) we first note that $(k,1)\cdot(1,h) = (k,h)$ since we are dealing with direct products. This reduces our problem down to finding elements which map to $(k,1)$ and $(1,h)$. To find such elements, we will assume that such an element exists, deduce its form in terms of elements we already know a priori, then show that it in fact maps via φ as desired.

First, assume there is $g \in G$ such that $r(g) = k$ and $p(g) = 1$, hence $g \in \mathrm{Ker}(p) = \mathrm{Im}(i)$. This means there is $k' \in K$ such that $i(k') = g$, hence $k' = ri(k') = r(g) = k$. We then verify that $\varphi(i(k)) = \big(ri(k), pi(k)\big) = (k, 1)$.

Next, assume there is $g \in G$ such that $r(g) = 1$ and $p(g) = h$. Recall that there is $x \in G$ such that $p(x) = h$, then $p(g) = p(x)$, so $p(gx^{-1}) = 1$. This means that $gx^{-1} \in \mathrm{Ker}(p) = \mathrm{Im}(i)$, and so there is $k' \in K$ such that $i(k') = gx^{-1}$, hence $g = i(k') \cdot x$. Furthermore, we have $k' = ri(k') = r(g) \cdot r(x^{-1}) = r(x^{-1})$, and so $g = ir(x^{-1}) \cdot x$. We then verify that $\varphi(ir(x^{-1}) \cdot x) = \big(rir(x^{-1}) \cdot r(x), pir(x^{-1} \cdot p(x)\big) = \big(r(x^{-1}) \cdot r(x), p(x)\big) = (1, h)$.

Lastly, it then follows that $\varphi\big(i(k) \cdot ir(x^{-1}) \cdot x\big) = \varphi(i(k)) \cdot \varphi\big(ir(x^{-1}) \cdot x\big) = (k, 1) \cdot (1, h) = (k, h)$ and therefore φ is an isomorphism. □

Lemma 19.10. *Let $1 \to K \xrightarrow{i} G \xrightarrow{p} H \to 1$ be an exact sequence of groups such that p has a section s, then $G \cong K \rtimes_\alpha H$ where $\alpha : H \to Aut(K)$ is given by $\alpha(h)(k) = s(h) \cdot k \cdot s(h)^{-1}$.*

Proof. Our goal will be to use Lemma 19.5. Let $\overline{K} = \mathrm{Im}(i) = \mathrm{Ker}(p)$, hence $\overline{K} \lhd G$, and let $\overline{H} = \mathrm{Im}(s)$. Now, let $g \in \overline{K} \cap \overline{H}$, so $g \in \mathrm{Ker}(p) \cap \mathrm{Im}(s)$. This means that $p(g) = 1$ and there is $h \in H$ such that $s(h) = g$, so $h = ps(h) = p(g) = 1$, thus $g = s(1) = 1$, therefore $\overline{K} \cap \overline{H} = 1$. Next, let $g \in G$, and let $h = p(g)$. It then follows that $p(g \cdot s(h^{-1})) = p(g) \cdot ps(h^{-1}) = hh^{-1} = 1$, so $g \cdot s(h^{-1}) \in \mathrm{Ker}(p) = \mathrm{Im}(i)$. Then, there is $k \in K$ such that $i(k) = g \cdot s(h)^{-1}$, so $g = i(k)s(h)$, and it follows that $G = \overline{H} \cdot \overline{K}$. Applying the desired lemma, we have that $G \cong K \rtimes_\alpha H$ where $\alpha(\hat{h})(k) = {}^{\hat{h}}k = \hat{h}k\hat{h}^{-1}$. Since $\hat{h} \in \overline{H} = \mathrm{Im}(s)$, there is $h \in H$ such that $s(h) = \hat{h}$, so $\alpha(h)(k) = s(h) \cdot k \cdot s(h)^{-1}$, as desired. □

Example 19.11. *Dihedral groups are semidirect products.*

Solution. Recall that the dihedral group on n elements is denoted by $D_{2n} = \langle s, t : s^n = t^2 = 1, tst^{-1} = s^{-1} \rangle$. This means that $H = \langle t \rangle \cong \mathbb{Z}_2$ and $K = \langle s \rangle \cong \mathbb{Z}_n$, and the relation $tst^{-1} = s^{-1}$ implies that $K \lhd D_{2n}$. We then note that $H \cap K = 1$ and $D_{2n} = HK$, so we can immediately recognize D_{2n} as a semidirect product $K \rtimes_\alpha H$ given by some inner automorphism α, i.e. $\alpha(h)(k) = hkh^{-1}$. In particular, let's look at how α acts on the generators of D_{2n}; we have $\alpha(t)(s) = tst^{-1} = s^{-1}$. This means that $\alpha(t)$ is the automorphism on K which inverts elements, i.e. $s^k \mapsto s^{-k}$. Furthermore, we observe that

$$\mathrm{Aut}(K) = \mathrm{Aut}(\mathbb{Z}_n) = \mathrm{End}(\mathbb{Z}_n)^\times = \mathrm{Hom}_{\mathbb{Z}_n}(\mathbb{Z}_n, \mathbb{Z}_n)^\times \cong \mathbb{Z}_n^\times$$

as $\mathbb{Z}_n$-modules by Theorem 1.11. In particular, this means we can view α as a map $\mathbb{Z}_2 \to \mathbb{Z}_n^\times$ such that $\overline{1} \mapsto -\overline{1}$. □

Moving along, we consider a slight modification to Lemma 19.5.

Lemma 19.12. *Let G be a group with $K \lhd G$ and $H \lhd G$ such that $G = KH$ and $H \cap K = 1$, then $G \cong K \times H$.*

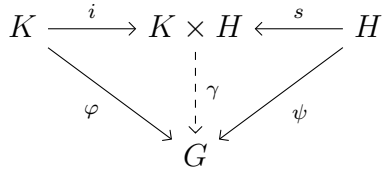
Proof. Define $\mu : K \times H \to G$ by $(k, h) \mapsto kh$, we must show that μ is a homomorphism. Let $h \in H$ and let $k \in K$, and observe that $hkh^{-1} \in K$ and $kh^{-1}k^{-1} \in H$ by normality of

H and K. It then follows that $(hkh^{-1})k \in K$ and $h(kh^{-1}k^{-1}) \in H$, hence $hkh^{-1}k^{-1} = 1$, so $hk = kh$. Then,

$$\mu\big((k,h)\cdot(k',h')\big) = \mu(kk',hh') = kk'hh' = khk'h' = \mu(k,h)\cdot\mu(k',h'),$$

and so μ is a homomorphism. Lastly, let $(k,h) \in \mathrm{Ker}(\mu)$, hence $1 = \mu(k,h) = kh$, and so $k = h^{-1} \in K \cap H = 1$, thus $k = h = 1$ and μ is injective. Let $g \in G$, and since $G = KH$, then $g = kh$ for some $k \in K$ and $h \in H$, and so $\mu(k,h) = kh = g$, therefore μ is an isomorphism. □

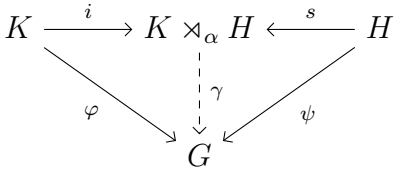
Proposition 19.13. *Let K and H be groups and let G be any group such that $\varphi : K \to G$ and $\psi : H \to G$ are group homomorphisms satisfying $\psi(h)\varphi(k) = \varphi(k)\psi(h)$. Then, there exists a unique induced map $\gamma : K \times H \to G$ such that the diagram*



commutes.

Proof. Define $\gamma : K \times H \to G$ by $(k,h) \mapsto \varphi(k)\psi(h)$. The fact that γ is a homomorphism, it makes the diagram commute, and is unique, are straightforward verifications. □

Proposition 19.14. *Let K and H be groups and let $\alpha : H \to Aut(K)$ be an action by automorphisms. Let G be any group and let $\varphi : K \to G$ and $\psi : H \to G$ be group homomorphisms such that $\psi(h)\varphi(k) = \varphi(\alpha(h)(k))\psi(h)$. Then, there exists a unique group homomorphism $\gamma : K \rtimes_\alpha H \to G$ such that the diagram*



commutes.

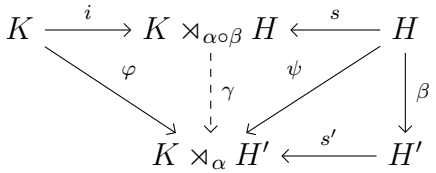
Proof. Define $\gamma : K \rtimes_\alpha H \to G$ by $(k,h) \mapsto \varphi(k)\psi(h)$. First, we verify that γ is a group homomorphism, and so

$$\begin{aligned}\gamma\big((k,h)\cdot(k',h')\big) &= \gamma\big(k\cdot\alpha(h)(k'),hh'\big) = \varphi(k)\varphi\big(\alpha(h)(k')\big)\psi(h)\psi(h') \\ &= \varphi(k)\psi(h)\varphi(k')\psi(h') = \gamma(k,h)\cdot\gamma(k',h')\end{aligned}$$

We then observe that $\gamma(i(k)) = \gamma(k,1) = \varphi(k)\psi(1) = \varphi(k)$ and $\gamma(s(h)) = \gamma(1,h) = \varphi(1)\psi(h) = \psi(h)$, hence $\gamma \circ i = \varphi$ and $\gamma \circ s = \psi$. Uniqueness is then an easy verification. □

Lemma 19.15. *Let $\beta : H \to H'$ be an isomorphism. Let $\alpha : H' \to Aut(K)$ be an action by automorphisms of H' on K. Then, H acts on K by automorphism via $\alpha \circ \beta : H \to Aut(K)$ and $K \rtimes_\alpha H' \cong K \rtimes_{\alpha\circ\beta} H$.*

Proof. Let $\varphi : K \to K \rtimes_\alpha H'$ and $s' : H' \to K \rtimes_\alpha H'$ be canonical inclusion maps, and define $\psi = s' \circ \beta$. Likewise, let $i : K \to K \rtimes_{\alpha\circ\beta} H$ and $s : H \to K \rtimes_{\alpha\circ\beta} H$ be canonical inclusions. We will show that φ and ψ satisfy the hypothesis of Proposition 19.14 and hence we induce a map γ such that the diagram



