

9 Sources of Modules

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-11-13

Modules over a commutative ring can be much more complicated than vector spaces. To understand this disparity, we need more mechanisms for producing modules.

9.0 Products and Direct Sums

The product of a family of modules is the “most general” module which admits a homomorphism to each family member. Reversing the maps, the direct sum of a family of modules is the “least specific” module to which each family member admits a homomorphism. Despite this seemingly innocuous change, direct sums are quite unlike products.

9.0.1 Definition. Let J be an index set and let $\{V_j\}_{j \in J}$ be a family of R -modules. The **product** $V := \prod_{j \in J} V_j$ is the Cartesian product of sets with the R -module structure defined componentwise: for any r and s in R , and any $u := (u_j)_{j \in J}$ and $v := (v_j)_{j \in J}$ in V , we have $ru + sv = (ru_j + sv_j)_{j \in J}$. This module structure is precisely the one that makes canonical projection maps $\varpi_j : V \rightarrow V_j$ R -linear.

When $J = \emptyset$, the product $\prod_{j \in J} V_j$ is the zero R -module.

9.0.2 Proposition (Universal mapping property for products). *Let $V := \prod_{j \in J} V_j$ be the product of a family of R -modules. For any R -module W and any family $\{\varphi_j : W \rightarrow V_j\}_{j \in J}$ of R -linear maps, there is a unique R -linear map $\varphi : W \rightarrow V$ such that $\varpi_j \circ \varphi = \varphi_j$ for all $j \in J$.*

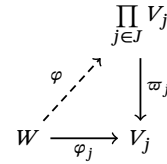


Figure 9.1: Commutative diagram arising from Proposition 9.0.2

Proof. This follows directly from the definitions. $\square$

9.0.3 Remark. Rephrasing this proposition, it follows that, for any R -module W and any family $\{V_j\}_{j \in J}$ of R -modules, the map

$$\mathrm{Hom}_R\left(W, \prod_{j \in J} V_j\right) \rightarrow \prod_{j \in J} \mathrm{Hom}_R(W, V_j)$$

which sends the map $\varphi : W \rightarrow \prod_{j \in J} V_j$ to the family $\{\varpi_j \circ \varphi\}_{j \in J}$ is an R -module isomorphism.

9.0.4 Remark. The product of R -modules is both commutative and associative: for any R -modules U , V , and W , there exists canonical isomorphisms $U \times V \cong V \times U$ and $(U \times V) \times W \cong U \times (V \times W)$.

9.0.5 Definition. Let J be an index set and let $\{V_j\}_{j \in J}$ be a family of R -modules. The **direct sum** $\bigoplus_{j \in J} V_j$ is the submodule of the product $V := \prod_{j \in J} V_j$ consisting of all elements v in V such that $\varpi_j(v) = 0$ for all but finitely many indices j . For any k in J , let $\gamma_k : V_k \rightarrow V$ be the unique map that sends an element v_k in V_k to the element in V satisfying $\varpi_j(\gamma_k(v_k)) = v_k \delta_{j,k}$. By construction, each map γ_k is an injective R -module homomorphism from V_k into $\bigoplus_{j \in J} V_j$. For any v in $\bigoplus_{j \in J} V_j$, we have $v = \sum_{j \in J} (\gamma_j \circ \varpi_j)(v)$.

When $J = \emptyset$, we have $\bigoplus_{j \in J} V_j = 0$.
When the index set J is finite, we also have $\bigoplus_{j \in J} V_j = \prod_{j \in J} V_j$.

9.0.6 Proposition (Universal mapping property for direct sums). *Let $\{V_j\}_{j \in J}$ be a family of R -modules. For any R -module W and any family $\{\psi_j : V_j \rightarrow W\}_{j \in J}$ of R -linear maps, there exists a unique R -linear map $\psi : \bigoplus_{j \in J} V_j \rightarrow W$ such that $\psi \circ \gamma_j = \psi_j$ for all $j \in J$.*

Proof. Suppose that ψ exists. For any v in $\bigoplus_{j \in J} V_j$, we have

$$\psi(v) = \sum_{j \in J} (\psi \circ \gamma_j \circ \varpi_j)(v) = \sum_{j \in J} (\psi_j \circ \varpi_j)(v),$$

whence the uniqueness of ψ . Setting $\psi(v) := \sum_{j \in J} (\psi_j \circ \pi_j)(v)$, one immediately verifies that an R -module homomorphism has been defined satisfying the conditions in the statement. $\square$

9.0.7 Remark. Rephrasing this proposition, it follows that, for any R -module W and any family $\{V_j\}_{j \in J}$ of R -modules, the map

$$\text{Hom}_R\left(\bigoplus_{j \in J} V_j, W\right) \rightarrow \prod_{j \in J} \text{Hom}_R(V_j, W)$$

which sends the map $\varphi : W \rightarrow \bigoplus_{j \in J} V_j$ to the family $\{\varphi \circ \gamma_j\}_{j \in J}$ is an R -module isomorphism.

