Commutative Algebra
Prof. Fabien Morel
SoSe 2026

Written Notes by Leon Man

Contents

Fehler gerne bei leon.man@campus.lmu.de melden :)

1 Introduction to Commutative Algebra

Unless explicitly stated, R denotes a ring, and all rings are commutative.

1.1 Commutative Rings

1.1.1 Recollection

We recollect already established important facts about rings first.

Definition 1.1.1. A **commutative ring** R is a triple $(R, +, \cdot)$, where $(R, +)$ is an abelian group with neutral element 0_R, $(R, \cdot)$ is a commutative monoid with neutral element 1_R, and *distributivity* holds:

$$\forall a, b, c \in R : a(b + c) = ab + ac.$$

Remark 1.1.2. For $x, y \in R$, $0 \cdot x = 0$ as well as $-(xy) = (-x)y = x(-y)$.

Definition 1.1.3. The **multiplicative group** $R^\times$ of R is defined as $R^\times := \{x \in R \mid \exists y \in R : xy = 1_R\}$. Its elements are called **units** or **invertible elements**. A nonzero commutative ring is called a **field** if $R^\times = R \setminus \{0\}$.

Definition 1.1.4. A map $\varphi : A \to B$ between rings is called a **ring homomorphism** if for $x, y \in A$: $\varphi(xy) = \varphi(x)\varphi(y)$, $\varphi(1_A) = 1_B$, and $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Remark 1.1.5. Given a ring homomorphism $\varphi : A \to B$, $\varphi(A^\times) \subseteq B^\times$. Thus, φ induces a morphism of groups $\varphi^\times := \varphi|_{A^\times} : A^\times \to B^\times$.

Remark 1.1.6. We denote the category of commutative rings as **CRing**. We have already seen two examples of functors **CRing** $\to$ **Ab**: The forgetful functor $R \mapsto (R, +)$ as well as the multiplicative group functor $R \mapsto (R^\times, \cdot)$.

Definition 1.1.7. An element $x \in R \setminus \{0\}$ is called a **zero divisor** if there is a $y \in R \setminus \{0\}$ with $xy = 0$. A commutative ring that has no such elements is called an **integral domain**.

Definition 1.1.8. A subset I of R is called an **ideal** if $(I, +)$ is a subgroup of $(R, +)$ and if given $x \in I$, $y \in R$, $xy \in I$. I is called **proper** if $I \neq R$. We denote the set of proper ideas of R by $\mathcal{I}(R)$.

Remark 1.1.9. We have shown that there is a unique ring structure on the additive quotient group R/I that makes the canonical projection $\pi : R \to R/I$ a ring homomorphism, i.e. for $x, y \in R$ with $\pi(x) := \bar{x}$: $\overline{xy} = \bar{x}\bar{y}$. This structure is called the **quotient ring**.

Definition 1.1.10. Note that $\mathcal{I}(R)$ is partially ordered by inclusion. The maximal elements with respect to this ordering are called **maximal ideals**

Remark 1.1.11. We have shown that an ideal I of R is maximal if and only if R/I is a field.

Definition 1.1.12. Given a family $(x_i)_{i \in J}$ of generators in R, the **generated ideal** $((x_i)_{i \in J})$ is defined as $\{\sum_{i=0}^{n} \lambda_i x_i \mid n \in \mathbb{N},\ \lambda_i \in R\}$. An ideal I is called **finitely generated** if there is a finite J and $(x_i)_{i \in J}$ such that the x_i generate I and **principal** if it can be generated by one. A ring in which every ideal is finitely generated is called **noetherian**. If every ideal is principal, it is called a **principal ideal domain**.

Definition 1.1.13. $x \in R \setminus (R^\times \cup \{0\})$ is called **irreducible** if for $a, b \in R$: $x = ab \implies a \in R^\times$ or $b \in R^\times$, and **prime** if $x \mid ab \implies x \mid a$ or $x \mid b$.

Definition 1.1.14. An ideal $\mathfrak{p} \in \mathcal{I}(R)$ is called **prime** if for $x, y \in R$, $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Remark 1.1.15. In a PID, for $\pi \in R \setminus (\{0\} \cup R^\times)$, the following are equivalent: π prime $\iff$ π irreducible $\iff$ (π) prime $\iff$ $R/(\pi)$ integral domain $\iff$ (π) maximal $\iff$ $R/(\pi)$ field. In particular, every nonzero prime ideal of a PID is maximal.

1.1.2 The Zariski Topology

Definition 1.1.16. The set of prime ideals in R is called the **spectrum** of R. We denote it by $\operatorname{Spec} R$. We denote by $\operatorname{Spec}_{\max} R$ the subset of maximal ideals.

Given $\mathfrak{p} \in \operatorname{Spec} R$, $R/\mathfrak{p}$ is an integral domain, and we write $\kappa(\mathfrak{p}) := \operatorname{Frac} R/\mathfrak{p}$. It is called the **residue field** of $\mathfrak{p}$.

Example 1.1.17. In $\mathbb{Z}$, a prime p generates the prime ideal $(p) =: \mathfrak{p}$. Since $\mathbb{Z}/\mathfrak{p} = \mathbb{F}_p$ is already a field, $\kappa(\mathfrak{p}) = \mathbb{F}_p$. For the prime ideal $0 \in \operatorname{Spec} \mathbb{Z}$, $\kappa(0) = \mathbb{Q}$.

Lemma 1.1.18. Let $\varphi : A \to B$ be a ring homomorphism, $\mathfrak{p} \in \operatorname{Spec} B$. Then, $\varphi^{-1}(\mathfrak{p}) \in \operatorname{Spec} A$.

Proof. Let $\mathfrak{p} \in \operatorname{Spec} B$. Consider the composition $\psi := \pi \circ \varphi : A \to B \twoheadrightarrow B/\mathfrak{p}$. Its kernel consists of elements that are mapped into $\mathfrak{p}$ in B, so it is exactly $\varphi^{-1}(\mathfrak{p}) \subseteq A$. Thus, an isomorphism $A/\varphi^{-1}(\mathfrak{p}) \xrightarrow{\cong} \operatorname{im} \psi \subseteq B/\mathfrak{p}$ is induced, so $A/\varphi^{-1}(\mathfrak{p})$ is isomorphic to a subring of an integral domain, which is still an integral domain. Thus, $\varphi^{-1}(\mathfrak{p}) \in \operatorname{Spec} A$. □

Remark 1.1.19. Recall that a **topology** on a set X is a collection of subsets called open sets, closed under arbitrary unions and finite intersections, and containing $\emptyset$ and X. A **basis** for a topology is a collection $\mathcal{B}$ of open sets such that every open set is a union of elements of $\mathcal{B}$. The **closure** $\overline{A}$ of a subset $A \subset X$ is the smallest closed set containing A, equivalently the intersection of all closed sets containing A.