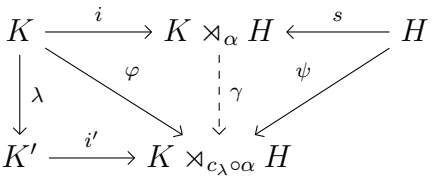
commutes. We then observe that

$$\psi(h)\varphi(k) = (1, \beta(h)) \cdot (k, 1) = \big((\alpha \circ \beta)(h)(k), \beta(h)\big) = \varphi\big((\alpha \circ \beta)(h)(k)\big)\psi(h),$$

and so there is a unique γ such that the above diagram commutes. Furthermore, γ is given by $(k, h) \mapsto \varphi(k)\psi(h) = (k, 1) \cdot (1, \beta(h)) = (k, \beta(h))$. This map is clearly injective, since $(k, \beta(h)) = (1, 1)$ implies that $k = 1$ and $\beta(h) = 1$, hence $h = 1$. Likewise, this map is clearly surjective, since for all $h' \in H'$ there is $h \in H$ such that $\beta(h) = h'$. It then follows that $\gamma(k, h) = (k, \beta(h)) = (k, h')$, therefore γ is an isomorphism. □

Proposition 19.16. *Let K and H be groups and $\alpha : H \to Aut(K)$ an action by automorphisms. Let $\lambda : K \to K'$ be an isomorphism. Then H acts on K' by automorphism and λ induces an isomorphism $c_\lambda : Aut(K) \to Aut(K')$ given by $\lambda \circ a \circ \lambda^{-1}$ for all $a \in Aut(K)$.*

Proof. This proof is similar to the proof in Lemma 19.15, with the following diagram:



□

The point of these two lemmas is to demonstrate that the structure of a semidirect product is unique up to isomorphism on both groups. We can replace the groups on which the semidirect product is constructed by groups which are isomorphic to the original and the semidirect product does not care. This observation affords us the convenience of working with groups which may be more computational tractable than our original group.

Example 19.17. *Determine all groups of order pq where p and q are both prime.*

Solution. Let G be a group such that $|G| = pq$ where $q < p$ and both are prime. Cauchy's Theorem tells us that there exist elements $h, k \in G$ such that $\text{ord}(k) = p$ and $\text{ord}(h) = q$. Define $K = \langle k \rangle \cong \mathbb{Z}_p$ and define $H = \langle h \rangle \cong \mathbb{Z}_q$. Since $[G : K] = |G|/|K| = pq/p = q$, the smallest prime dividing $|G|$, then $K \triangleleft G$ by Theorem 16.13. Furthermore, $H \cap K = 1$, since $\gcd(p, q) = 1$, and the Second Isomorphism Theorem tells us that $HK \leq G$ and $\frac{H}{H \cap K} \cong \frac{HK}{K}$. This means that $|G| = pq = |K| \cdot |H| = |HK| \cdot |H \cap K| = |HK|$, hence $G = HK$. It then follows that $G \cong K \rtimes H$, and the results from our previous two lemmas then say that $G \cong \mathbb{Z}_q \rtimes \text{Aut}(\mathbb{Z}_p)$. However, we further observe that $\text{Aut}(Z_p) \cong \mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$ and so $G \cong \mathbb{Z}_q \rtimes_\alpha \mathbb{Z}_p$ where $\alpha : \mathbb{Z}_q \to \mathbb{Z}_{p-1}$.

In order to classify all groups of order pq, we consider two separate cases. First, suppose $q \nmid (p-1)$ and suppose α is a nontrivial map, hence α must be injective since q is prime. However, Lagrange's Theorem then implies that q divides $p-1$, a contradiction; therefore α must be a trivial action, and so $G \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$ by Corollary 19.8 and Lemma 8.6.

Now, suppose q divides $p - 1$, and let α be a nontrivial map, hence injective. This means that $G \cong \mathbb{Z}_q \rtimes_\alpha \mathbb{Z}_p$... pretty anticlimactic, huh? Well, what about the action α? We've shown that the structure of a semidirect product does not change by replacing the groups that construct it with isomorphic copies; however, the action can (and in general does) alter the structure of the group. So how do we classify all groups of order pq?

First, we note that $\mathbb{Z}_{p-1}$ has a unique subgroup of order q, hence if α' is another nontrivial action (i.e. injection), then $\text{Im}(\alpha) = \text{Im}(\alpha')$. We can then define an isomorphism $\beta : \mathbb{Z}_q \to \mathbb{Z}_q$ given by $\beta = \alpha^{-1} \circ \alpha'$. It then follows that

$$\mathbb{Z}_p \rtimes_\alpha \mathbb{Z}_q \cong \mathbb{Z}_p \rtimes_{\alpha\circ\beta} \mathbb{Z}_q = \mathbb{Z}_p \rtimes_{\alpha'} \mathbb{Z}_q$$

since $\alpha \circ \beta = \alpha'$. This means that any nontrivial action we define will uniquely determine the semidirect product structure of G up to isomorphism. □

We can further generalize our result in the last paragraph by observing that as long as two actions α and α' are such that $\text{Im}(\alpha) \cong \text{Im}(\alpha')$, then the semidirect product cannot distinguish between them. In this way, we are allowed to choose an action which is most convenient.

Example 19.18 (Groups of order 12)**.** *Classify all groups of order 12.*

Proof. We showed in Proposition 17.5 that there are no simple groups of order 12, and so it follows that either $n_2 = 1$ or $n_3 = 1$. This means that $P_3 \cong \mathbb{Z}_3$ and either $P_2 \cong \mathbb{Z}_4$ or $P_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Suppose that $n_2 = 1$, hence $P_2 \triangleleft G$. Consider the short exact sequence

$$1 \to P_2 \to G \xrightarrow{\pi} G/P_2 \to 1.$$

Since $|G/P_2| = 3$, then $\pi|_{P_3} : P_3 \to G/P_2$ is an isomorphism, and so π has a section. Then, by Lemma 19.10 it follows that $G \cong P_2 \rtimes_\alpha P_3$ such that $\alpha : P_3 \to \text{Aut}(P_2)$.

Suppose $P_2 \cong \mathbb{Z}_4$, then $\text{Aut}(\mathbb{Z}_4) \cong (\mathbb{Z}_4)^\times = \{\pm 1\}$, and so α must be trivial, hence $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.

Now, suppose $P_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then it is clear that $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \text{GL}_2(\mathbb{F}_2) \cong S_3$ by Proposition 16.4. Our action can be viewed as $\alpha : \mathbb{Z}_3 \to S_3$, and so α is either trivial

or injective. If α is trivial, then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. If α is injective, then $\mathrm{Im}(\alpha)$ is the unique 3-Sylow subgroup of S_3. In fact, α must be given by $1 \mapsto (1\,2\,3)$ or by $1 \mapsto (1\,3\,2)$; however, both cases yield the same image in S_3, so it doesn't matter which mapping we choose. To make this isomorphism explicit, we fix $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$ which sends $(1,0)$ to $(0,1)$ to $(1,1)$ to $(1,0)$. Then, we have $G \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\alpha \mathbb{Z}_3$ where

$$\alpha : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \text{ given by } \overline{1} \to \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Now, suppose $n_3 = 1$ and so $P_3 \lhd G$, and consider the exact sequence

$$1 \to P_3 \to G \xrightarrow{\pi} G/P_3 \to 1.$$

Since $P_3 \cap P_2 = 1$, then $\pi|_{P_2} : P_2 \to G/P_3$ is an isomorphism, and so π has a section. As before, this means that $G \cong P_3 \rtimes_\alpha P_2$ where $\alpha : P_2 \to \mathrm{Aut}(P_3)$. Since $P_3 \cong \mathbb{Z}_3$, then $\mathrm{Aut}(P_3) \cong \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$, and so we have $\alpha : P_2 \to \mathbb{Z}_2 = \{\pm 1\}$.

Suppose $P_2 \cong \mathbb{Z}_4$. If α is trivial, then $G \cong \mathbb{Z}_{12}$; however, if α is nontrivial, then α must be given by $\overline{1} \mapsto -1$. This means that $G \cong \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4$ where $(s,t) \cdot (s',t') = (s + (-1)^t s', t + t')$.

Suppose $P_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then $G \cong \mathbb{Z}_3 \rtimes_\alpha (\mathbb{Z}_2 \times \mathbb{Z}_2)$ for some $\alpha : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2 = \{\pm 1\}$. If α is trivial, then $G \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Otherwise, if α is nontrivial, then all such maps have identical images, and so we fix an element $(1,0) \in \mathbb{Z}_2 \times \mathbb{Z}_2$. It then follows that $G \cong \mathbb{Z}_3 \rtimes_\alpha (\mathbb{Z}_2 \times \mathbb{Z}_2)$ where

$$(s,(t,u)) \cdot (s',(t',u')) = (s + (-1)^t s', (t + t', u + u')).$$

Therefore all groups of order 12 are of the form

$$\mathbb{Z}_{12}, \quad \mathbb{Z}_4 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \quad (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3, \quad \mathbb{Z}_3 \rtimes \mathbb{Z}_4, \quad \mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2).$$

□

20. Tensor Products

In this section we will need to distinguish between left R-modules and right R-modules. We will do so by adopting the following notation: M_R denotes a right R-module, i.e. the ring action occurs on the right, and ${}_R M$ denotes a left R-module, i.e. the ring action occurs on the left.

Definition 20.1 (Biadditive/R-Balanced)**.** *Let M_R and ${}_R N$ be modules and A a $\mathbb{Z}$-module. A function $\mu : M \times N \to A$ is biadditive if $\mu(m_1 + m_2, n) = \mu(m_1, n) + \mu(m_2, n)$ and $\mu(m, n_1 + n_2) = \mu(m, n_1) + \mu(m, n_2)$. Additionally, μ is said to be R-balanced if $\mu(m.r, n) = \mu(m, r.n)$.*

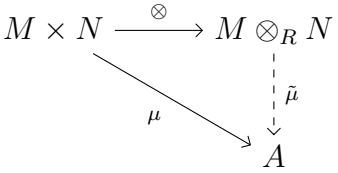
Our first goal will be to construct the tensor product as a universal biadditive, R-balanced map $\otimes : M \times N \to M \otimes N$ for modules M_R and ${}_R N$. To construct this map, we begin by letting $F(M \times N)$ denote the free $\mathbb{Z}$-module generated by $M \times N$. Define $e_{(m,n)} := \iota(m,n)$ and let J be the $\mathbb{Z}$-submodule of $F(M \times N)$ generated by all elements of the form

- $e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}$;
- $e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}$; and
- $e_{(m.r,n)} - e_{(m,r.n)}$

for all appropriately chosen elements. We then define $M \otimes_R N := F(M \times N)/J$ and let $\otimes = \pi \circ \iota$ where π is the canonical projection map determined by J.