9.0.8 Remark. The direct sum is also commutative and associative: for any R -modules U , V , and W , there are canonical isomorphisms $U \oplus V \cong V \oplus U$ and $(U \oplus V) \oplus W \cong U \oplus (V \oplus W)$.

9.0.9 Definition. An R -module W is a *direct sum* of a family $\{V_j\}_{j \in J}$ of submodules of W if the canonical R -linear map $\bigoplus_{j \in J} V_j \rightarrow W$ is an isomorphism. This is equivalent to saying that every element w in W can be written uniquely in the form $w = \sum_{j \in J} v_j$ where v_j in V_j for all $j \in J$.

9.0.10 Definition. The submodule of W generated by the union of a family $\{V_j\}_{j \in J}$ of submodules is the *sum* of the family and denoted by $\sum_{j \in J} V_j$. Writing $\gamma_j : V_j \rightarrow W$ for the canonical injection and $\gamma : \bigoplus_{j \in J} V_j \rightarrow W$ for the unique map satisfying $\gamma(v_j) = \sum_{j \in J} \gamma_j(v_j)$, the R -module $\sum_{j \in J} V_j$ is the image of γ .

9.0.11 Proposition. *Let W be an R -module. For any family $\{V_j\}_{j \in J}$ of submodules in W , the following properties are equivalent:*

- The submodule $\sum_{j \in J} V_j$ is the direct sum of the family $\{V_j\}_{j \in J}$.*
- The relation $\sum_{j \in J} v_j = 0$ where $v_j \in V_j$ implies $v_j = 0$ for all $j \in J$.*
- For all $k \in J$, the intersection of V_k and $\sum_{j \neq k} V_j$ is 0.*

Proof.

$a \Leftrightarrow b$: Since $\sum_{j \in J} v_j = \sum_{j \in J} u_j$ if and only if $\sum_{j \in J} (v_j - u_j) = 0$, we see that properties a and b are equivalent.

$a \Rightarrow c$: The uniqueness of the expression for an element in the sum $\sum_{j \in J} V_j$ guarantees that the intersections are 0.

$c \Rightarrow b$: The relation $\sum_{j \in J} v_j = 0$ can be written as $v_k = \sum_{j \neq k} -v_j$ and property c implies that $v_k = 0$. $\square$

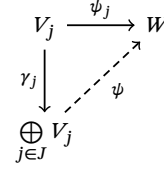


Figure 9.2: Commutative diagrams arising from Proposition 9.0.6

9.1 Exactness

The theory of modules benefits greatly from diagrammatic reasoning. Despite its banal definition, the exactness property is surprisingly useful in this regard.

9.1.1 Definition. Let $\varphi: U \rightarrow V$ and $\psi: V \rightarrow W$ be R -linear maps. The pair (φ, ψ) or the diagram

$$U \xrightarrow{\varphi} V \xrightarrow{\psi} W$$

is an *exact* sequence if $\text{Ker}(\psi) = \text{Im}(\varphi)$. Consider the diagram

$$U \xrightarrow{\varphi} V \xrightarrow{\psi} W \xrightarrow{\theta} X.$$

This diagram is *exact at V* if the pair (φ, ψ) is exact. It is exact at W if the pair (ψ, θ) is exact. If the diagram is exact at each module, it is an exact sequence. Exact sequences with an arbitrary number of terms are defined similarly.

9.1.2 Remarks. The sequence $0 \longrightarrow U \xrightarrow{\varphi} V$ is exact if and only if φ be injective. Similarly, the sequence $U \xrightarrow{\varphi} V \longrightarrow 0$ is exact if and only if φ be surjective.