Definition 1.1.20. Let $f \in R$. The **vanishing locus** $V(f)$ of f in $\operatorname{Spec} R$ is defined as

$$V(f) = \{\mathfrak{p} \in \operatorname{Spec} R \mid f \in \mathfrak{p}\}.$$

It is the set of prime ideals $\mathfrak{p}$ for which f vanishes in the residue field $\kappa(\mathfrak{p})$. We write

$$D(f) = \operatorname{Spec} R \setminus V(f) = \{\mathfrak{p} \in \operatorname{Spec} R \mid f \notin \mathfrak{p}\}.$$

Similarly, given an ideal I in R, we write $V(I) = \bigcap_{f \in I} V(f) = \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\}$, as well as $D(I) = \bigcup_{f \in I} D(f) = \operatorname{Spec} R \setminus V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid I \nsubseteq \mathfrak{p}\}$.

The sets $V(I)$ for an ideal I form the closed sets of a topology called the **Zariski topology**.

Proposition 1.1.21. The Zariski topology is indeed a topology on $\operatorname{Spec} R$ with basis $\mathcal{B} = \{D(f) \mid f \in R\}$.

Proof. We verify that $\mathcal{B} = \{D(f) \mid f \in R\}$ is the basis of a topology. First, $D(1) = \operatorname{Spec} R$ since 1 lies in no prime ideal, so $\mathcal{B}$ covers $\operatorname{Spec} R$. Second, $D(f) \cap D(g) = D(fg)$: a prime ideal $\mathfrak{p}$ avoids both f and g if and only if it avoids fg, by definition of primeness. Hence the intersection of two basis elements is again a basis element, and $\mathcal{B}$ is indeed a basis.

The closed sets of this topology are exactly the sets of the form $V(I)$: a set is closed iff its complement is a union of $D(f)$'s, and $\operatorname{Spec} R \setminus \bigcup_{f \in I} D(f) = \bigcap_{f \in I} V(f) = V(I)$. □

Lemma 1.1.22. Let $\mathfrak{m}$ be a maximal ideal in R and $\mathfrak{p} \in \operatorname{Spec} R$. Then $\mathfrak{p} \neq \mathfrak{m}$ if and only if there exists $f \in \mathfrak{m}$ with $f \notin \mathfrak{p}$.

Proof. The implication ($\Leftarrow$) is clear. For ($\Rightarrow$): if every $f \in \mathfrak{m}$ lies in $\mathfrak{p}$, then $\mathfrak{m} \subseteq \mathfrak{p}$. Since $\mathfrak{m}$ is maximal and $\mathfrak{p}$ is proper, this forces $\mathfrak{m} = \mathfrak{p}$. □

Corollary 1.1.23. For every maximal ideal $\mathfrak{m}$ in R, the singleton $\{\mathfrak{m}\}$ is closed in the Zariski topology.

Proof. By the lemma, $\operatorname{Spec} R \setminus \{\mathfrak{m}\} = \{\mathfrak{p} \in \operatorname{Spec} R \mid \exists f \in \mathfrak{m} : f \notin p\} = \bigcup_{f \in \mathfrak{m}} D(f)$, which is open. □

Remark 1.1.24. More generally, for any $\mathfrak{p} \in \operatorname{Spec} R$, the closure of the singleton is $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$. Indeed, $V(\mathfrak{p})$ is closed and contains $\mathfrak{p}$, and any closed set $V(I)$ containing $\mathfrak{p}$ satisfies $I \subseteq \mathfrak{p}$, hence $V(\mathfrak{p}) \subseteq V(I)$, so $V(\mathfrak{p})$ is the smallest closed set containing $\mathfrak{p}$. In particular, $\mathfrak{p}$ is maximal if and only if $\{\mathfrak{p}\}$ is closed in $\operatorname{Spec} R$ (because every non-maximal $\mathfrak{p} \in \operatorname{Spec} R$ is contained in a maximal ideal, so $V(\mathfrak{p}) \supseteq \{\mathfrak{p}, \mathfrak{m}\}$ already).

Remark 1.1.25. Let $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R$. If $\mathfrak{p} \in \overline{\{\mathfrak{q}\}} = V(\mathfrak{q})$, i.e. $\mathfrak{q} \subseteq \mathfrak{p}$, one says that $\mathfrak{p}$ is a **specialization** of $\mathfrak{q}$.

If R is an integral domain, then $(0) \in \operatorname{Spec} R$ and $\overline{\{(0)\}} = V((0)) = \operatorname{Spec} R$. The ideal (0) is called the **generic point** of $\operatorname{Spec} R$.

Example 1.1.26. $\operatorname{Spec}(\mathbb{Z}) = \{(0)\} \sqcup \{(p) \mid p \in \mathbb{P}\}$. For $f \in \mathbb{Z}$ with prime factorisation $f = \varepsilon p_1^{m_1} \cdots p_s^{m_s}$, we have $V(f) = \{(p_1), \ldots, (p_s)\}$. Hence the open sets of $\operatorname{Spec}(\mathbb{Z})$ are exactly the complements of finite subsets of $\mathbb{P}$ (together with $\varnothing$), and the generic point (0) lies in every nonempty open set.

1.1.3 Localization

Definition 1.1.27. A ring R is called **local** if it has a unique maximal ideal $\mathfrak{m}$. The field $k := R/\mathfrak{m}$ is then called the **residue field** of R. A local PID is called a **discrete valuation ring** (DVR).

Example 1.1.28.

1. Any field K is local with unique maximal ideal (0) and residue field K itself.
2. For a prime p, the ring $\mathbb{Z}_{(p)} := \{a/b \in \mathcal{Q} \mid a, b \in \mathbb{Z},\ \gcd(p, b) = 1\}$ is local with maximal ideal $\mathfrak{m}_p = p\mathbb{Z}_{(p)}$, which is the unique prime ideal other than (0).
3. The evaluation map $\mathrm{ev} : K[[X]] \to K$, $\sum a_i X^i \mapsto a_0$, is a surjective ring homomorphism with kernel (X), so $K[[X]]/(X) \cong K$ is a field and (X) is maximal. To see it is the unique maximal ideal, note that every $f = \sum_{i=0}^{\infty} a_i X^i$ with $a_0 \neq 0$ is a unit: one constructs an inverse $g = \sum b_i X^i$ inductively by $b_0 = a_0^{-1}$ and $b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-i}$. Hence any proper ideal consists entirely of series with zero constant term, i.e. is contained in (X). In particular every maximal ideal is contained in (X), so (X) is the unique maximal ideal, making $K[[X]]$ a local ring.

Lemma 1.1.29. Let R be a ring and $\mathfrak{m} \subset R$ an ideal. Then R is local with maximal ideal $\mathfrak{m}$ if and only if $R^\times = R \setminus \mathfrak{m}$.

Proof. $(\Rightarrow)$: Assume R is local with maximal ideal $\mathfrak{m}$. Every unit lies in no proper ideal, so $R^\times \subseteq R \setminus \mathfrak{m}$. Conversely, if $f \notin \mathfrak{m}$, then $(f) \not\subseteq \mathfrak{m}$, so $(f) = R$ (since $\mathfrak{m}$ is the unique maximal ideal), and f is a unit.