We will now show that the tensor product has a universal mapping property for biadditive, R-balanced maps.

Lemma 20.2 (Universality of the Tensor Product)**.** *Let M_R and ${}_RN$ be modules and let $\otimes : M \times N \to M \otimes_R N$ be given as in the construction just provided. The tensor product has a universal mapping property: i.e., for all abelian groups A and all biadditive, R-balanced maps $\mu : M \times N \to A$, there is a unique map $\tilde{\mu} : M \otimes_R N \to A$ such that the diagram*



commutes.

Proof. Recall that Definition 3.1 induces a unique map $\overline{\mu} : F(M \times N) \to A$ such that $\mu = \overline{\mu} \circ \iota$. If we can show that $\overline{\mu}$ vanishes on the generators of J, then $\overline{\mu}$ vanishes on all of J, and so $J \leq \mathrm{Ker}(\overline{\mu})$. This would then induce a unique map $\tilde{\mu} : M \otimes_R N \to A$ such that $\overline{\mu} = \tilde{\mu} \circ \pi$ where π is the canonical projection determined by J.

We will only demonstrate $\overline{\mu}$ vanishing on one generator, as follows:

$$\begin{aligned} \overline{\mu}(e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}) &= \overline{\mu}(\iota(m_1+m_2,n)) - \overline{\mu}(\iota(m_1,n)) - \overline{\mu}(\iota(m_2,n)) \\ &= \mu(m_1+m_2,n) - \mu(m_1,n) - \mu(m_2,n) = 0, \end{aligned}$$

since μ is biadditive; the remaining verifications are just as straightforward. This means that $\mu = \overline{\mu} \circ \iota = \tilde{\mu} \circ \pi \circ \iota = \tilde{\mu} \circ \otimes$, and uniqueness is given. □

Definition 20.3 (Simple Tensor)**.** *The element $\otimes(m,n)$ is called a simple tensor and is denoted by $m \otimes n$.*

By the way that $M \otimes_R N$ and $\otimes$ were defined, it is easy to see that $\otimes$ is biadditive and R-balanced. After all, J was generated by elements which force these conditions. We then make the following observation

$$0 \otimes n = (0+0) \otimes n = 0 \otimes n + 0 \otimes n \quad \text{and} \quad m \otimes 0 = m \otimes (0+0) = m \otimes 0 + m \otimes 0,$$

and so $0 \otimes n = 0$ and $m \otimes 0 = 0$.

At this point it's appropriate to address two common problems encountered when dealing with tensor products.

First, it is generally very difficult to define a map out of a tensor product by virtue of the fact that we are dealing with a quotient group of a free module. In fact, an arbitrary

element of $M \otimes_R N$ need not be a simple tensor. Furthermore, to define such a map, one would need to show that the map is well-defined. Instead, it is usually best to determine some way to utilize the universal mapping properties of tensor products to induce a map out of a tensor product. In this way, we are guaranteed that the map is well-defined, and as a bonus, has many desired properties which would be otherwise troublesome to verify.

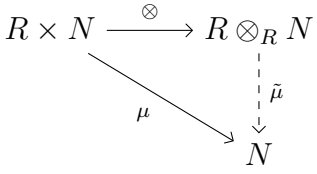
Second, although an arbitrary element is not necessarily a simple tensor, the tensor product is generated by simple tensors. This means that an arbitrary element of a tensor product is a finite sum of simple tensors, which may not necessarily be unique. In some circumstances it will be necessary to evaluate a map out of a tensor product; the fact that the simple tensors generate the tensor product implies that we will often need only perform such tasks on the simple tensors.

Proposition 20.4. *Let R be a ring and let R_N be a left R-module, then $R \otimes_R N \cong N$.*

Proof. We can define a biadditive R-balanced map $\mu : R \times N \to N$ given by $(r, n) \mapsto r.n$. This follows by observing that

$$\begin{gathered}\mu(r_1 + r_2, n) = (r_1 + r_2).n = r_1.n + r_2.n = \mu(r_1, n) + \mu(r_2, n); \\ \mu(r, n_1 + n_2) = r.(n_1 + n_2) = r.n_1 + r.n_2 = \mu(r, n_1) + \mu(r, n_2); \text{ and} \\ \mu(r_1 r_2, n) = (r_1 r_2).n = r_1.(r_2.n) = \mu(r_1, r_2.n).\end{gathered}$$

We then induce a map $\tilde{\mu} : R \otimes_N N \to N$ by the universal property of tensor products such that the diagram



commutes. The structure on a tensor product is, in general, far too complex to make a standard injectivity/surjectivity argument to prove that $\tilde{\mu}$ is an isomorphism. Instead, we will construct an inverse map. Define $\rho : N \to R \otimes_R N$ by $n \mapsto 1 \otimes n$. This is a homomorphism by the observation that $\rho(n_1 + n_2) = 1 \otimes (n_1 + n_2) = 1 \otimes n_1 + 1 \otimes n_2 = \rho(n_1) + \rho(n_2)$. Lastly, we have

$$(\rho \circ \tilde{\mu})(r \otimes n) = \rho\tilde{\mu} \otimes (r, n) = \rho\mu(r, n) = \rho(r.n) = 1 \otimes (r.n) = r \otimes n,$$

and

$$(\tilde{\mu} \circ \rho)(n) = \tilde{\mu}(1 \otimes n) = \mu(1, n) = 1.n = n,$$

therefore $\tilde{\mu}$ is an isomorphism. □

Proposition 20.5. *Let R be a ring with ideal $I \lhd R$, and let R_N be a left R-module. Then R/I is a right R-module, and $R/I \otimes_R N \cong N/IN$.*

Proof. Fix $n \in N$ and define $f_n : R \to N/IN$ by $f_n(r) = \overline{r.n}$. For $i \in I$, it follows that $f_n(i) = \overline{i.n} = 0$, and so $I \leq \mathrm{Ker}(f_n)$. The fundamental theorem on homomorphisms then induces a unique map $\overline{f_n} : R/I \to N/IN$ such that $f_n = \overline{f_n} \circ \pi$ where $\pi : R \to R/I$.

Now, define $\mu : R/I \times N \to N/IN$ by $(\overline{r}, n) \mapsto \overline{f_n}(\overline{r}) = f_n(r) = \overline{r.n}$. We now verify that μ is biadditive

$$\mu(\overline{r_1} + \overline{r_2}, n) = \overline{(r_1 + r_2).n} = \overline{r_1.n} + \overline{r_2.n} = \mu(\overline{r_1}, n) + \mu(\overline{r_2}, n)$$

and

$$\mu(\overline{r}, n_1 + n_2) = \overline{r.(n_1 + n_2)} = \overline{r.n_1} + \overline{r.n_2} = \mu(\overline{r}, n_1) + \mu(\overline{r}, n_2);$$

as well as R-balanced

$$\mu(\overline{r_1}.r_2, n) = \overline{(r_1 r_2).n} = \overline{r_1.(r_2.n)} = \mu(\overline{r_1}, r_2.n).$$

We then induce a unique map $\tilde{\mu} : R/I \otimes_R N \to N/IN$ such that the diagram

$$\begin{array}{ccc} R/I \times N & \xrightarrow{\otimes} & R/I \otimes_R N \\ & \searrow^{\mu} & \downarrow{\scriptstyle \tilde{\mu}} \\ & & N/IN \end{array}$$

commutes, and it is easily seen that $\tilde{\mu}(\overline{r} \otimes n) = \overline{r.n}$ on generators. Now, define $h : N \to R/I \otimes_R N$ by $n \mapsto \overline{1} \otimes n$. Clearly, h is a homomorphism, since $h(n_1 + n_2) = \overline{1} \otimes (n_1 + n_2) = \overline{1} \otimes n_1 + \overline{1} \otimes n_2 = h(n_1) + h(n_2)$. Then, for $i.n \in IN$, we observe that $h(i.n) = \overline{1} \otimes i.n = \overline{1}.i \otimes n = \overline{i} \otimes n = 0 \otimes n = 0$, so $IN \leq \mathrm{Ker}(h)$. We then induce a unique homomorphism $\overline{h} : N/IN \to R/I \otimes_R N$ such that $h = \overline{h} \circ \pi$ where $\pi : N \to N/IN$; we note that $\overline{h}(\overline{n}) = \overline{1} \otimes n$ by this relationship. Lastly, we verify that $\overline{h}$ is indeed an inverse to $\tilde{\mu}$. Observe that

$$(\overline{h} \circ \tilde{\mu})(\overline{r} \otimes n) = \overline{h}(\overline{r.n}) = \overline{1} \otimes r.n = \overline{1}.r \otimes n = \overline{r} \otimes n$$

and

$$(\tilde{\mu} \circ \overline{h})(\overline{n}) = \tilde{\mu}(\overline{1} \otimes n) = \overline{1.n} = \overline{n};$$

we therefore conclude that $\tilde{\mu}$ is an isomorphism. □

Corollary 20.6. *Let $d = \gcd(m, n)$, then $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \cong \mathbb{Z}_d$; in particular, if $d = 1$, then the tensor product is zero.*

Proof. This is a straightforward calculation:

$$\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \cong \frac{\mathbb{Z}/m\mathbb{Z}}{n\mathbb{Z}(\mathbb{Z}/m\mathbb{Z})} = \frac{\mathbb{Z}/m\mathbb{Z}}{(m\mathbb{Z} + n\mathbb{Z})/m\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z} + n\mathbb{Z}} = \mathbb{Z}_d.$$

If $\gcd(m, n) = d = 1$, then $\mathbb{Z}_d = 0$. □

Lemma 20.7. *Let R_M and ${}_RN$ be R-modules and let $g : N \to N'$ be a left R-module map. Then, there is a unique map $1 \otimes g : M \otimes_R N \to M \otimes'_R N'$ such that $(1 \otimes g) \circ \otimes = \otimes' \circ (1 \times g)$.*