Suppose that U is a submodule of an R -module V . The canonical inclusion $\iota: U \rightarrow V$ and the canonical surjection $\pi: V \rightarrow V/U$ form the exact sequence $0 \longrightarrow U \xrightarrow{\iota} V \xrightarrow{\pi} V/U \longrightarrow 0$, and any R -module homomorphism $\varphi: U \rightarrow V$ yields the exact sequence

$$0 \longrightarrow \text{Ker}(\varphi) \longrightarrow U \xrightarrow{\varphi} V \longrightarrow \text{Coker}(\varphi) \longrightarrow 0.$$

9.1.3 Proposition. For any submodules U and W of an R -module V , there exists two exact sequences

$$\begin{aligned} 0 \longrightarrow U \cap W &\xrightarrow{\begin{bmatrix} \eta_U \\ \eta_W \end{bmatrix}} U \oplus W \xrightarrow{[\zeta_U \ -\zeta_W]} U + W \longrightarrow 0 \\ 0 \longrightarrow \frac{V}{U \cap W} &\xrightarrow{\begin{bmatrix} \beta_U \\ \beta_W \end{bmatrix}} \frac{V}{U} \oplus \frac{V}{W} \xrightarrow{[\alpha_U \ -\alpha_W]} \frac{V}{U + W} \longrightarrow 0 \end{aligned}$$

where the R -linear maps $\eta_U: U \cap W \rightarrow U$, $\eta_W: U \cap W \rightarrow W$, and $\zeta_U: U \rightarrow U + W$, $\zeta_W: W \rightarrow U + W$ are the canonical injections, the R -linear maps $\beta_U: V/(U \cap W) \rightarrow V/U$ and $\beta_W: V/(U \cap W) \rightarrow V/W$ are induced by the identity map $\text{id}_V: V \rightarrow V$, and the R -linear maps $\alpha_U: V/U \rightarrow V/(U + W)$ and $\alpha_W: V/W \rightarrow V/(U + W)$ are the canonical surjections.

Proof. From the definition of $U + W$, we see that the map $[\zeta_U \ -\zeta_W]$ is surjective. As the maps η_U and η_W are injective, the map $\begin{bmatrix} \eta_U \\ \eta_W \end{bmatrix}$ is also injective. To say that $[\zeta_U \ -\zeta_W](u, w) = 0$ for some u in U and some w in W means that $\zeta_U(u) - \zeta_W(w) = 0$. Thus, there is v in $U \cap W$ such that $v = \zeta_U(u) = \zeta_W(w)$, so $u = \eta_U(v)$ and $w = \eta_W(v)$. We conclude that $\text{Ker}([\zeta_U \ -\zeta_W]) = \text{Im}(\begin{bmatrix} \eta_U \\ \eta_W \end{bmatrix})$.

For the pair (φ, ψ) to form an exact sequence, one must have $\psi \circ \varphi = 0$ because this property yields the inclusion $\text{Im}(\varphi) \subseteq \text{Ker}(\psi)$.

Multiplication by 2 yields the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/\langle 2 \rangle \longrightarrow 0$$

of $\mathbb{Z}$ -modules.

As the maps α_U and α_W are surjective, the map $[\alpha_U - \alpha_W]$ is also surjective. If $[\begin{smallmatrix} \beta_U \\ \beta_W \end{smallmatrix}](v) = 0$ for some v in $V/(U \cap W)$, then we have $\beta_U(v) = \beta_W(v) = 0$ which implies that v is the class of an element in $U \cap W$. To say that $[\alpha_U - \alpha_W](u, w) = 0$ for some u in V/U and some w in V/W means that $\alpha_U(u) = \alpha_W(w)$. Thus, there exists u' and w' in V whose classes modulo U and W are u and w respectively and $u' - w'$ lies in $U + W$. It follows that there are u'' in U and w'' in W such that $u' - w' = u'' - w''$, so there also exists v' in V such that $u' - u'' = w' - w'' = v'$. Let v be the class of the element v' modulo $U \cap W$. Since $\beta_U(v) = u$ and $\beta_W(v) = w$, we see that $\text{Ker}([\alpha_U - \alpha_W]) = \text{Im}([\begin{smallmatrix} \beta_U \\ \beta_W \end{smallmatrix}])$. $\square$

9.1.4 Definition. In an R -module V , the submodules U and W are *complementary* if $V = U \oplus W$.

9.1.5 Example. All submodules of the $\mathbb{Z}$ -module $\mathbb{Z}^1$ have the form $\langle m \rangle$ for some nonnegative integer m , but $\langle m \rangle \cap \langle n \rangle = \langle \text{lcm}(m, n) \rangle$. Thus, $\mathbb{Z}^1$ and 0 are the only complementary submodules in $\mathbb{Z}^1$. $\diamond$

9.1.6 Proposition. When $V = U \oplus W$, the restriction $\pi|_U: U \rightarrow V/W$ of the canonical map $\pi: V \rightarrow V/W$ is an isomorphism.