$(\Leftarrow)$: Assume $R^\times = R \setminus \mathfrak{m}$. Then $\mathfrak{m}$ is a proper ideal. If $\mathfrak{m} \subsetneq I \subseteq R$, pick $x \in I \setminus \mathfrak{m}$; then $x \in R^\times$, so $I = R$. Hence $\mathfrak{m}$ is maximal. Any other maximal ideal $\mathfrak{m}'$ contains no unit, so $\mathfrak{m}' \subseteq R \setminus R^\times = \mathfrak{m}$, forcing $\mathfrak{m}' = \mathfrak{m}$. □

Definition 1.1.30. Let R be a ring. A subset $S \subseteq R$ is called **multiplicative** if $1 \in S$ and $s, t \in S \Rightarrow st \in S$, i.e. S is a submonoid of $(R, \times)$.

Remark 1.1.31.

1. If R is an integral domain, $R \setminus \{0\}$ is multiplicative.
2. For any $\mathfrak{p} \in \operatorname{Spec} R$, the complement $S_{\mathfrak{p}} := R \setminus \mathfrak{p}$ is multiplicative: if $f, g \notin \mathfrak{p}$ then $fg \notin \mathfrak{p}$ by primeness.
3. For $f \in R$, the set $S_f := \{f^n \mid n \in \mathbb{N}\}$ is multiplicative.

Definition 1.1.32. Let $S \subseteq R$ be a multiplicative subset. On $S \times R$ (whose elements we write as $\frac{x}{s}$) define the relation

$$\frac{x}{s} \sim \frac{y}{t} \iff \exists\, u \in S : u(tx - sy) = 0.$$

Lemma 1.1.33. This is an equivalence relation on $S \times R$.

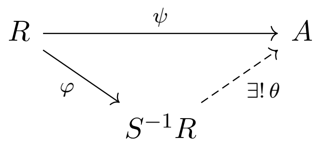
Proof. Reflexivity and symmetry are immediate. For transitivity, suppose $\frac{x_1}{s_1} \sim \frac{x_2}{s_2} \sim \frac{x_3}{s_3}$, so there exist $s, t \in S$ with $s(s_2x_1 - s_1x_2) = 0$ and $t(s_3x_2 - s_2x_3) = 0$. Multiplying the first by ts_3 and the second by ss_1 and adding shows that $sts_2(s_3x_1 - s_1x_3) = 0$, and since $sts_2 \in S$, we get $\frac{x_1}{s_1} \sim \frac{x_3}{s_3}$. □

The **localization** of R at S is $S^{-1}R := (S \times R)/{\sim}$. There is a unique ring structure on $S^{-1}R$ such that

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st}, \qquad \frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st},$$

and the canonical map $\varphi = \varphi_{R,S} : R \to S^{-1}R$, $x \mapsto \frac{x}{1}$, is a ring homomorphism.

Proposition 1.1.34 (Universal property of localisation)**.** Let $\psi : R \to A$ be a ring homomorphism with $\psi(S) \subseteq A^\times$. Then there exists a unique ring homomorphism $\theta : S^{-1}R \to A$ with $\theta \circ \varphi = \psi$, given explicitly by $\theta\left(\frac{x}{s}\right) = \psi(s)^{-1}\psi(x)$. That is, if $\psi(S) \subseteq A^\times$, the following diagram commutes:



Proof. Uniqueness. Any such θ must satisfy $\theta\left(\frac{x}{s}\right) = \theta\left(\frac{x}{1}\right)\theta\left(\frac{1}{s}\right) = \psi(x)\,\psi(s)^{-1}$, which determines θ uniquely.

Existence. Define $\theta\left(\frac{x}{s}\right) := \psi(s)^{-1}\psi(x)$. This is well-defined: if $\frac{x}{s} \sim \frac{y}{t}$ then $\exists\, u \in S$ with $u(tx - sy) = 0$, so $\psi(u)(\psi(t)\psi(x) - \psi(s)\psi(y)) = 0$. Since $\psi(u) \in \psi(S) \subseteq A^\times$, we conclude $\psi(t)\psi(x) = \psi(s)\psi(y)$, hence $\psi(s)^{-1}\psi(x) = \psi(t)^{-1}\psi(y)$. That θ is a ring homomorphism satisfying $\theta \circ \varphi = \psi$ is straightforward to verify. □

Definition 1.1.35. Recall that $S_f = \{f^n \mid n \in \mathbb{N}\}$ is a multiplicative subset. We write $R_f := S_f^{-1}R$ for the localization of R at S_f and call it "R with f inverted".

Lemma 1.1.36. R_f can equivalently be constructed as $R[X]/(fX - 1)$ (i.e. there is a canonical isomorphism).

Proof. Let $A = R[X]/(fX - 1)$ and $\psi : R \to A$ the canonical inclusion. Since $f \cdot X \equiv 1$ in A, the element $\psi(f)$ is a unit with inverse $\bar{X}$, so $\psi(S) \subseteq A^\times$. The universal property then yields a unique ring homomorphism $\theta : R_f \to A$ with $\theta \circ \varphi = \psi$. Conversely, the map $R[X] \to R_f$ fixing R and sending $X \mapsto \frac{1}{f}$ kills $fX - 1$ (since $f \cdot \frac{1}{f} - 1 = 0$ in R_f), so it descends to a ring homomorphism $\bar{\theta} : A \to R_f$. One checks directly that θ and $\bar{\theta}$ are mutually inverse. □

Remark 1.1.37.

1. More generally, for any multiplicative subset $S \subseteq R$,

$$S^{-1}R \;\cong\; R[(X_s)_{s \in S}]\,/(sX_s - 1)_{s \in S}$$

by the same argument.

2. If S is generated as a monoid by $s_1, \ldots, s_n \in R$, then

$$S^{-1}R \;\cong\; R[X_1, \ldots, X_n]/(s_1X_1 - 1, \ldots, s_nX_n - 1).$$

Set $A := R[X_1, \ldots, X_n]/(s_1X_1 - 1, \ldots, s_nX_n - 1)$. Each s_i is a unit in A, and since every element of S is a product of the s_i, the universal property gives $\theta : S^{-1}R \to A$. The inverse sends $X_i \mapsto \frac{1}{s_i}$.

Lemma 1.1.38. Let $f \in R$. Then, R_f is the zero ring if and only if f is nilpotent.

Proof. ($\Rightarrow$): $R_f = 0$ means $\frac{0}{1} = \frac{1}{1}$ in R_f, so there exists $f^N \in S_f$ with $f^N(1 \cdot 1 - 1 \cdot 0) = 0$, i.e. $f^N = 0$ for some $N \in \mathbb{N}$.