Proof. The map $1 \times g : M \times N \to M \times N'$ is given by $(m, n) \mapsto (m, g(n))$. Then, $\otimes' \circ (1 \times g) : M \times N \to M \otimes'_R N$ is given by $(m, n) \mapsto m \otimes' g(n)$, which is clearly biadditive and R-balanced. This induces a unique map $1 \otimes g : M \otimes_R N \to M \otimes'_R N'$ such that the diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_R N \\ & \searrow^{\otimes' \circ (1 \times g)} & \downarrow{\scriptstyle 1 \otimes g} \\ & & M \otimes'_R N \end{array}$$

commutes. □

There is, of course, an analogous lemma for inducing a map $f \otimes 1$ from a right R-module map $f : M \to M'$. Likewise, given maps f and g, we can induce a map $f \otimes g : M \otimes_R N \to M' \otimes'_R N'$ such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Theorem 20.8 (Left Functoriality of the Tensor Product)**.** *Let R be a ring and let M be a right R-module. Let $\mathcal{L}$ be the category of left R-modules, and let $\mathcal{D}$ be the category of abelian groups, i.e $\mathbb{Z}$-modules. Define $M \otimes_R (\cdot) : \mathcal{L} \to \mathcal{D}$ by $N \mapsto M \otimes_R N$ on objects, and $g \mapsto 1 \otimes g$ on arrows. Then, $M \otimes_R (\cdot)$ is a functor.*

Proof. Let $g : N \to N'$ and $h : N' \to N''$ be left R-module maps, and consider the diagram:

$$\begin{array}{ccccc} M \times N & \xrightarrow{1 \times g} & M \times N' & \xrightarrow{1 \times h} & M \times N'' \\ \downarrow{\scriptstyle \otimes} & & \downarrow{\scriptstyle \otimes'} & & \downarrow{\scriptstyle \otimes''} \\ M \otimes_R N & \xrightarrow{1 \otimes g} & M \otimes'_R N' & \xrightarrow{1 \otimes' h} & M \otimes''_R N'' \end{array}.$$

We then consider the analogous diagram on $h \circ g$, and note that

$$\begin{aligned} (1 \otimes (h \circ g)) \circ \otimes &= \otimes'' \circ (1 \times (h \circ g)) = \otimes'' \circ (1 \times h) \circ (1 \times g) \\ &= (1 \otimes h) \circ \otimes' \circ (1 \times g) = (1 \otimes' h) \circ (1 \otimes g) \circ \otimes. \end{aligned}$$

Uniqueness of $1 \otimes (h \circ g)$ then implies that $1 \otimes (h \circ g) = (1 \otimes' h) \circ (1 \otimes g)$. Preservation of the identity map follows trivially, therefore $M \otimes_R (\cdot)$ is a functor. □

Theorem 20.9 (Right Functoriality of the Tensor Product)**.** *Let R be a ring and let N be a left R-module. Let $\mathcal{R}$ be the category of right R-modules and let $\mathcal{D}$ be the category of abelian groups. Define $(\cdot) \otimes_R N : \mathcal{R} \to \mathcal{D}$ by $M \mapsto M \otimes_R N$ on objects, and $g \mapsto g \otimes 1$ on arrows. Then, $(\cdot) \otimes_R N$ is a functor.*

Proof. Similar to Theorem 20.8. □

Definition 20.10. *Let S and R be rings. An S-R-bimodule is an abelian group M which is a left S-module and a right R-module, such that the two module actions are compatible, i.e. $(s.m).r = s.(m.r)$.*

Proposition 20.11. *Let M be an S-R-bimodule and let N be a left R-module. Then, $M \otimes_R N$ is a left S-module by $s.(m \otimes n) = (s.m) \otimes n$.*

Proof. Our goal will be to construct a ring map $\Phi : S \to \text{End}(M \otimes_R N)$, which by Theorem 1.3 will demonstrate that $M \otimes_R N$ is a left S-module. By virtue of M being a left S-module, we already have a ring map $\varphi : S \to \text{End}(M)$ given by $\varphi(s)(m) = s.m$; however, we can view $\text{End}(M)$ as the R-module endomorphisms of M (my notes aren't clear on this point, needs clarification). This means that for all $s \in S$, we have that $\varphi(s) : M \to M$ is a map of right R-modules. Functoriality of $(\cdot) \otimes_R N$ then induces a map $\varphi(s) \otimes 1 : M \otimes_R N \to M \otimes_R N$ which is given by $m \otimes n \mapsto \varphi(s)(m) \otimes n = (s.m) \otimes n$. Define $\Phi : S \to \text{End}(M \otimes_R N)$ by $s \to \varphi(s) \otimes 1$. We must verify that this, in fact, defines a ring homomorphism. It then follows that

$$\Phi(s_1 + s_2) = \varphi(s_1 + s_2) \otimes 1 = \varphi(s_1) \otimes 1 + \varphi(s_2) \otimes 1 = \Phi(s_1) + \Phi(s_2),$$

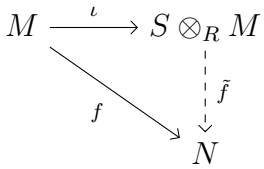
and

$$\Phi(s_1 s_2) = \varphi(s_1 s_2) \otimes 1 = (\varphi(s_1) \circ \varphi(s_2)) \otimes 1 = (\varphi(s_1) \otimes 1) \circ (\varphi(s_2) \otimes 1) = \Phi(s_1) \circ \Phi(s_2).$$

Lastly, we verify that $\Phi(1) = \varphi(1) \otimes 1 = 1 \otimes 1 = 1$, and so Φ is a ring map, hence $M \otimes_R N$ is a left S-module. □

Definition 20.12 (Pullback Functor)**.** *Let R and S be rings and let $\varphi : R \to S$ be a ring map. Let $\mathcal{S}$ be the category of left S-modules and let $\mathcal{R}$ be the category of left R-modules. Define the pullback functor $\mathcal{U} : \mathcal{S} \to \mathcal{R}$ on objects by pullback (Lemma 5.10) and identity on arrows.*

Theorem 20.13 (Extension of Scalars)**.** *Let S and R be rings and let $\varphi : R \to S$ be a ring map, and let M be a left R-module. Then, $\iota : M \to S \otimes_R M$ given by $m \mapsto 1 \otimes m$ is universal: i.e., for all left S-modules N and for all R-module map $f : M \to N$ where N is viewed as an R-module by pullback, there is a unique S-module map $\tilde{f} : S \otimes_R M \to N$ such that the diagram*



commutes. In other words, there is a natural bijection

$$Hom_{\mathcal{R}}(M, \mathcal{U}(N)) \longleftrightarrow Hom_{\mathcal{S}}(S \otimes_R M, N),$$

i.e., $S \otimes_R (\cdot)$ is left adjoint to $\mathcal{U}$.

Proof. Define $\mu : S \times M \to N$ by $(s, m) \mapsto s.f(m)$, we will show that μ is biadditive and S-balanced. We then have $\mu(s_1 + s_2, m) = (s_1 + s_2).f(m) = s_1.f(m) + s_2.f(m) = \mu(s_1, m) + \mu(s_2, m)$, and $\mu(s, m_1 + m_2) = s.f(m_1 + m_2) = s.(f(m_1) + f(m_2)) = s.f(m_1) + s.f(m_2) = \mu(s, m_1) + \mu(s, m_2)$, so μ is biadditive. Furthermore,

$$\mu(s.\varphi(r), m) = (s.\varphi(r)).f(m) = s.(\varphi(r).f(m)) = s.f(\varphi(r).m) = \mu(s, \varphi(r).m),$$

so μ is S-balanced. Then, by Lemma 20.2 there is a unique map $\tilde{\mu} : S \otimes_R M \to N$ such that $\mu = \tilde{\mu} \circ \otimes$. It then follows that $(\tilde{\mu} \circ \iota)(m) = \tilde{\mu}(1 \otimes m) = \mu(1, m) = 1.f(m) = f(m)$,

hence $\tilde{\mu} \circ \iota = f$. Now, suppose there is a function $\tilde{f} : S \otimes_R M \to N$ such that $\tilde{f} \circ \iota = f = \tilde{\mu} \circ \iota$. Then,

$$\tilde{\mu}(s \otimes m) = \mu(s, m) = s.f(m) = f(s.m) = \tilde{f}(\iota(s.m)) = \tilde{f}(1 \otimes (s.m)) = \tilde{f}(s \otimes m),$$

and so $\tilde{\mu}$ and $\tilde{f}$ agree on generators, therefore $\tilde{\mu}$ is unique. □

Example 20.14. *We will prove the result from Proposition 20.4 using Theorem 20.13. The identity $id : R \to R$ induces an R-module map $\tilde{id} : R \otimes_R N \to N$ such that $id = \tilde{id} \circ \iota$. Then, $(\iota \circ \tilde{id})(r \otimes n) = \iota(r.n) = 1 \otimes (r.n) = r \otimes n$, hence $R \otimes_R N \cong N$.*

This result tells us that extending scalars from a ring R to itself does not fundamentally change the module structure of an R-module.