Proof. The map $\pi|_U$ is surjective because $U + W = V$. It is injective because its kernel is $U \cap W = 0$. $\square$

9.1.7 Proposition. Given an exact sequence of R -modules

$$0 \longrightarrow U \xrightarrow{\varphi} V \xrightarrow{\psi} W \longrightarrow 0,$$

the following are equivalent:

- There exists an R -linear map $\theta: V \rightarrow U$ such that $\theta \circ \varphi = \text{id}_U$.
- There exists an R -linear map $\sigma: W \rightarrow V$ such that $\psi \circ \sigma = \text{id}_W$.
- There exists an isomorphism $V \cong U \oplus W$.

The homomorphisms θ and σ are said to **split** the exact sequence.

Sketch of proof.

$a \Rightarrow c$: For any v in V , we have

$$\theta(v - (\varphi \circ \theta)(v)) = \theta(v) - (\theta \circ \varphi)(\theta(v)) = 0,$$

so $v - (\varphi \circ \theta)(v) \in \text{Ker}(\theta)$ and $V = \text{Ker}(\theta) + \text{Im}(\varphi)$. Consider u in U such that $\varphi(u) \in \text{Ker}(\theta) \cap \text{Im}(\varphi)$. It follows that $0 = \theta(\varphi(u)) = u$, so $\varphi(u) = \varphi(0) = 0$. We conclude that $V \cong \text{Im}(\varphi) \oplus \text{Ker}(\theta)$.

$a \Rightarrow b$: For any w in W , there exists v in V such that $\psi(v) = w$ because ψ is surjective. Define $\sigma: W \rightarrow V$ by $\sigma(w) := v - (\varphi \circ \theta)(v)$.

If $\psi(v) = u = \psi(v')$, then we have $v - v' \in \text{Ker}(\psi) = \text{Im}(\varphi)$, so

$$v - (\varphi \circ \theta)(v) - (v' - (\varphi \circ \theta)(v')) = (v - v') - (\varphi \circ \theta)(v - v')$$

belongs to $\text{Im}(\varphi) \cap \text{Ker}(\theta) = 0$ and the map σ is well-defined. By construction, we have $\psi \circ \sigma = \text{id}_W$.

$c \Rightarrow a$: When $V \cong U \oplus W$, the mapping property of product shows that the canonical surjection $\varpi: V \rightarrow U$ satisfies $\varpi \circ \varphi = \text{id}_U$. $\square$

The characterization of direct sums of submodules implies that U and W are complementary submodules of V if and only if $U + W = V$ and $U \cap W = 0$.

Any two complements of a submodule are isomorphic.

$b \Rightarrow c$ is similar to $a \Rightarrow c$.

$b \Rightarrow a$ is similar to $a \Rightarrow b$.

$c \Rightarrow b$ is similar to $c \Rightarrow a$.

9.2 Free Modules

In analogy with free groups, we identify those modules having only the relations required by the module axioms.

9.2.1 Definition. Let R be a commutative ring. For any index set J , consider the R -module $R^{(J)} := \bigoplus_{j \in J} R^1$. For each $j \in J$ and each canonical map $\gamma_j: R^1 \rightarrow R^{(J)}$, set $e_j := \gamma_j(1_R)$. With this notation, every $r := (r_j) \in R^{(J)}$ may be written uniquely as $r = \sum_{j \in J} r_j e_j$. Let $\varepsilon: J \rightarrow R^{(J)}$ be set map defined by $j \mapsto e_j$.

9.2.2 Lemma. For any R -module V and any map $\xi: J \rightarrow V$, there is a unique R -module homomorphism $\varphi: R^{(J)} \rightarrow V$ such that $\xi = \varphi \circ \varepsilon$.

Proof. The condition $\xi = \varphi \circ \varepsilon$ means that $\varphi(e_j) = \xi(j)$ for all $j \in J$ which is equivalent to $\varphi(r e_j) = r \xi(j)$ for all $r \in R$ and $j \in J$. It also means that the composition $\varphi \circ \gamma_j: R \rightarrow V$ is the R -module homomorphism given by $r \mapsto r \xi(j)$. The proposition is therefore a special case of the mapping property for direct sums. $\square$

9.2.3 Remark. The linear map $\varphi: R^{(J)} \rightarrow V$ is said to be **determined** by the family $\{\xi(j)\}_{j \in J}$ of elements in V . By definition, we have

$$\varphi\left(\sum_{j \in J} r_j e_j\right) = \sum_{j \in J} r_j \xi(j).$$

9.2.4 Definition. A family $\{v_j\}_{j \in J}$ of elements in an R -module V is **linearly independent** (resp. a **basis**) if the R -module homomorphism $R^{(J)} \rightarrow V$ determined by this family is injective (resp. bijective). A module is **free** if it has a basis.