($\Leftarrow$): If $f^n = 0$ for some $n \in \mathbb{N}$, then $0 = f^n \in S_f$, so $S_f^{-1}R = 0$ by Remark 3 above. □

Recall that for any prime $\mathfrak{p} \in \operatorname{Spec} R$ the complement $S_\mathfrak{p} := R \setminus \mathfrak{p}$ is a multiplicative subset, and we write $R_\mathfrak{p} := S_\mathfrak{p}^{-1}R$ for the localization of R at $\mathfrak{p}$. The following proposition describes the spectrum of any localization.

Proposition 1.1.39. Let $S \subseteq R$ be a multiplicative subset. The canonical map $\varphi : R \to S^{-1}R$ induces an injective order-preserving map

$$\operatorname{Spec}(\varphi) : \operatorname{Spec}(S^{-1}R) \longrightarrow \operatorname{Spec}(R),$$

whose image is $\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\}$. More precisely, the maps

$$\mathfrak{p} \longmapsto S^{-1}\mathfrak{p}, \qquad \bar{\mathfrak{q}} \longmapsto \varphi^{-1}(\bar{\mathfrak{q}})$$

are mutually inverse bijections between $\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\}$ and $\operatorname{Spec}(S^{-1}R)$.

Proof. First note that for any $\bar{\mathfrak{q}} \in \operatorname{Spec}(S^{-1}R)$ we have $\varphi^{-1}(\bar{\mathfrak{q}}) \cap S = \emptyset$: if $s \in S$ then $s/1$ is a unit in $S^{-1}R$, hence $s/1 \notin \bar{\mathfrak{q}}$, so $s \notin \varphi^{-1}(\bar{\mathfrak{q}})$. Thus $\operatorname{Spec}(\varphi)$ lands in the claimed subset.

Next, for any $\mathfrak{p} \in \operatorname{Spec}(R)$ with $\mathfrak{p} \cap S = \emptyset$, the ideal $S^{-1}\mathfrak{p} = \{x/s \in S^{-1}R \mid x \in \mathfrak{p}\}$ is prime in $S^{-1}R$: if $(x/s)(y/t) \in S^{-1}\mathfrak{p}$ then $xy/st = p/u$ for some $p \in \mathfrak{p}$, $u \in S$, so $\exists v \in S$ with $v(uxy - pst) = 0$, giving $vuxy \in \mathfrak{p}$. Since $vu \in S$ and $\mathfrak{p} \cap S = \emptyset$, $vu \notin \mathfrak{p}$, so $xy \in \mathfrak{p}$, hence $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Moreover $\varphi^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$: the inclusion $\mathfrak{p} \subseteq \varphi^{-1}(S^{-1}\mathfrak{p})$ is clear, and if $x/1 \in S^{-1}\mathfrak{p}$ then $x \in \mathfrak{p}$.

Finally, for any $\bar{\mathfrak{q}} \in \operatorname{Spec}(S^{-1}R)$ we have $S^{-1}\varphi^{-1}(\bar{\mathfrak{q}}) = \bar{\mathfrak{q}}$: if $x/s \in \bar{\mathfrak{q}}$ then $s/1$ is a unit so $x/1 = (s/1)(x/s) \in \bar{\mathfrak{q}}$, hence $x \in \varphi^{-1}(\bar{\mathfrak{q}})$ and $x/s \in S^{-1}\varphi^{-1}(\bar{\mathfrak{q}})$. The reverse inclusion is clear. Thus the two maps are mutually inverse. □

Corollary 1.1.40. For every $\mathfrak{p} \in \operatorname{Spec}(R)$, the ring $R_\mathfrak{p}$ is local with unique maximal ideal $\mathfrak{m}_\mathfrak{p} := S_\mathfrak{p}^{-1}\mathfrak{p} = \{x/s \in R_\mathfrak{p} \mid x \in \mathfrak{p}\}$.

Proof. By the proposition, $\operatorname{Spec}(R_\mathfrak{p}) \cong \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \cap S_\mathfrak{p} = \emptyset\} = \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\}$. Under this bijection $\mathfrak{m}_\mathfrak{p}$ corresponds to $\mathfrak{p}$ itself, which is the unique maximal element of $\{\mathfrak{q} \subseteq \mathfrak{p}\}$. Hence $\mathfrak{m}_\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$. □

Definition 1.1.41. Let R be a commutative ring. The **nilradical** of R is

$$\operatorname{Nil}(R) := \{f \in R \mid \exists n \geq 1 : f^n = 0\}.$$

The **Jacobson radical** of R is

$$\operatorname{Jac}(R) := \bigcap_{\mathfrak{m} \in \operatorname{Spec}_{\max}(R)} \mathfrak{m}.$$

One has $\operatorname{Nil}(R) \subseteq \operatorname{Jac}(R) \subseteq R$.

Corollary 1.1.42. Let R be a commutative ring. Then

$$\operatorname{Nil}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}.$$

Proof. If $f \in \text{Nil}(R)$, say $f^n = 0$, then $f^n \in \mathfrak{p}$ for every prime $\mathfrak{p}$, and since $\mathfrak{p}$ is prime, $f \in \mathfrak{p}$. Thus $\text{Nil}(R) \subseteq \bigcap_{\mathfrak{p}} \mathfrak{p}$.

Conversely, suppose $f \notin \text{Nil}(R)$, i.e. f is not nilpotent. Then $R_f \neq 0$ by the previous lemma, so R_f has at least one prime ideal $\bar{\mathfrak{q}}$. By the proposition, $\mathfrak{p} := \varphi^{-1}(\bar{\mathfrak{q}}) \in \text{Spec}(R)$ satisfies $\mathfrak{p} \cap S_f = \emptyset$, which means $f \notin \mathfrak{p}$. Hence $f \notin \bigcap_{\mathfrak{p}} \mathfrak{p}$. □

Proposition 1.1.43. Let $\mathfrak{p} \in \text{Spec}(R)$. Define $\kappa(\mathfrak{p}) := R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$. Then

$$\kappa(\mathfrak{p}) \;\cong\; \text{Frac}(R/\mathfrak{p}).$$

Proof. The composition $\pi \circ \varphi : R \to R_{\mathfrak{p}} \twoheadrightarrow R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ has kernel $\varphi^{-1}(\mathfrak{m}_{\mathfrak{p}}) = \mathfrak{p}$, yielding an injection $\bar{\varphi} : R/\mathfrak{p} \hookrightarrow R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$. Since every $s \notin \mathfrak{p}$ satisfies $s/1 \notin \mathfrak{m}_{\mathfrak{p}}$, hence $\bar{\varphi}(\bar{s})$ is a unit in the field $R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$, the universal property of the fraction field gives a ring homomorphism $\theta : \text{Frac}(R/\mathfrak{p}) \to R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ extending $\bar{\varphi}$. It is injective since it is a nonzero homomorphism between fields, and surjective since any $\alpha \in R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ is the image of some x/s with $x \in R$, $s \notin \mathfrak{p}$, giving $\alpha = \bar{\varphi}(\bar{x}) \cdot \bar{\varphi}(\bar{s})^{-1} = \theta(\bar{x}/\bar{s})$. □

Proposition 1.1.44. Let R be a PID and $S \subseteq R$ a multiplicative subset. Then $S^{-1}R$ is a PID (and thus a DVR).