Example 20.15. *Let R be a ring and let $I \lhd R$ be an ideal, then there is a ring map $\varphi : R \to R/I$. Let M be a left R-module, and let $\pi : M \to M/IM$ be the canonical projection. Then Theorem 20.13 induces a unique map $\tilde{\pi} : R/I \otimes_R M \to M/IM$. We then define a map $\psi : M/IM \to R/I \otimes_R M$ by $\overline{m} \mapsto \overline{1} \otimes m$ which is inverse to $\tilde{\pi}$. It then follows that $R/I \otimes_R M \cong M/IM$ as demonstrated in Proposition 20.5.*

Proposition 20.16. *Let R be a commutative ring, let $S \subset R$ be a multiplicatively closed set, and let $\varphi : R \to S^{-1}R$ be the ring of fractions map from Definition 5.2. Let M be a left R-module, then $S^{-1}R \otimes_R M \cong S^{-1}M$.*

Proof. Let $i : M \to S^{-1}M$ be the inclusion given by Theorem 5.12, then Theorem 20.13 induces a unique map $\tilde{i} : S^{-1}R \otimes_R M \to S^{-1}M$ such that $i = \tilde{i} \circ \iota$ where $\iota : M \to S^{-1}R \otimes_R M$ is given by $m \mapsto \overline{1} \otimes m$. Define $\psi : S^{-1}M \to S^{-1}R \otimes_R M$ by $\frac{m}{s} \mapsto \frac{1}{s} \otimes m$, which is clearly an R-module map. Then,

$$(\psi \circ \tilde{i}) \left(\frac{r}{s} \otimes m \right) = \psi \left(\frac{r}{s} . \tilde{i}(1 \otimes m) \right) = \psi \left(\frac{r}{s} . i(m) \right) = \psi \left(\frac{r.m}{s} \right) = \frac{1}{s} \otimes (r.m) = \frac{r}{s} \otimes m,$$

and

$$(\tilde{i} \circ \psi) \left(\frac{m}{s} \right) = \tilde{i} \left(\frac{1}{s} \otimes m \right) = \frac{1}{s} . \tilde{i}(1 \otimes m) = \frac{1}{s} . i(m) = \frac{m}{s}.$$

Therefore, $\tilde{i}$ is an isomorphism. □

Theorem 20.17 (Tensor Product and Coproducts)**.** *Let M be a right R-module and let $\{N_\alpha\}_\alpha$ be a collection of left R-modules. Then, $M \otimes_R (\coprod_\alpha N_\alpha) \cong \coprod_\alpha (M \otimes_R N_\alpha)$.*

Proof. For each α, the inclusion $\iota_\alpha : N_\alpha \to \coprod_\alpha N_\alpha$ induces a unique map

$$1 \otimes \iota_\alpha : M \otimes_R N_\alpha \to M \otimes_R \left(\coprod_\alpha N_\alpha \right)$$

by Lemma 20.7. By Definition 1.15, the collection $\{1 \otimes \iota_\alpha\}_\alpha$ induce a unique map

$$\Psi : \coprod_\alpha (M \otimes_R N_\alpha) \to M \otimes_R \left(\coprod_\alpha N_\alpha \right)$$

such that $1 \otimes \iota_\alpha = \Psi \circ f_\alpha$ for all α where $f_\alpha : M \otimes_R N_\alpha \to \coprod_\alpha (M \otimes_R N_\alpha)$ is the inclusion map. Define $\omega : M \times (\coprod_\alpha N_\alpha) \to \coprod_\alpha (M \otimes_R N_\alpha)$ by $(m, (n_\alpha)_\alpha) \mapsto (m \otimes n_\alpha)_\alpha$, which is clearly biadditive and R-balanced. We then induce a unique map

$$\Phi : M \otimes \left(\coprod_\alpha N_\alpha \right) \to \coprod_\alpha (M \otimes_R N_\alpha)$$

by Lemma 20.2 such that $\omega = \Phi \circ \otimes$. All that remains to show is that $\Phi\Psi = 1$ and $\Psi\Phi = 1$:

$$\begin{aligned} \Phi\Psi(m_\alpha \otimes n_\alpha)_\alpha &= \Phi\Psi(f_\alpha(m_\alpha \otimes n_\alpha))_\alpha = \Phi((1 \otimes \iota_\alpha)(m_\alpha \otimes n_\alpha))_\alpha = \Phi(m_\alpha \otimes \iota_\alpha(n_\alpha)_\alpha) \\ &= \omega(m_\alpha, (n_\alpha)_\alpha) = (m_\alpha \otimes n_\alpha)_\alpha, \end{aligned}$$

and

$$\begin{aligned} \Psi\Phi(m \otimes (n_\alpha)_\alpha) &= \Psi\omega(m, (n_\alpha)_\alpha) = \Psi(m \otimes n_\alpha)_\alpha = (\Psi f_\alpha(m \otimes n_\alpha))_\alpha \\ &= (1 \otimes \iota_\alpha)(m \otimes n_\alpha)_\alpha = (m \otimes \iota_\alpha(n_\alpha))_\alpha = m \otimes (n_\alpha)_\alpha. \end{aligned}$$

Therefore, $\coprod_\alpha (M \otimes_R N_\alpha) \cong M \otimes_R (\coprod_\alpha N_\alpha)$. □

The analogous theorem for arbitrary products will not be true in general. However, for finite families of modules, it will be true, since in this instance coproducts and products coincide, as discussed after Example 1.19.

Corollary 20.18 (Extension of Scalars for Free Modules)**.** *Let $\varphi : R \to S$ be a ring map. If F is a free R-module on $\{e_\alpha\}_\alpha$, then $S \otimes_R F$ is a free S-module on $\{1 \otimes e_\alpha\}_\alpha$.*

Proof. Since F is a free R-module, then $F \cong \coprod_\alpha R$ by Theorem 3.2. Then,

$$S \otimes_R F \cong S \otimes \left(\coprod_\alpha R \right) \cong \coprod_\alpha (S \otimes_R R) \cong \coprod_\alpha S,$$

hence $S \otimes_R F$ is a free S-module. It then follows that $1 \otimes (e_\alpha)_\alpha \mapsto (1 \otimes e_\alpha)_\alpha$ isomorphically, therefore $S \otimes_R F$ is generated by $\{1 \otimes e_\alpha\}_\alpha$. □

Example 20.19. *Let $\mathbb{C}/\mathbb{R}$ be a field extension and let $\varphi : \mathbb{R} \to \mathbb{C}$ be a ring map by inclusion. Let V be a finite-dimensional $\mathbb{R}$-vector space, and let $n = \dim(V)$, hence V is a free $\mathbb{R}$-module. In particular, $V \cong \coprod_{i=1}^n \mathbb{R}$, which we denote by $V \cong \mathbb{R}^n$. Then, it follows by Corollary 20.18 that*

$$\mathbb{C} \otimes_{\mathbb{R}} V \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n.$$

Corollary 20.20. *Let R be a commutative ring. If M is a free R-module on a basis $\{e_\alpha\}_\alpha$ and N is a free R-module on a basis $\{e'_\beta\}_\beta$, then $M \otimes_R N$ is free with basis $\{e_\alpha \otimes e'_\beta\}_{\alpha,\beta}$.*

Proof. Observe that

$$M \otimes_R N \cong \left(\coprod_\alpha R \right) \otimes \left(\coprod_\beta R \right) \cong \coprod_\beta \left(\left(\coprod_\alpha R \right) \otimes_R R \right) \cong \coprod_\beta \coprod_\alpha R,$$

and so $(e_\alpha)_\alpha \otimes (e'_\beta)_\beta \mapsto ((e_\alpha)_\alpha \otimes e'_\beta)_\beta \mapsto (e_\alpha \otimes e'_\beta)_{\alpha,\beta}$ isomorphically. Therefore $M \otimes_R N$ is a free R-module with the desired basis. □

Lastly, we state one last theorem regarding tensor products, without proof.

Theorem 20.21 (Associativity of Tensor Products)**.** *Let R and S be rings. Let M be a right R-module, let N be an R-S-bimodule, and let P be a left S-module. Then,*

$$M \otimes_R (N \otimes_S P) \cong (M \otimes_R N) \otimes_S P.$$

21. Even More Linear Algebra!!

Now that we've developed the theory behind tensor products, it is time to take a look back at Linear Algebra from a more sophisticated point of view.

Definition 21.1 (Natural Transformation)**.** *Let $\mathcal{C}$ and $\mathcal{D}$ be categories, and let $\mathcal{F}$ and $\mathcal{G}$ be functors $\mathcal{C} \to \mathcal{D}$. A natural transformation is a map $\tau : \mathcal{C} \to \mathcal{D}$ consisting of a collection of $\mathcal{D}$-morphisms $\{\tau_X : \mathcal{F}(X) \to \mathcal{G}(X)\}_{X \in Ob(\mathcal{C})}$ such that for all $f \in Hom_{\mathcal{C}}(X, Y)$, the following diagram*

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\tau_X} & \mathcal{G}(X) \\ {\scriptstyle \mathcal{F}(f)}\downarrow & & \downarrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(Y) & \xrightarrow{\tau_Y} & \mathcal{G}(Y) \end{array}$$

commutes. In addition, we say that τ is a natural isomorphism if each τ_X is a $\mathcal{D}$-isomorphism.

In order to show that something is a natural isomorphism, it suffices to choose an arbitrary object $X \in \mathrm{Ob}(\mathcal{C})$ and show that τ_X is an isomorphism in the the category $\mathcal{D}$. This will be our approach in the following theorem.

Proposition 21.2. *Let k be a field and let V and W be finite-dimensional k-vector spaces. Then there is a natural isomorphism $V^* \otimes_k W \longleftrightarrow Hom_k(V, W)$ given by $\varphi \otimes w \mapsto (v \mapsto \varphi(v)w)$.*

Proof. In lieu of Definition 21.1, we let $\mathcal{C}$ be the category of finite-dimensional k-vector spaces with linear transformations as their morphisms; let $\mathcal{D}$ be the category of abelian groups with homomorphisms as their morphisms; let $\mathcal{F}$ be the functor $V^* \otimes_k (\cdot)$; and let $\mathcal{G}$ be the functor $\mathrm{Hom}_k(V, \cdot)$. We will fix $W \in \mathrm{Ob}(\mathcal{C})$ and show that τ_W is an isomorphism in the category of abelian groups as given by the statement of the Proposition, and conclude that τ is a natural isomorphism.

Let $\varphi \in V^*$ and let $w \in W$, and define $\psi_{\varphi,w} : V \to W$ by $v \mapsto \varphi(v)w$, which is clearly a linear transformation. Define $\mu : V^* \times W \to \mathrm{Hom}_k(V, W)$ by $(\varphi, w) \mapsto \psi_{\varphi,w}$, which is also verified to be biadditive and k-balanced. This induces a map $\tilde{\mu} : V^* \otimes_k W \to \mathrm{Hom}_k(V, W)$ such that $\mu = \tilde{\mu} \circ \otimes$, which we intend to show is an isomorphism.