9.2.5 Example. Let m be an integer greater than 1. In the quotient $\mathbb{Z}$ -module $\mathbb{Z}^1 / \langle m \rangle$, no element is linearly independent, so $\mathbb{Z}^1 / \langle m \rangle$ is not a free module. $\diamond$

9.2.6 Example. A free module can have nonzero elements which are not part of a basis. The R -module R^1 is free, but zerodivisors in R are not part of a basis (they are not linearly independent). $\diamond$

9.2.7 Example. Every nonzero element of an R -module can form a linearly independent set without the module being free. The field $\mathbb{Q}$ is a $\mathbb{Z}$ -module with this property: a pair nonzero rational numbers are always linearly dependent. For any a, b, c , and d in $\mathbb{Z}$ with $b \neq 0$ and $d \neq 0$, we have

$$(bc)\frac{a}{b} - (ad)\frac{c}{d} = 0.$$

Hence, a basis could only have at most one element. However, for any q in $\mathbb{Q}$, the set $\{nq \mid n \in \mathbb{Z}\}$ is a proper subset of $\mathbb{Q}$. $\diamond$

9.2.8 Proposition. Let V be a free R -module with basis $\{v_j\}_{j \in J}$. For any family $\{w_j\}_{j \in J}$ of elements in an R -module W , there is a unique R -linear

Compare with Definition 4.2.1.

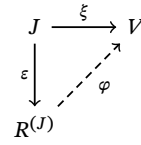


Figure 9.3: Commutative diagram arising from Lemma 9.2.2

When R is a domain and f and g are distinct nonzero elements in R , then set $\{f, g\}$ is linearly dependent because $(-g)f + f(g) = 0$.

map $\psi: V \rightarrow W$ such that $\psi(v_j) = w_j$ for all $j \in J$. The map ψ is injective (resp. surjective) if and only if the family $\{w_j\}_{j \in J}$ of elements in W be a linearly independent (resp. generating set of W).

Proof. This follows from the definitions and Lemma 9.2.2. $\square$

9.2.9 Corollary. Every R -module V is the quotient of a free R -module.

Compare with Proposition 4.3.4.

Proof. When J indexes a generating set of V , there is a surjective R -module homomorphism $R^{(J)} \rightarrow V$. In particular, one may take $J = V$. If U denotes the kernel of this map, then Theorem 8.4.13 shows that the R -module V is isomorphic to $R^{(J)}/U$. $\square$

9.2.10 Corollary. Every exact sequence of R -modules

$$0 \longrightarrow U \xrightarrow{\varphi} V \xrightarrow{\psi} W \longrightarrow 0,$$

in which W is a free R -module, splits. To be precise, if $\{w_j\}_{j \in J}$ is a basis for W , and v_j is an element of V such that $\psi(v_j) = w_j$ for all $j \in J$, then the family $\{v_j\}_{j \in J}$ is linearly independent and generates a complementary submodule of $\varphi(U)$.

Proof. Since W is a free R -module, Proposition 9.2.8 demonstrates that there exists a unique R -module homomorphism $\sigma: W \rightarrow V$ such that $\sigma(w_j) = v_j$ for all $j \in J$ and Proposition 9.1.7 shows that the exact sequence splits. $\square$

With the aim of understanding all free modules, we record the following minor observation.

9.2.11 Lemma. Let K be a field and let $\{u_j\}_{j \in J}$ be linearly independent elements in K -vector space V . Given an element w in V that does not belong to the submodule U generated by $\{u_j\}_{j \in J}$, the family $\{w\} \cup \{u_j\}_{j \in J}$ is linearly independent.

Proof. Suppose that we have a relation $s w + \sum_{j \in J} r_j u_j = 0$ for some s in K , some r_j in K for all $j \in J$, and only finitely many of the r_j are nonzero. If $s \neq 0$, then it would follow that $w = -\sum_{j \in J} (s^{-1} r_j) u_j$ and hence $w \in U$ contrary to hypothesis. Thus, we must have $s = 0$ and the relation becomes $\sum_{j \in J} r_j u_j = 0$ which implies that $r_j = 0$ for all $j \in J$. Since the only relation among the elements is trivial, the family $\{w\} \cup \{u_j\}_{j \in J}$ is linearly independent. $\square$

9.3 Vector Spaces

Characterizing modules over a field, also known as vector spaces, leads to deeper insights into all free modules.

9.3.1 Theorem. *Every module over a field K is a free.*

We must demonstrate that every vector space admits a basis. The following more precise theorem accomplishes this task.