Proof. Let $\mathfrak{a} \subseteq S^{-1}R$ be an ideal, and set $I = \varphi^{-1}(\mathfrak{a})$, which is an ideal in R. Since R is a PID, $I = (a)$ for some $a \in R$. We claim $\mathfrak{a} = (a/1)$. The inclusion $(a/1) \subseteq \mathfrak{a}$ is clear. Conversely, if $x/s \in \mathfrak{a}$, then since $1/s$ is a unit in $S^{-1}R$, we have $x/1 = (s/1)(x/s) \in \mathfrak{a}$, so $x \in I = (a)$, say $x = ra$, and thus $x/s = (r/s)(a/1) \in (a/1)$. □

1.1.4 Krull Dimension

Definition 1.1.45. We say that an ascending chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ in R has length r. Let $\mathfrak{p} \in \text{Spec}\, R$. The **height** $\text{ht}(\mathfrak{p})$ is the supremum of lengths of strictly ascending chains of primes contained in it:

$$\text{ht}(\mathfrak{p}) = \sup\{n \in \mathbb{N} \mid \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p},\, \mathfrak{p}_i \in \text{Spec}\, R\}$$

The **Krull dimension** $\dim R$ of R is the supremum of the heights of all prime ideals:

$$\dim R = \sup_{\mathfrak{p} \in \text{Spec}\, R} \text{ht}(\mathfrak{p}).$$

Example 1.1.46.

1. If k is a field, $\text{Spec}\, k = \{(0)\}$, so $\dim k = 0$.
2. Let R be a PID that is not a field. Then, $\text{Spec}\, R = \{(0)\} \cup \{(\pi) \mid \pi \text{ prime in } R\}$. Since in PIDs, ideals generated by prime elements are maximal, there cannot be nontrivial prime ideals $\mathfrak{p}, \mathfrak{q}$ with $\mathfrak{p} \subsetneq \mathfrak{q}$, so $\dim R = 1$. In particular, this holds for $\mathbb{Z}$ and any of its localizations, $k[X]$, and arbitrary DVRs.
3. If R is an integral domain, $R[X_1, \ldots X_n]$ contains the ascending chain $0 \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \ldots, X_n)$, so $\dim(R[X_1 \ldots X_n]) \geq n$.
4. By Proposition 1.1.39, given a multiplicative subset S of R, $\text{Spec}\, S^{-1}R$ injects into $\text{Spec}\, R$ in an order-preserving way. Thus, any ascending chain in $S^{-1}R$ corresponds to an ascending chain of equal length in R. Thus, $\dim S^{-1}R \leq \dim R$.
5. Given a surjective ring homomorphism $\pi : A \twoheadrightarrow B$ with kernel K, any ascending chain in $B \cong A/K$ pulls back to an ascending chain in A, so $\dim B \leq \dim A$.

Remark 1.1.47. For any $\mathfrak{p} \in \text{Spec}(R)$, the proposition on $\text{Spec}(S^{-1}R)$ gives a bijection between $\text{Spec}(R_{\mathfrak{p}})$ and the primes of R contained in $\mathfrak{p}$. Ascending chains below $\mathfrak{p}$ in R thus correspond directly to chains in $R_{\mathfrak{p}}$, giving

$$\text{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}}).$$

Lemma 1.1.48. Let $\mathfrak{q} \subsetneq \mathfrak{q}'$ be prime ideals of $R[X]$ with $\mathfrak{q} \cap R = \mathfrak{q}' \cap R =: \mathfrak{p}$. Then $\mathfrak{q} = \mathfrak{p}R[X]$.

Proof. Replacing R by $R/\mathfrak{p}$ we may assume R is an integral domain and $\mathfrak{p} = 0$. Set $S := R\setminus\{0\}$; since $S^{-1}(R[X]) = K[X]$ where $K = \mathrm{Frac}(R)$, and $\mathfrak{q} \cap R = 0$ implies $\mathfrak{q} \cap S = \emptyset$, the ideal $\mathfrak{q}K[X]$ is a proper prime of $K[X]$. Likewise $\mathfrak{q}'K[X]$ is proper, and $\mathfrak{q}K[X] \subsetneq \mathfrak{q}'K[X]$. Since $K[X]$ is a PID, every nonzero prime is maximal, so $\mathfrak{q}K[X]$ cannot be properly contained in another proper prime. Hence $\mathfrak{q}K[X] = 0$, and since $K[X]$ is an integral domain, $\mathfrak{q} = 0 = \mathfrak{p}R[X]$. □

Theorem 1.1.49. For any commutative ring R,

$$\dim R + 1 \;\leq\; \dim R[X] \;\leq\; 2\dim R + 1.$$

If R is Noetherian, then $\dim R[X] = \dim R + 1$.

Proof. Lower bound. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a chain in $\mathrm{Spec}(R)$ of length $r = \dim R$. Set $\mathfrak{q}_i := \mathfrak{p}_i R[X]$; since $R[X]/\mathfrak{q}_i \cong (R/\mathfrak{p}_i)[X]$ is an integral domain, each $\mathfrak{q}_i$ is prime, and $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_r$ is a chain of length r. The ideal $\mathfrak{q}_r + (X)$ is prime (as $R[X]/(\mathfrak{q}_r + (X)) \cong R/\mathfrak{p}_r$ is a domain) and strictly contains $\mathfrak{q}_r$, so $\dim R[X] \geq r + 1$.

Upper bound. Let $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ be a chain in $\mathrm{Spec}(R[X])$. Call a step $\mathfrak{q}_i \subsetneq \mathfrak{q}_{i+1}$ good if $\mathfrak{q}_i \cap R \subsetneq \mathfrak{q}_{i+1} \cap R$, and bad otherwise. There are at most $\dim R$ good steps. By the lemma, a bad step forces $\mathfrak{q}_i = (\mathfrak{q}_i \cap R)R[X]$; applying the lemma to both $\mathfrak{q}_i \subsetneq \mathfrak{q}_{i+1}$ and $\mathfrak{q}_{i+1} \subsetneq \mathfrak{q}_{i+2}$ shows two consecutive bad steps cannot occur. Hence there are at most $\dim R + 1$ bad steps, giving $n \leq 2\dim R + 1$. □

Before moving on to modules, we recall some important facts about noetherian rings proven in the tutorials:

Lemma 1.1.50. A ring R is Noetherian if and only if every submodule of a finitely generated R-module is itself finitely generated.

Theorem 1.1.51 (Hilbert's basis theorem)**.** If R is Noetherian, then $R[X]$ is Noetherian. □

Corollary 1.1.52. If R is Noetherian and A is a finitely generated R-algebra, then A is Noetherian. In particular, any such A is of the form $R[X_1, \ldots, X_n]/I$ for some n and some ideal I.