Recall that Theorem 1.22 tells us that there is an isomorphism between $\mathrm{Hom}_k(V, W)$ and $M_{m \times n}(k)$ where $n = \dim(V)$, $m = \dim(W)$, and $M_{m \times n}(k)$ is the abelian group (under addition) of $m \times n$ matrices over k. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be the basis of V and let $\mathcal{C} = \{w_1, \ldots, w_m\}$ be the basis of W. Similarly, let $\mathcal{B}^* = \{v^1, \ldots, v^n\}$ be the dual basis of V^*. Corollary 20.20 then provides us with a basis $\{v^j \otimes w_i\}_{ij}$ for $V^* \otimes_k W$.

Let E^{ij} denote the matrix consisting entirely of zeros, except for a one at position (i,j), then it is clear that $\{E^{ij}\}_{ij}$ is a basis for $M_{m\times n}(k)$. Note that $\tilde{\mu}(v^j \otimes w_i)(v_r) = \mu(v^j, w_i)(v_r) = v^j(v_r)w_i = \delta_{jr}w_i$. It then follows that

$$[\tilde{\mu}(v^j \otimes w_i)]_{\mathcal{C}}^{\mathcal{B}} = [T(v_1) \cdots T(v_r) \cdots T(v_n)] = E^{ij},$$

and so $\tilde{\mu}$ maps the basis of $V^* \otimes_k W$ to the basis of $M_{m\times n}(k)$. Therefore $\tilde{\mu}$ is an isomorphism, and we're done. □

Definition 21.3 (Trace of a Matrix)**.** *Let $A \in M_{n\times n}(k)$ for some field k such that $A = [a_{ij}]_{ij}$ for coefficients $a_{ij} \in k$, then the trace of A is denoted trace$(A) = \sum_i a_{ii}$, i.e. the sum of the terms along the diagonal of A.*

Corollary 21.4 (Trace Invariance)**.** *Let V be a finite-dimensional k-vector space and let $T : V \to V$ be a linear transformation. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_n\}$ be bases for V, and let $\mathcal{B}^*$ and $\mathcal{C}^*$ be corresponding dual bases for V^*. Denote $B = [T]_{\mathcal{B}}^{\mathcal{B}}$ and $C = [T]_{\mathcal{C}}^{\mathcal{C}}$, then trace$(B)$ = trace(C), i.e. trace is independent of choice of basis.*

Proof. Denote $B = [b_{ij}]_{ij}$ and $C = [c_{ij}]_{ij}$ and so

$$T = \sum_{ij} b_{ij}E_{\mathcal{B}}^{ij} = \sum_{ij} c_{ij}E_{\mathcal{C}}^{ij},$$

where E^{ij} is defined in Proposition 21.2 with respect to their respective bases. The natural isomorphism from Proposition 21.2 maps $v^j \otimes v_i \leftrightarrow E_{\mathcal{B}}^{ij}$ and $w^j \otimes w_i \leftrightarrow E_{\mathcal{C}}^{ij}$. Now, define $\eta : V^* \otimes_k V \to k$ on generators by $\varphi \otimes v \to \varphi(v)$, and so

$$E_{\mathcal{B}}^{ij} \longmapsto v^j \otimes v_i \overset{\eta}{\longmapsto} v^j(v_i) = \delta_{ij} \quad \text{and} \quad E_{\mathcal{C}}^{ij} \longmapsto w^j \otimes w_i \overset{\eta}{\longmapsto} w^j(w_i) = \delta_{ij}.$$

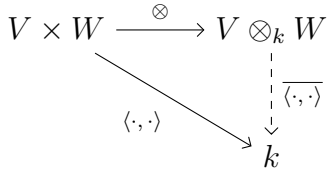
It then follows that

$$T \mapsto \sum_{i,j} b_{ij}E_{\mathcal{B}}^{ij} \mapsto \sum_{i,j} b_{ij}\delta_{ij} = \sum_i b_{ii} = \text{trace}(B),$$

and likewise for trace(C), hence trace(B) = trace(C). □

Definition 21.5 (Trace of a Linear Transformation)**.** *Let V be a finite-dimensional k-vector space and let $T : V \to V$, by Corollary 21.4, we then define the trace of T by trace(T) = trace(A) where A is a representing matrix of T for any basis $\mathcal{B}$ of V.*

Definition 21.6 (Tensor Product Duality)**.** *Let V and W be finite-dimensional k-vector spaces and let $\langle\cdot,\cdot\rangle : V \times W \to k$ be a bilinear form. Since $\langle\cdot,\cdot\rangle$ is biadditive and k-balanced, then it induces a map by Proposition 20.2 such that the diagram*



commutes. We then define $(V \otimes_k W)^* = Hom_k(V \otimes_k W, k)$.

Proposition 21.7 (Tensor Duality)**.** *Let V and W be finite-dimensional k-vector spaces, then*

$$(V \otimes_k W)^* \cong V^* \otimes_k W^*.$$

Proof. Proposition 20.4 yields an isomorphism $\mu : k \otimes_k k \to k$ given by $x \otimes y \mapsto xy$ on generators. Now, let $\varphi \in V^*$ and $\psi \in W^*$, hence $\varphi : V \to k$ and $\psi : W \to k$. We can then induce a map $\varphi \otimes \psi : V \otimes_k W \to k \otimes_k k$ given by $v \otimes w \mapsto \varphi(v) \otimes \psi(w)$ by Lemma 20.7. Define a map $\varphi \underline{\otimes} \psi = \mu \circ (\varphi \otimes \psi) : V \otimes_k W \to k$, hence $\varphi \underline{\otimes} \psi \in (V \otimes_k W)^*$, and the diagram

$$\begin{array}{ccc} V \otimes_k W & \xrightarrow{\varphi \otimes \psi} & k \otimes_k k \\ & \searrow^{\varphi \underline{\otimes} \psi} & \downarrow \mu \\ & & k \end{array}$$

commutes, i.e. $(\varphi \underline{\otimes} \psi)(v \otimes w) = \mu(\varphi(v) \otimes \psi(w)) = \varphi(v)\psi(w)$. Now, define $\tau : V^* \otimes_k W^* \to (V \otimes_k W)^*$ on generators by $\varphi \otimes \psi \mapsto \varphi \underline{\otimes} \psi$.

Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of V and let $\mathcal{C} = \{w_1, \ldots, w_m\}$ be a basis of W, and $\mathcal{B}^*$ and $\mathcal{C}^*$ be the associated dual bases for V^* and W^*, respectively. By Corollary 20.20, it follows that $\{v_i \otimes w_j\}_{ij}$ is a basis for $V \otimes_k W$ and $\{v^i \otimes w^j\}_{ij}$ is a k-basis for $V^* \otimes_k W^*$. Let $\{e^{pr}\}_{pr}$ be the dual basis of $(V \otimes_k W)^*$ such that $e^{pr}(v_i \otimes w_j) = \delta_{pi}\delta_{rj}$. It then follows by Lemma 12.3 that

$$\begin{aligned} \tau(v^i \otimes w^j) &= \sum_{p,r} \tau(v^i \otimes w^j)(v_p \otimes w_r) e^{pr} = \sum_{p,r} (v^i \underline{\otimes} w^j)(v_p \otimes w_r) e^{pr} \\ &= \sum_{p,r} v^i(v_p) w^j(w_r) e^{pr} = \sum_{p,r} \delta_{ip}\delta_{jr} e^{pr} = e^{ij}. \end{aligned}$$

This means that τ maps basis elements of $V^* \otimes_k W^*$ to basis elements of $(V \otimes_k W)^*$, and is therefore an isomorphism. □

Lemma 21.8. *Let M be a left R-module and let A be an abelian group, i.e. a $\mathbb{Z}$-module. Then, $Hom_{\mathbb{Z}}(A, M)$ is a left R-module and $Hom_{\mathbb{Z}}(M, A)$ is a right R-module.*

Proof. Let $f \in \mathrm{Hom}_{\mathbb{Z}}(A, M)$, let $r \in R$, and define $(r.f) \in \mathrm{Hom}_{\mathbb{Z}}(A, M)$ by $(r.f)(a) = r.f(a)$. Since M is a left R-module, then we have a map $\varphi : R \to \mathrm{End}_{\mathbb{Z}}(M)$ given by $r \mapsto (m \mapsto r.m)$. Define $\Phi : R \to \mathrm{End}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(A, M))$ by $r \mapsto (f \mapsto \varphi(r) \circ f) = \varphi(r)_*$, which is clearly a ring map, hence $\mathrm{Hom}_{\mathbb{Z}}(A, M)$ is a left R-module.

Now, let $f \in \mathrm{Hom}_{\mathbb{Z}}(M, A)$, let $r \in R$, and define $f.r \in \mathrm{Hom}_{\mathbb{Z}}(M, A)$ by $(f.r)(m) = f(r.m)$. We then define $\Phi : R \to \mathrm{End}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M, A))$ by $r \mapsto (f \mapsto f \circ \varphi(r)) = \varphi(r)^*$, hence $\mathrm{Hom}_{\mathbb{Z}}(M, A)$ is a right R-module. □

Theorem 21.9 (Adjoint Isomorphism)**.** *Let R and S be rings, let M be a left R-module, let N be an S-R-bimodule, and let P be a left S-module. Then, $M \otimes_R N$ is a left S-module by Proposition 20.11, and so*

$$Hom_S(N \otimes_R M, P) \cong Hom_R(M, Hom_S(N, P)).$$

Proof. Let $m \in M$, let $f \in \mathrm{Hom}_S(M \otimes_R N, P)$, and define $\varphi_{f,m} : N \to P$ by $n \mapsto f(n \otimes m)$, which is clearly a homomorphism. Furthermore, $\varphi_{f,m}(s.n) = f((s.n) \otimes m) f(s.(n \otimes m)) = s.f(n \otimes m) = s.\varphi_{f,m}(n)$, hence $\varphi_{f,m} \in \mathrm{Hom}_S(N, P)$.

Now, define $\varphi_f : M \to \mathrm{Hom}_S(N, P)$ by $m \mapsto \varphi_{f,m}$. Then, $\varphi_f(m_1 + m_2)(n) = \varphi_{f,m_1+m_2}(n) = f(n \otimes (m_1 + m_2)) = f(n \otimes m_1) + f(n \otimes m_2) = \varphi_{f,m_1}(n) + \varphi_{f,m_2}(n) = \varphi_f(m_1)(n) + \varphi_f(m_2)(n)$, so φ is a homomorphism. We then have that $(\varphi_f(m).r)(n) = \varphi_f(m)(n.r) = \varphi_{f,m}(n.r) = f((n.r) \otimes m) = f(n \otimes (r.m)) = \varphi_{f,r.m}(n) = \varphi_f(r.m)(n)$, hence $\varphi_f(m).r = \varphi_f(r.m)$, and $\varphi_f \in \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$. Define $\Phi : \mathrm{Hom}_S(N \otimes_R M, P) \to \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$ by $f \mapsto \varphi_f$, which is easily shown to be a homomorphism.