9.3.2 Theorem. *For any generating set $\mathcal{S}$ of a K -vector space V and any linearly independent set $\mathcal{L}$ of V contained in $\mathcal{S}$, there exists a basis $\mathcal{B}$ of V such that $\mathcal{L} \subseteq \mathcal{B} \subseteq \mathcal{S}$.*

Proof of Theorem 9.3.1. The existence of a basis for any vector space V follows from Theorem 9.3.2 by taking $\mathcal{L} = \emptyset$ and $\mathcal{S} = V$. $\square$

Proof of Theorem 9.3.2. Let $\mathcal{E}$ be the set of all linearly independent subsets of V that contain $\mathcal{L}$ and are contained in $\mathcal{S}$. This family is nonempty, because $\mathcal{L} \in \mathcal{E}$. Partially order $\mathcal{E}$ by inclusion. Given a chain $\mathcal{C}$ in $\mathcal{E}$, we claim that $\mathcal{C}^* := \bigcup_{L \in \mathcal{C}} L$ is an upper bound for $\mathcal{C}$. Consider a finite subset $\{u_1, u_2, \dots, u_m\} \subseteq \mathcal{C}^*$. Since $\mathcal{C}$ is a chain, there exists $L \in \mathcal{C}$ such that $\{u_1, u_2, \dots, u_m\} \subseteq L$. Hence, the set $\{u_1, u_2, \dots, u_m\}$ is linearly independent. It follows that every chain in $\mathcal{E}$ has an upper bound. Hence, Zorn's Lemma implies that there is a maximal element $\mathcal{B}$ and Lemma 9.2.11 implies that the submodule $\langle \mathcal{B} \rangle$ is equal to V . $\square$

9.3.3 Corollary. *For any subset $\mathcal{B}$ of a K -vector space V , the following properties are equivalent:*

- $\mathcal{B}$ is a basis of V .
- $\mathcal{B}$ is a maximal linearly independent subset of V .
- $\mathcal{B}$ is a minimal generating set of V .

$\square$

9.3.4 Example. Any ring R containing a field K may be regarded as a K -vector space, so it admits a basis. In particular, every extension field of K has a basis. $\diamond$

The field $\mathbb{R}$ admits an infinite basis as a $\mathbb{Q}$ -vector space.

9.3.5 Theorem. *Two bases of a vector space have the same cardinality.*

Proof. Suppose that V is a vector space with a basis $\mathcal{B}$ of cardinality n for some nonnegative integer n . We show, by induction on n , that every other basis $\mathcal{B}'$ has at most n elements. The claim is trivial for $n = 0$. When $n \geq 1$, the set $\mathcal{B}'$ is nonempty so choose $w \in \mathcal{B}'$. By Theorem 9.3.2, there exists a subset $\mathcal{C} \subseteq \mathcal{B}$ such that $\{w\} \cup \mathcal{C}$ is a basis of V and $w \notin \mathcal{C}$ because $\{w\} \cup \mathcal{B}$ is obviously a generating set for V . As $\mathcal{B}$ is a basis for V , $\mathcal{C} = \mathcal{B}$ is impossible and hence $\mathcal{C}$ has at most $n - 1$ elements. Let U be the subspace generated by $\mathcal{C}$ and W be the subspace generated by $\mathcal{B}' \setminus \{w\}$. Both U and W are

complementary to $\langle w \rangle$ and hence isomorphic. As U admits a basis with at most $n - 1$ elements, $\mathcal{B}' \setminus \{w\}$ has at most $n - 1$ elements by the induction hypothesis. Therefore, $\mathcal{B}'$ has at most n elements.

Next suppose that V has an infinite basis so $V = \prod_{j \in J} V_j$ where J has infinite cardinality. We claim that every generating set has cardinality at least that of J . Let $\mathcal{S}$ be a generating set for V . For each $s \in \mathcal{S}$, let C_s be the finite set of indices $j \in J$ such that the component of s in V_j is nonzero and let $C := \bigcup_{s \in \mathcal{S}} C_s$. Every $s \in \mathcal{S}$ belongs to the submodule $\bigoplus_{j \in C} V_j$; since $\mathcal{S}$ generates V it follows that $C = J$. Since $|J| = |C| \leq |\mathcal{S}|$, the claim follows. $\square$

9.3.6 Definition. Let K be a field. The *dimension* of a K -vector space V is the cardinality of any of the bases of V and denoted by $\dim_K V$.

When $\dim_K V < \infty$, the K -vector space V is finite-dimensional and otherwise it infinite-dimensional.