Proof. Since A is a finitely generated R-algebra, there exist $a_1, \ldots, a_n \in A$ such that the evaluation map $R[X_1, \ldots, X_n] \to A$, $X_i \mapsto a_i$, is a surjective ring homomorphism. Setting I to be its kernel gives $A \cong R[X_1, \ldots, X_n]/I$. Applying Hilbert's basis theorem n times, $R[X_1, \ldots, X_n]$ is Noetherian. Since any surjective ring homomorphism $\pi : B \twoheadrightarrow A$ with Noetherian B gives a bijection between ideals of A and ideals of B containing $\ker \pi$ (all of which are finitely generated), A is Noetherian. □

1.2 R-Modules

1.2.1 Recollection

Definition 1.2.1. Let R be a commutative ring. An R-**module** is an abelian group $(M, +)$ equipped with a scalar multiplication $R \times M \to M$, $(\lambda, m) \mapsto \lambda m$, satisfying for all $\lambda, \lambda_1, \lambda_2 \in R$ and $m, m_1, m_2 \in M$:

1. $(\lambda_1\lambda_2)m = \lambda_1(\lambda_2 m)$,
2. $(\lambda_1 + \lambda_2)m = \lambda_1 m + \lambda_2 m$,
3. $\lambda(m_1 + m_2) = \lambda m_1 + \lambda m_2$,
4. $1 \cdot m = m$.

If R is not commutative, one distinguishes **left** and **right** R-modules; for commutative R the two notions coincide.

Example 1.2.2. $\mathbb{Z}$-modules are precisely abelian groups; k-modules for a field k are k-vector spaces; R is an R-module over itself.

Definition 1.2.3. A **morphism of R-modules** $f : M \to N$ is a group homomorphism satisfying $f(\lambda m) = \lambda f(m)$ for all $\lambda \in R$, $m \in M$. We write $\mathrm{Hom}_R(M, N)$ for the set of all such morphisms; it is an abelian group under pointwise addition, and an R-module when R is commutative. The category of R-modules is denoted R-**Mod**. A **sub-R-module** of M is a subgroup $N \subseteq M$ with $\lambda n \in N$ for all $\lambda \in R$, $n \in N$.

Definition 1.2.4. Let M be an R-module and $S \subseteq M$ a subset. The **submodule generated by** S is the smallest submodule of M containing S, given explicitly by

$$\langle S \rangle := \left\{ \sum_{i=1}^{n} r_i s_i \mid n \in \mathbb{N},\ r_i \in R,\ s_i \in S \right\}.$$

We say M is **generated by** S if $\langle S \rangle = M$. The module M is of **finite type** if it admits a finite generating set, equivalently if there exists a surjection $R^n \twoheadrightarrow M$ for some $n \in \mathbb{N}$.

Definition 1.2.5. The **cokernel** of an R-module homomorphism f is $\operatorname{coker} f := N/\operatorname{im}(f)$. This allows us to recover the image as $\operatorname{im} f = \ker(N \to \operatorname{coker} f)$. Clearly, f is surjective if and only if $\operatorname{coker} f$ is trivial.

Definition 1.2.6. The category of R-modules admits all limits and colimits. For a family $(M_i)_{i \in I}$ of R-modules, these are realised as follows.

The **direct product** $\prod_{i \in I} M_i$, with componentwise R-module structure, is the limit, characterised by the natural isomorphism

$$\mathrm{Hom}_R\left(N, \prod_{i \in I} M_i \right) \cong \prod_{i \in I} \mathrm{Hom}_R(N, M_i).$$

The **direct sum** $\bigoplus_{i \in I} M_i \subseteq \prod_{i \in I} M_i$, consisting of tuples with only finitely many nonzero entries, is the colimit, characterised by the natural isomorphism

$$\mathrm{Hom}_R\left(\bigoplus_{i \in I} M_i,\ N \right) \cong \prod_{i \in I} \mathrm{Hom}_R(M_i, N).$$

Definition 1.2.7. An R-module M is **free** if it is isomorphic to a direct sum of copies of R, i.e. $M \cong \bigoplus_{i \in I} R =: R[I]$ for some index set I. Equivalently, M is free if it admits a **basis**: a subset $S \subseteq M$ such that every element of M can be written uniquely as a finite R-linear combination of elements of S. The **rank** of a free R-module $M \cong R^[I]$ is the cardinality $|I|$.

Proposition 1.2.8. For R commutative and nonzero, rank is well-defined.

Proof. Let $\mathcal{I}, \mathcal{I}'$ be index sets with $\bigoplus_{i \in \mathcal{I}} R \cong \bigoplus_{i \in \mathcal{I}'} R$ via some ϕ, and choose a maximal ideal $\mathfrak{m} \trianglelefteq R$. Since ϕ is R-linear, it maps $\mathfrak{m} \cdot \bigoplus_{i \in \mathcal{I}} R = \bigoplus_{i \in \mathcal{I}} \mathfrak{m}$ isomorphically onto $\bigoplus_{i \in \mathcal{I}'} \mathfrak{m}$, and therefore descends to an isomorphism of $R/\mathfrak{m}$-vector spaces

$$\bigoplus_{i \in \mathcal{I}} R/\mathfrak{m} \xrightarrow{\sim} \bigoplus_{i \in \mathcal{I}'} R/\mathfrak{m}.$$

Since $R/\mathfrak{m}$ is a field, isomorphic vector spaces have the same dimension, so $|\mathcal{I}| = |\mathcal{I}'|$. □

1.2.2 Exact Sequences

Definition 1.2.9. A diagram in the category of R-modules

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \dots \xrightarrow{f_n} M_n,\ n \geq 2$$

is an **exact sequence** if $\operatorname{im} f_i = \ker f_{i+1}$ for each $i \in \{1, \dots, n-1\}$. An exact sequence of the form $0 \to M_0 \to M_1 \to M_2 \to 0$ is called a **short exact sequence**; one indexed by $\mathbb{Z}$ a **long exact sequence**.

A **cochain complex** is a sequence indexed by $\mathbb{Z}$, often denoted as (M^*, d)

$$\dots \to M^i \xrightarrow{d^i} M^{i+1} \xrightarrow{d^{i+1}} M^{i+2} \to \dots,$$

satisfying the weaker condition $d^{i+1} \circ d^i = 0$, or equivalently $\operatorname{im} d^i \subseteq \ker d^{i+1}$, for all $i \in \mathbb{Z}$.

For a cochain complex (M^*, δ), we define the **n-th cohomology module**

$$H^n(M^*, \delta) := Z^n/B^n, \quad Z^n := \ker \delta_n, \quad B^n := \operatorname{im} \delta_{n-1}.$$

Example 1.2.10.

1. A diagram $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ being exact means exactly that f is injective, g is surjective and $\operatorname{im} f = \ker g$.

2. An example of a long exact sequence is:

$$\dots \to \mathbb{Z}/4\mathbb{Z} \xrightarrow{f} \mathbb{Z}/4\mathbb{Z} \xrightarrow{f} \mathbb{Z}/4\mathbb{Z} \to \dots$$

with $f : x \mapsto 2x$, since $\ker f = \operatorname{im} f = \{\bar{0}, \bar{2}\}$.