We now define a map in the reverse direction. Let $g \in \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$ and define $\psi_g : N \times M \to P$ by $(n, m) \mapsto (g(m))(n)$, which is clearly biadditive. We then observe that $\psi_g(n.r, m) = g(m)(n.r) = (g(m).r)(n) = g(r.m)(n) = \psi_g(n, r.m)$ since $\mathrm{Hom}_S(N, P)$ is a right R-module. This induces a map $\hat{\psi}_g : N \otimes_R M \to P$ such that $\hat{\psi}_g(n \otimes m) = g(m)(n)$ on generators. Now, define $\Psi : \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P)) \to \mathrm{Hom}_S(N \otimes_R M, P)$ by $g \mapsto \hat{\psi}_g$, which is likewise easily shown to be a homomorphism.

Lastly, we observe that

$$\Psi\Phi g(m)(n) = \Psi\phi_g(m)(n) = \Psi\phi_{g,m}(n) = \Psi g(n \otimes m) = \hat{\psi}_g(n \otimes m) = g(m)(n)$$

and

$$\Phi\Psi f(n \otimes m) = \Phi\hat{\psi}_f(n \otimes m) = \Phi f(m)(n) = \varphi_{f,m}(n) = f(n \otimes m),$$

therefore $\Psi\Phi = 1$ and $\Phi\Psi = 1$. □

In the above theorem, let $\mathcal{F} = N \otimes_R (\cdot)$ and let $\mathcal{G} = \mathrm{Hom}_S(N, \cdot)$ be shorthand for the functors we are dealing with. This means that $\mathcal{F} : \mathcal{R} \to \mathcal{S}$ and $\mathcal{G} : \mathcal{S} \to \mathcal{R}$ where $\mathcal{R}$ is the category of left R-modules, and $\mathcal{S}$ is the category of left S-modules. The adjoint isomorphism then says that there is a natural bijection

$$\mathrm{Hom}_S(\mathcal{F}(M), P) \longleftrightarrow \mathrm{Hom}_R(M, \mathcal{G}(P))$$

for any left R-module M and any left S-module P. This leads us to final definition of this section.

Definition 21.10 (Adjoint Functors)**.** *Let $\mathcal{C}$ and $\mathcal{D}$ be categories, and let $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ and $\mathcal{G} : \mathcal{D} \to \mathcal{C}$ be covariant functors. We say that $\mathcal{F}$ and $\mathcal{G}$ are adjoint functors, if there is a natural isomorphism $\tau : Hom_{\mathcal{D}}(\mathcal{F}(\cdot), \cdot) \to Hom_{\mathcal{C}}(\cdot, \mathcal{G}(\cdot))$ where both of these are viewed as functors $\mathcal{C}^{op} \times \mathcal{D} \to \mathfrak{Sets}$ where $\mathfrak{Sets}$ is the category of sets.*

22. Tensor Product of Algebras

We previously defined a k-algebra in Definition 11.2, and we will now give two additional equivalent definitions.

Definition 22.1 (k-Algebra #2)**.** *A k-algebra is a ring A equipped with a ring map $\eta : k \to Z(A)$, where $Z(A)$ denotes the center of A.*

Lemma 22.2. *Definition 11.2 and Definition 22.1 are equivalent.*

Proof. We begin by assuming Definition 11.2. Define $\eta : k \to Z(A)$ by $\lambda \mapsto \lambda.1_A$, and so we must show that η actually does map into $Z(A)$. Let $\lambda \in k$ and $a \in A$, then

$$a\eta(\lambda) = a.(\lambda.1_A) = \lambda.(a \cdot 1_A) = \lambda.(1_A \cdot a) = (\lambda.1_A).a = \eta(\lambda)a.$$

It is easy to verify that η is indeed a ring map.

Now, assume Definition 22.1 and note that A is a $Z(A)$-module by $Z(A) \times A \to A$ given by $(z, a) \mapsto z.a = za$, which is easily verified. Since we have a ring map $\eta : k \to Z(A)$, then Lemma 5.10 implies that A is a k-module by pullback given by $(\lambda, a) \mapsto \lambda.a = \eta(\lambda)a$. It then follows that $(\lambda.a)b = (\eta(\lambda)a)b = \eta(\lambda)ab = \lambda.(ab)$, and $\eta(\lambda)ab = a\eta(\lambda)b = a.(\lambda.b)$, therefore Definition 11.2 holds. □

In light of all the tensor product work we've done up to this point, it should come as no surprise that our third equivalent definition involves tensor products.

Definition 22.3 (k-Algebra #3)**.** *A k-algebra is a k-module A equipped with k-module maps $\eta : k \to A$ and $\mu : A \otimes_k A \to A$ such that the following three diagrams*

$$\begin{array}{ccc} A \otimes_k A & \xrightarrow{\mu} & A \\ {\scriptstyle \eta \otimes 1}\uparrow & & \uparrow{\scriptstyle id} \\ k \otimes_k A & \xleftarrow{\iota_A} & A \end{array} \qquad \begin{array}{ccc} A \otimes_k A & \xrightarrow{\mu} & A \\ {\scriptstyle 1 \otimes \eta}\uparrow & & \uparrow{\scriptstyle id} \\ A \otimes_k k & \xleftarrow{\iota_A} & A \end{array} \qquad \begin{array}{ccc} A \otimes_k A \otimes_k A & \xrightarrow{\mu \otimes 1} & A \otimes_k A \\ {\scriptstyle 1 \otimes \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes_k A & \xrightarrow{\mu} & A \end{array}$$

commute, where μ is given by $a \otimes b \mapsto ab$ via Proposition 20.4.

Given a k-module A which satisfies Definition 22.3, the above diagrams imply precisely that A is a ring. By following the first two diagrams, we can then define the multiplicative identity in A by $1_A := \eta(1)$, and by following the third diagram tells us that multiplication in A is associative. Explicitly, the first diagram says that $\eta(1)a = a$; the second diagrams says that $a\eta(1) = a$; and the third diagram says that $(ab)c = a(bc)$.

Lemma 22.4. *Let A and B be k-algebras, then $A \otimes_k B$ is a k-algebra by $(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb')$.*

Proof. Let μ_A, μ_B, η_A, and η_B be the appropriate k-modules maps produced by Definition 22.3. Define $\eta : k \to A \otimes_k B$ by $1 \mapsto \eta_A(1) \otimes \eta_B(1) = 1_A \otimes 1_B$. It is easily seen that

$$(A \otimes_k B) \otimes_k (A \otimes_k B) \cong (A \otimes_k A) \otimes_k (B \otimes_k B),$$

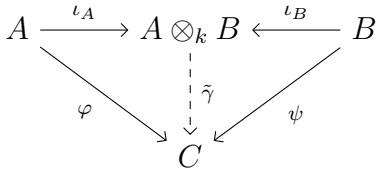
and so define $\mu : (A \otimes_k B) \otimes_k (A \otimes_k B) \to (A \otimes_k A) \otimes_k (B \otimes_k B)$ on generators by

$$(a \otimes b) \otimes (a' \otimes b') \mapsto (\mu_A \otimes \mu_B)((a \otimes a') \otimes (b \otimes b')) = (aa') \otimes (bb').$$

Verifying that the three diagrams commute is easily verified, albeit tedious. □

Proposition 22.5 (Tensor Algebra Universality)**.** *Let A and B be k-algebras. For any k-algebra C and any k-algebra maps $\varphi : A \to C$ and $\psi : B \to C$ such that $\varphi(a)\psi(b) =$*

$\psi(b)\varphi(a)$ for all $a \in A$, $b \in B$, there is a unique k-algebra map $\gamma : A \otimes_k B \to C$ such that the diagram



commutes.

Proof. Define $\gamma : A \times B \to C$ by $(a, b) \mapsto \varphi(a)\psi(b)$, which is clearly biadditive and k-balanced. We then induce a unique map $\tilde{\gamma} : A \otimes_k B \to C$ such that the given diagram commutes. On generators, it follows that $\tilde{\gamma}(a \otimes b) = \varphi(a)\psi(b)$, and so we need only verify that it is a k-algebra map. So,

$$\tilde{\gamma}((a \otimes b) \cdot (a' \otimes b')) = \tilde{\gamma}(aa' \otimes bb') = \varphi(aa')\psi(bb') = \varphi(a)\varphi(a')\psi(b)\psi(b'),$$

and

$$\tilde{\gamma}(a \otimes b)\tilde{\gamma}(a' \otimes b') = \varphi(a)\psi(b)\varphi(a')\psi(b') = \varphi(a)\varphi(a')\psi(b)\psi(b'),$$

hence $\tilde{\gamma}((a \otimes b) \cdot (a' \otimes b')) = \tilde{\gamma}(a \otimes b)\tilde{\gamma}(a' \otimes b')$. Lastly, $\tilde{\gamma}(1 \otimes 1) = \varphi(1)\psi(1) = 1$, and so $\tilde{\gamma}$ is a k-algebra map. □

Lemma 22.6. *Let K be a commutative k-algebra and let B be a k-algebra, then $K \otimes_k B$ is a K-algebra.*

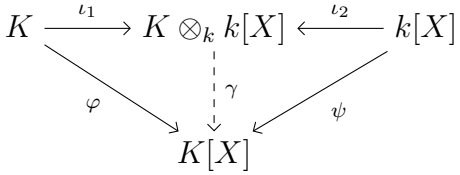
Proof. By Lemma 22.4, we know that $K \otimes_k B$ is a k-algebra, and so $K \otimes_k B$ is a ring by Definition 22.1. Define a map $\eta : K \to K \otimes_k B$ by $x \mapsto x \otimes 1_B$, which is a ring map since $\eta(xy) = (xy) \otimes 1_B = (x \otimes 1_B) \cdot (y \otimes 1_B) = \eta(x)\eta(y)$ and $\eta(x + y) = (x + y) \otimes 1_B = x \otimes 1_B + y \otimes 1_B = \eta(x) + \eta(y)$. To prove that $K \otimes_k B$ is a K-algebra, we need only show that $x \otimes 1_B \in Z(K \otimes_k B)$. Let $y \otimes b$ be a simple tensor in $K \otimes_k B$, then

$$(y \otimes b) \cdot (x \otimes 1_B) = (yx) \otimes (b1_B) = (xy) \otimes (1_B b) = (x \otimes 1_B) \cdot (y \otimes b),$$

therefore $K \otimes_k B$ is a K-algebra. □

Theorem 22.7. *Let K be a field extension of k, i.e. K/k, then $K \otimes_k k[X] \cong K[X]$ as K-algebras.*

Proof. Define a set map $f : \{X\} \to K \otimes_k k[X]$ by $X \mapsto 1 \otimes X$, and so there is a unique K-algebra map $\epsilon : K[X] \to K \otimes_k k[X]$ such that $f = \epsilon \circ \iota$. Furthermore, define maps $\varphi : K \to K[X]$ and $\psi : k[X] \to K[X]$ by inclusion, then this induces a K-algebra map $\gamma : K \otimes_k k[X] \to K[X]$ by Proposition 22.5 such that the diagram



commutes. At this point, we need only verify that $\epsilon\gamma = 1$ and $\gamma\epsilon = 1$ to make the desired conclusion.