9.3.7 Lemma. For any family $\{V_j\}_{j \in J}$ of K -vector spaces, we have

$$\dim_K \left(\bigoplus_{j \in J} V_j \right) = \sum_{j \in J} \dim_K V_j.$$

Sketch of proof. When $\mathcal{B}_j$ is a basis for the K -vector space V_j for any $j \in J$, the union $\mathcal{B} := \bigcup_{j \in J} \mathcal{B}_j$ is a basis for $\bigoplus_{j \in J} V_j$. The formula follows because the $\mathcal{B}_j$ are pairwise disjoint. $\square$

9.3.8 Proposition. For any exact sequence of K -vector spaces

$$0 \longrightarrow V_\ell \xrightarrow{\varphi_\ell} V_{\ell-1} \xrightarrow{\varphi_{\ell-1}} \cdots \longrightarrow V_1 \xrightarrow{\varphi_1} V_0 \longrightarrow 0,$$

we have $\sum_{j=0}^{\ell} (-1)^j \dim_R V_j = 0$.

Proof. Setting $U_{-1} := 0$, $U_\ell := 0$, and $U_{j-1} := \text{Im}(\varphi_j) = \text{Ker}(\varphi_{j-1})$ for all $1 \leq j \leq \ell$, we obtain the short exact sequences

$$0 \longrightarrow U_j \longrightarrow V_j \longrightarrow U_{j-1} \longrightarrow 0,$$

Corollary 9.2.10 demonstrates that $V_j = U_j \oplus U_{j-1}$ and Lemma 9.3.7 establishes that $\dim_K V_j = \dim_K U_j + \dim U_{j-1}$. The alternating sum telescopes, so we have

$$0 = \sum_{j=0}^{\ell} (-1)^j (\dim_K U_j + \dim_K U_{j-1}) = \sum_{j=0}^{\ell} (-1)^j \dim_K V_j. \quad \square$$

9.3.9 Corollary. For any nonzero ring R and any free R -module V , any two basis of V have the same cardinality.

Idea of proof. Let I be a maximal ideal in the ring R , let $K := R/I$ be the associated field, and let $\pi: R \rightarrow K$ be the canonical R -linear map. Consider the K -vector space $\pi^*(V) = K \otimes_R V = V/IV$ obtained by extending scalars to K and let $\phi: V \rightarrow \pi^*(V)$ be the map defined by $v \mapsto 1 \otimes v$. Given a basis $\{v_j\}_{j \in J}$ of V , the family $\{\phi(v_j)\}_{j \in J}$ is a basis of $\pi^*(V)$. $\square$

9.3.10 Definition. The cardinality of any basis for a free R -module V is called the *rank* of V and denoted by $\text{rank}_R V$.

9.4 Exercises

9.4.1 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

- i. For any submodule U of K -vector space V , we have

$$\dim_K U + \dim_K V/U = \dim_K V.$$

- ii. For any submodules U and W of a K -vector space V , we have

$$\dim_K(U \cap W) + \dim_K(U + W) = \dim_K(U) + \dim_K(W).$$

9.4.2 Problem.

- i. Let $\varphi: V' \rightarrow V$ and $\psi: V \rightarrow V''$ be R -linear maps. Prove that the sequence

$$V' \xrightarrow{\varphi} V \xrightarrow{\psi} V'' \longrightarrow 0$$

is exact if and only if, for every R -module W , the sequence

$$0 \longrightarrow \operatorname{Hom}_R(V'', W) \xrightarrow{\operatorname{Hom}_R(\psi, W)} \operatorname{Hom}_R(V, W) \xrightarrow{\operatorname{Hom}_R(\varphi, W)} \operatorname{Hom}_R(V', W)$$

is exact.

- ii. Show that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/\langle m \rangle, \mathbb{Z}/\langle n \rangle) \cong \mathbb{Z}/\langle d \rangle$ where $d := \gcd(m, n)$.

9.4.3 Problem. Let K be a field and let U , V , and W be K -vector spaces. Consider K -linear maps $\varphi: U \rightarrow V$ and $\psi: V \rightarrow W$. The map φ has *finite index* if both of the K -modules $\operatorname{Ker}(\varphi)$ and $\operatorname{Coker}(\varphi)$ are finite-dimensional. The *index* of φ is

$$\operatorname{ind}(\varphi) := \dim \operatorname{Ker}(\varphi) - \dim \operatorname{Coker}(\varphi).$$

- i. Prove that U decomposes into a direct sum of $\operatorname{Ker}(\varphi)$ and two K -modules U' and U'' such that $\operatorname{Ker}(\psi \circ \varphi) = \operatorname{Ker}(\varphi) \oplus U'$ and $\operatorname{Im}(\psi \circ \varphi) = \psi(\varphi(U''))$.
- ii. Prove that if two of the three K -linear maps φ , ψ , and $\psi \circ \varphi$ are of finite index, then so is the third and $\operatorname{ind}(\psi \circ \varphi) = \operatorname{ind}(\varphi) + \operatorname{ind}(\psi)$.