3. A cochain complex (M^*, δ) is a long exact sequence if and only if $H^n(M^*, \delta) = 0$ for all n.

4. Let M be a C^∞-differentiable manifold of dimension n. The De Rham complex (Ω^*_M, δ) is the cochain complex

$$\Omega^0(M) \xrightarrow{\delta^1} \Omega^1(M) \xrightarrow{\delta^2} \Omega^2(M) \xrightarrow{\delta^3} \dots \to \Omega^n(M) \to 0,$$

where $\Omega^0(M) = C^\infty(M, \mathcal{R})$ and $\Omega^k(M)$ denotes the space of smooth k-forms on M. The differential is the exterior derivative; on 0-forms it acts as $\delta^1(f) = df$, where $df \in \Omega^1_M(M)$ is the map $T_M \to \mathcal{R}$. Note that $\Omega^1_M = T^*_M$ is the cotangent bundle, dual to the tangent bundle T_M. The cohomology of this complex is the De Rham cohomology

$$H^*(\Omega^*_M, \delta) = H^*_{\mathrm{dR}}(M).$$

Definition 1.2.11. A **presentation** of an R-module M is an exact sequence of the form

$$L_1 \to L_0 \to M \to 0,$$

where L_0 and L_1 are free R-modules.

We say that M is **of finite presentation** if there are such L_0 and L_1 of finite type.

Remark 1.2.12. Let $L_1 \to L_0 \to M \to 0$ be a presentation of the R-module M.

1. Note that

$$\operatorname{coker}(L_1 \to L_0) = L_0/\operatorname{im}(L_1 \to L_0) = L_0/\ker(L_0 \to M) \cong \operatorname{im}(L_0 \to M) = M,$$

since $L_0 \to M$ is surjective.

2. A choice of basis of L_0 corresponds to a choice of generators of M, and a choice of basis of L_1 corresponds to a choice of generators for the module of relations: the image of $L_1 \to L_0$ is exactly the submodule of L_0 that is killed in passing to M.

3. M always admits the presentation

$$\bigoplus_{\ker \pi} R \to \bigoplus_{M} R \xrightarrow{\pi} M \to 0.$$

Indeed, $\pi : \bigoplus_M R \to M$ sending each basis element $e_m \mapsto m$ is a well-defined surjection, and $\bigoplus_{\ker \pi} R \to \bigoplus_M R$ sending each basis element $e_x \mapsto x$ has image exactly $\ker \pi$, giving exactness.

4. If R is Noetherian, M is of finite type if and only if M is of finite presentation. Indeed: given a surjection $\pi : R^m \twoheadrightarrow M$, the kernel $\ker \pi \subseteq R^m$ is finitely generated since R^m is Noetherian, and so $\ker \pi$ admits a surjection from some R^n, yielding a finite presentation $R^n \to R^m \to M \to 0$. The other direction is clear.

Lemma 1.2.13 (Snake Lemma)**.** Let

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{\varphi} & M_2 & \xrightarrow{\psi} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow[\varphi']{} & N_2 & \xrightarrow[\psi']{} & N_3 & & \end{array}$$

be a commutative diagram in R-**Mod** with exact rows. Then there exists a canonical exact sequence

$$\ker f_1 \longrightarrow \ker f_2 \longrightarrow \ker f_3 \xrightarrow{\partial} \operatorname{coker} f_1 \longrightarrow \operatorname{coker} f_2 \longrightarrow \operatorname{coker} f_3,$$

where the maps on kernels and cokernels are induced by φ, ψ and φ', ψ' respectively, and ∂ is the connecting homomorphism constructed in the proof.

Proof. Construction of ∂. Let $x \in \ker f_3$. Since ψ is surjective, choose $y \in M_2$ with $\psi(y) = x$. By commutativity,

$$\psi'(f_2(y)) = f_3(\psi(y)) = f_3(x) = 0,$$

so $f_2(y) \in \ker \psi' = \operatorname{im} \varphi'$. Since φ' is injective, there exists a unique $n_1 \in N_1$ with $\varphi'(n_1) = f_2(y)$. Define $\partial(x) := \bar{n}_1 \in \operatorname{coker} f_1$

Well-definedness of ∂. If $y' \in M_2$ is another lift of x, then $\psi(y' - y) = 0$, so $y' - y \in \ker \psi = \operatorname{im} \varphi$ by exactness at M_2. Write $y' - y = \varphi(m_1)$. By commutativity, $f_2(y') - f_2(y) = \varphi'(f_1(m_1))$, so the corresponding $n_1' \in N_1$ satisfies $n_1' - n_1 = f_1(m_1) \in \operatorname{im} f_1$, hence $\bar{n}_1' = \bar{n}_1$ in $\operatorname{coker} f_1$. R-linearity of ∂ follows directly from the construction.

Exactness at $\ker f_2$. For im $\subseteq$ ker: if $y = \varphi(m_1)$ with $f_1(m_1) = 0$, then $\psi(y) = 0$ by exactness at M_2. For ker $\subseteq$ im: let $y \in \ker f_2$ with $\psi(y) = 0$, so $y = \varphi(m_1)$ by exactness. Then $\varphi'(f_1(m_1)) = f_2(y) = 0$, and injectivity of φ' gives $m_1 \in \ker f_1$.

Exactness at $\ker f_3$. For im $\subseteq$ ker: if $x = \psi(y)$ with $y \in \ker f_2$, then $f_2(y) = 0$, so $\partial(x) = 0$. For ker $\subseteq$ im: let $x \in \ker f_3$ with $\partial(x) = 0$. Choose a lift y and let $f_2(y) = \varphi'(n_1)$ with $\bar{n}_1 = 0$, so $n_1 = f_1(m_1)$ for some m_1. Then $f_2(y - \varphi(m_1)) = \varphi'(n_1) - \varphi'(f_1(m_1)) = 0$, and $\psi(y - \varphi(m_1)) = x$, so $y - \varphi(m_1) \in \ker f_2$ is a preimage of x.

Exactness at $\operatorname{coker} f_1$. For im $\subseteq$ ker: with $f_2(y) = \varphi'(n_1)$, the image of $\bar{n}_1$ in $\operatorname{coker} f_2$ is $\overline{\varphi'(n_1)} = \overline{f_2(y)} = 0$. For ker $\subseteq$ im: if $\varphi'(n_1) \in \operatorname{im} f_2$, write $\varphi'(n_1) = f_2(y)$ and set $x := \psi(y)$. Then $f_3(x) = \psi'(f_2(y)) = \psi'(\varphi'(n_1)) = 0$, so $x \in \ker f_3$ and $\partial(x) = \bar{n}_1$ by construction.