First, however, we note that $\{1, X, X^2, \dots\}$ is a k-basis of $k[X]$ and $\{1\}$ is a K-basis of K, and so by Corollary 20.20, it follows that $\{1 \otimes 1, 1 \otimes X, 1 \otimes X^2, \dots\}$ is a K-basis for $K \otimes_k k[X]$. Moreover, we note that $(1 \otimes X) \cdot (1 \otimes X) = 1 \otimes X^2$, and by induction $\{1 \otimes 1, 1 \otimes X, 1 \otimes X^2, \dots\} = \{(1 \otimes X)^i\}_{i=0}^{\infty}$. This means that we need only concern ourselves with $1 \otimes X$ to verify that $\epsilon\gamma = 1$. And so,

$$\epsilon\gamma(1 \otimes X) = \epsilon(\varphi(1)\psi(X)) = \epsilon(X) = 1 \otimes X,$$

and

$$\gamma\epsilon(X) = \gamma(1 \otimes X) = \varphi(1)\psi(X) = X,$$

therefore $K \otimes_k k[X] \cong K[X]$ as K-algebras. □

Example 22.8. *Let $\mathbb{C}/\mathbb{R}$ be a field extension, then by Theorem 22.7, it follows that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X] \cong \mathbb{C}[X]$.*

Theorem 22.9. *Let Y be an abelian group. If $X' \xrightarrow{u} X \xrightarrow{v} X'' \to 0$ is an exact sequence of abelian groups, then $0 \to Hom(X'', Y) \xrightarrow{v^*} Hom(X, Y) \xrightarrow{u^*} Hom(X', Y)$ is exact. Furthermore, if the Hom sequence is exact for all abelian groups Y, then the sequence of X's is exact.*

Proof. We will first prove the forward direction. Let $f \in \mathrm{Ker}(v^*)$, hence $f \circ v = 0$, and so $\mathrm{Im}(v) \subset \mathrm{Ker}(f)$; however $\mathrm{Im}(v) = X''$, thus $\mathrm{Ker}(f) = X''$, therefore $f = 0$ and v^* is injective. Now, let $f \in \mathrm{Im}(v^*)$, so there is $h \in \mathrm{Hom}(X'', Y)$ such that $v^*(h) = f$, hence $h \circ v = f$. Let $x \in \mathrm{Im}(u) = \mathrm{Ker}(v)$, so $v(x) = 0$ and $hv(x) = h(0) = 0$, hence $f(x) = 0$, so $x \in \mathrm{Ker}(f)$. This means that $\mathrm{Im}(u) \subset \mathrm{Ker}(f)$, so $0 = f \circ u = u^*(f)$ and $f \in \mathrm{Ker}(u^*)$, thus $\mathrm{Im}(v^*) \subset \mathrm{Ker}(u^*)$.

Now, let $f \in \mathrm{Ker}(u^*)$, hence $u^*(f) = 0$ so $f \circ u = 0$. Define $h : X'' \to Y$ by $x'' \mapsto f(x)$ where $v(x) = x''$ since v is surjective. To show that h is well-defined, suppose $x'' = v(a) = v(b)$, then $v(a - b) = 0$, so $a - b \in \mathrm{Ker}(v) = \mathrm{Im}(u)$, hence there is $x' \in X'$ such that $u(x') = a - b$. Then, $0 = fu(x') = f(a - b) = f(a) - f(b)$, so $f(a) = f(b)$, and h is well-defined; likewise, h is clearly a homomorphism. It then follows that $v^*(h)(x) = hv(x) = f(x)$, therefore $\mathrm{Ker}(u^*) = \mathrm{Im}(v^*)$.

(Not sure how to do the other direction...) □

Theorem 22.10 (Right Exactness of Tensor Product)**.** *Let M be a left right R-module and let $N' \xrightarrow{u} N \xrightarrow{v} N'' \to 0$ be an exact sequence of left R-modules. Then,*

$$M \otimes_R N' \xrightarrow{1 \otimes u} M \otimes_R N \xrightarrow{1 \otimes v} M \otimes_R N'' \to 0$$

is exact. In other words, $M \otimes_R (\cdot)$ is right exact.

Proof. Let P be any $\mathbb{Z}$-module. Then, since $N' \to N \to N'' \to 0$ is exact, Theorem 22.9 tells us that

$$0 \to \mathrm{Hom}_R(N'', \mathrm{Hom}_{\mathbb{Z}}(M, P)) \xrightarrow{v^*} \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M, P)) \xrightarrow{u^*} \mathrm{Hom}_R(N', \mathrm{Hom}_{\mathbb{Z}}(M, P))$$

is exact. By the Adjoint Isomorphism Theorem (Theorem 21.9), it follows that

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N'', P) \xrightarrow{(1\otimes v)^*} \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, P) \xrightarrow{(1\otimes u)^*} \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N', P)$$

is exact. Lastly, since P was chosen arbitrarily, then again Theorem 22.9 tells us that

$$M \otimes_R N' \xrightarrow{1\otimes u} M \otimes_R N \xrightarrow{1\otimes v} M \otimes_R N'' \to 0$$

is exact, as desired. □

Definition 22.11 (Flat Modules)**.** *Analogous to Definition 7.4, for F a left R-module, we say that F is flat if $M \otimes_R (\cdot)$ is exact.*

Corollary 22.12. *Let K/k be a field extension and let $f \in k[X]$, then $K \otimes_k \frac{k[X]}{(f)} \cong \frac{K[X]}{(f)}$ as K-algebras.*

Proof. We know that

$$k[X] \xrightarrow{\cdot f} k[X] \xrightarrow{\pi} \frac{k[X]}{(f)} \to 0$$

is exact. Then by Theorems 22.10 and 22.7, it follows that

$$\begin{array}{ccccccc} K \otimes_k k[X] & \xrightarrow{1\otimes \cdot f} & K \otimes_k k[X] & \xrightarrow{1\otimes \pi} & K \otimes_k \frac{k[X]}{(f)} & \longrightarrow & 0 \\ \downarrow \sim & & \downarrow \sim & & & & \\ K[X] & \longrightarrow & K[X] & & & & \end{array}$$

Since the first vertical isomorphism is given by $1 \otimes 1 \mapsto 1$ and the second vertical isomorphism is given by $1 \otimes f \mapsto f$, then exactness of

$$K[X] \xrightarrow{\cdot f} K[X] \longrightarrow K \otimes_k \frac{k[X]}{(f)} \to 0$$

implies that $K \otimes_k \frac{k[X]}{(f)} \cong \frac{K[X]}{(f)}$. □

Example 22.13. *Let $\mathbb{C}/\mathbb{R}$ be a field extension, then $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$.*

Proof. Let $\varphi : \{X\} \to \mathbb{C}$ be a set map given by $X \mapsto i$. This map induces $\tilde{\varphi} : \mathbb{R}[X] \to \mathbb{C}$ such that $\tilde{\varphi}(X) = i$. Let $g \in \mathrm{Ker}(\tilde{\varphi})$ and let $g = q(X^2+1)+r$ by the division algorithm, such that $\deg(r) < 2$. Then $0 = \tilde{\varphi}(g) = \tilde{\varphi}(q \cdot (X^2+1) + r) = \tilde{\varphi}(q)\tilde{\varphi}(X^2+1) + \tilde{\varphi}(r) = \tilde{\varphi}(q)(i^2+1)+\tilde{\varphi}(r) = \tilde{\varphi}(r)$. Since $\deg(r) < 2$, then $r = r_0+r_1X$, hence $0 = \tilde{\varphi}(r) = r_0+r_1 i$, so $r = 0$. It then follows that $\mathrm{Ker}(\tilde{\varphi})$ is a principal ideal generated by X^2+1. By the First Isomorphism Theorem, this implies that $\mathbb{C} \cong \frac{\mathbb{R}[X]}{(X^2+1)}$. We then have by Corollary 22.12 and the Chinese Remainder Theorem that

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \frac{\mathbb{R}[X]}{(X^2+1)} \cong \frac{\mathbb{C}[X]}{(X^2+1)} \cong \frac{\mathbb{C}[X]}{(X+i)(X-i)} \cong \frac{\mathbb{C}[X]}{(X-i)} \times \frac{\mathbb{C}[X]}{(X+i)} \cong \mathbb{C} \times \mathbb{C}.$$

By following $1 \otimes 1$ and $1 \otimes i$ through each isomorphism, we observe that

$$1 \otimes 1 \mapsto 1 \otimes \overline{1} \mapsto \overline{1} \mapsto \overline{1} \mapsto (\overline{1}, \overline{1}) \mapsto (1, 1)$$

and

$$1 \otimes i \mapsto 1 \otimes \overline{X} \mapsto \overline{X} \mapsto \overline{X} \mapsto (\overline{X}, \overline{X}) \mapsto (i, -i),$$

hence the isomorphism is given by $1 \otimes 1 \mapsto (1, 1)$ and $1 \otimes i \mapsto (i, -i)$. □