Can the false statements be salvaged in some way? In other words, can one find a closely related nontrivial true statement.

Bibliography

- Arnold, Vladimir I. 1998. *On teaching mathematics*, Russian Math. Surveys 53, no. 1, 229–236.
- Cayley, Arthur. 1854. *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$* , Phil. Mag. (4) 42, no. 7, 40–47.
- . 1893. *Note on the so-called quotient G/H in the theory of groups*, Amer. J. Math. 15, no. 4, 387–388.
- Cauchy, Augustin Louis. 1844. *Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*, Exercices d'analyse et de physique mathématique 3, 151–252.
- Chevalley, Claude. 1943. *On the theory of local rings*, Ann. of Math. (2) 44, 690–708.
- Cox, David A. 2011. *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first*, Amer. Math. Monthly 118, no. 1, 3–21.
- Dedekind, Richard. 1871. *Supplement X*, in *Vorlesungen über Zahlentheorie* by Peter Gustav Lejeune Dirichlet, Braunschweig: Vieweg.
- de Groot, Johannes. 1959. *Groups represented by homeomorphism groups*, Math. Ann. 138, 80–102.
- Dyck, Walther. 1882. *Gruppentheoretische Studien*, Math. Ann. 20, no. 1, 1–44.
- Eisenstein, Gotthold. 1850. *Über die Irreducibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39, 160–179.
- Frucht, Roberto. 1939. *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. 6, 239–250.
- Galois, Évariste. 1846. *Œuvres Mathématiques*, J. Math. Pures Appl. XI, 381–444.
- Granville, Andrew. 2024. *It is not "Bézout's identity"*. available at [arXiv:2406.15642](https://arxiv.org/abs/2406.15642) [math.HO].
- Hilbert, David. 1890. *Über die Theorie der algebraischen Formen*, Mathematische Annalen 36, 473–534.
- . 1897. *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4, no. I–XVIII, 175–546.
- Hodges, Wilfrid. 1979. *Krull implies Zorn*, J. London Math. Soc. (2) 19, no. 2, 285–287.
- Jordan, Camille. 1861. *Mémoire sur le nombre des valeurs des fonctions*, Journal de l'École polytechnique 22, 113–194.
- . 1870. *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris. 667 p.
- Klein, Felix. 1884. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig.
- Krull, Wolfgang. 1929. *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Math. Ann. 101, no. 1, 729–744.
- Lagrange, Joseph-Louis. 1771. *Suite des réflexions sur la résolution algébrique des équations. Section troisième. De la résolution des équations du cinquième degré & des degrés ultérieurs*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 5, no. 4, 138–254.
- . 1795. *Leçon Cinquième. Sur l'usage des courbes dans la solution des problèmes*, Leçons Élémentaires sur les Mathématiques. Republished in Serret, Joseph-Alfred, ed. (1877). *Oeuvres de Lagrange*. Vol. 7. Gauthier-Villars. pp. 271–287.
- Miller, George Abram. 1910. *On a method due to Galois*, The Quarterly Journal of Pure and Applied Mathematics 41, 382–384.
- Möbius, August F. 1832. *Über eine besondere Art von Umkehrung der Reihen*, J. Reine Angew. Math. 9, 105–123.
- Noether, Emmy. 1921. *Idealtheorie in Ringbereichen*, Math. Ann. 83, no. 1-2, 24–66.
- . 1927. *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96, no. 1, 26–61.
- Novikov, Pëtr Sergeevich. 1955. *Ob algoritmičeskoj nerazrešimosti problemy toždestva slov v teorii grupp*, Izdat. Akad. Nauk SSSR, Moscow. Trudy Mat. Inst. Steklov. no. 44.

- Poonen, Bjorn. 2019. *Why all rings should have a 1*, Math. Mag. 92, no. 1, 58–62.
- Sabidussi, Gert. 1960. *Graphs with given infinite group*, Monatsh. Math. 64, 64–67.
- Schönemann, Theodor. 1846. *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32, 93–105.
- Smith, Henry J. S. 1861. *On systems of linear indeterminate equations and congruences*, Philos. Trans. Roy. Soc. . 151, 293–32.
- Sylow, Ludwig. 1872. *Théorèmes sur les groupes de substitutions*, Math. Ann. 5, no. 4, 584–594.
- Waring, Edward. 1779. *Problems concerning interpolations*, Philosophical Transactions of the Royal Society 69, 59–67.
- Wielandt, Helmut. 1959. *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. 10, no. 1, 401–402.
- Zorn, Max. 1935. *A remark on method in transfinite algebra*, Bull. Amer. Math. Soc. 41, no. 10, 667–670.