Exactness at $\operatorname{coker} f_2$. For im $\subseteq$ ker: $\overline{\psi'(\varphi'(n_1))} = 0$ since $\operatorname{im} \varphi' = \ker \psi'$. For ker $\subseteq$ im: let $\bar{n}_2 \in \operatorname{coker} f_2$ with $\psi'(n_2) \in \operatorname{im} f_3$. Write $\psi'(n_2) = f_3(\psi(m_2))$ using surjectivity of ψ. Then $\psi'(n_2 - f_2(m_2)) = 0$, so $n_2 - f_2(m_2) = \varphi'(n_1)$ for some $n_1 \in N_1$, and $\bar{n}_2 = \overline{\varphi'(n_1)}$ in $\operatorname{coker} f_2$. □

Remark 1.2.14. 1. If in the situation of the lemma, φ is injective and ψ' is surjective, we get an exact sequence

$$0 \to \ker f_1 \to \ker f_2 \to \ker f_3 \xrightarrow{\partial} \operatorname{coker} f_1 \to \operatorname{coker} f_2 \to \operatorname{coker} f_3 \to 0.$$

2. Let

$$0 \longrightarrow C_* \longrightarrow D_* \longrightarrow E_* \longrightarrow 0$$

be a short exact sequence of chain complexes, i.e. for each n we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_n & \longrightarrow & D_n & \longrightarrow & E_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} & & \\ 0 & \longrightarrow & C_{n-1} & \longrightarrow & D_{n-1} & \longrightarrow & E_{n-1} & \longrightarrow & 0 \end{array}$$

with exact rows. Then there exists a canonical long exact sequence in homology:

$$\cdots \longrightarrow H_n(C_*) \longrightarrow H_n(D_*) \longrightarrow H_n(E_*) \xrightarrow{\partial} H_{n-1}(C_*) \longrightarrow H_{n-1}(D_*) \longrightarrow H_{n-1}(E_*) \longrightarrow \cdots$$

where the connecting homomorphism ∂ is precisely the one given by the Snake Lemma applied to the diagram above.

1.2.3 Extensions

Definition 1.2.15. Let M, N be R-modules. An **extension of M by N** is a short exact sequence

$$(\mathcal{E}) : 0 \to N \to E \to M \to 0.$$

A **morphism of extensions** from $(\mathcal{E})$ to $(\mathcal{E}') : 0 \to N \to E' \to M \to 0$ is an R-module homomorphism $\varphi : E \to E'$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 0 & \longrightarrow & N & \longrightarrow & E' & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

commute. Two extensions are **equivalent** if there exists such a φ.

Lemma 1.2.16 (Short Five Lemma)**.** Given a commutative diagram of R-modules with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow[i']{} & B' & \xrightarrow[p']{} & C' & \longrightarrow & 0 \end{array}$$

if α and γ are isomorphisms, then so is β.

Proof. Injectivity. Suppose $\beta(b) = 0$. Then $\gamma(p(b)) = p'(\beta(b)) = 0$, so $p(b) = 0$ since γ is injective, hence $b = i(a)$ for some $a \in A$. Then $i'(\alpha(a)) = \beta(i(a)) = 0$, so $\alpha(a) = 0$ since i' is injective, hence $a = 0$ and $b = 0$.

Surjectivity. Let $b' \in B'$. Since γ is surjective, there exists $b \in B$ with $\gamma(p(b)) = p'(b')$, i.e. $p'(b' - \beta(b)) = 0$. Thus $b' - \beta(b) = i'(a')$ for some $a' \in A'$, and since α is surjective, $a' = \alpha(a)$ for some a, giving $b' = \beta(b + i(a))$. □

Notice that the structure of the extension diagram is the same as the diagram from the five lemma. Thus we have shown:

Corollary 1.2.17. Any morphism of extensions is an isomorphism.

Definition 1.2.18. We define $\mathrm{Ext}^1_R(M,N)$ to be the set of equivalence classes $[\mathcal{E}]$ of extensions of M by N, where $(\mathcal{E}) \sim (\mathcal{E}')$ if there exists a morphism of extensions from $(\mathcal{E})$ to $(\mathcal{E}')$.

Definition 1.2.19. Let $(\mathcal{E}) : 0 \to N \xrightarrow{\iota} E \xrightarrow{\pi} M \to 0$ be an extension.

Given a morphism $f : M' \to M$, the **pullback** $f^*(\mathcal{E})$ is the extension

$$0 \to N \xrightarrow{\iota^*} f^*E \xrightarrow{\pi^*} M' \to 0$$

with $f^*E := \{(e,m') \in E \times M' \mid \pi(e) = f(m')\}$, $\iota^*(n) := (\iota(n), 0)$, $\pi^*(e,m') := m'$.

Given a morphism $g : N \to N'$, the **pushforward** $g_*(\mathcal{E})$ is the extension

$$0 \to N' \xrightarrow{\iota_*} g_*E \xrightarrow{\pi_*} M \to 0$$

with $g_*E := \mathrm{coker}(N \xrightarrow{(g,-\iota)} N' \oplus E) = \frac{N' \oplus E}{\{(g(n),-\iota(n)) | n \in N\}}$, $\iota_*(n') := \overline{(n',0)}$, $\pi_*(\overline{(n',e)}) := \pi(e)$. Note that π_* is well-defined on the quotient since $\pi(\iota(n)) = 0$ for all $n \in N$ by exactness of $(\mathcal{E})$.

Proposition 1.2.20. In the situation above, $f^*(\mathcal{E})$ and $g_*(\mathcal{E})$ are indeed extensions.

Proof. We show that the diagrams are exact:

Pullback. Injectivity of ι^*: if $(\iota(n), 0) = (0,0)$ then $\iota(n) = 0$, hence $n = 0$ by injectivity of ι. Surjectivity of π^*: given $m' \in M'$, surjectivity of π yields $e \in E$ with $\pi(e) = f(m')$, so $(e,m') \in f^*E$ and $\pi^*(e,m') = m'$. Exactness at f^*E: if $\pi^*(e,m') = m' = 0$ then $\pi(e) = f(0) = 0$, so $e = \iota(n)$ for some $n \in N$ by exactness of $(\mathcal{E})$, hence $(e,m') = \iota^*(n)$.

Pushforward. Injectivity of ι_*: if $\overline{(n',0)} = \bar{0}$ then $(n',0) = (g(n), -\iota(n))$ for some $n \in N$, so $\iota(n) = 0$, hence $n = 0$ by injectivity of ι, and thus $n' = g(n) = 0$. Surjectivity of π_*: given $m \in M$, take $e \in E$ with $\pi(e) = m$, then $\pi_*(\overline{(0,e)}) = \pi(e) = m$. Exactness at g_*E: if $\pi_*(\overline{(n',e)}) = \pi(e) = 0$ then $e = \iota(n)$ for some $n \in N$, so $\overline{(n',e)} = \overline{(n',\iota(n))} = \overline{(n'-g(n),0)} = \iota_*(n'-g(n))$. □

Remark 1.2.21. These constructions are instances of the categorical notions of pullback and pushout in R-**Mod**: $f^*E = E \times_M M'$ is the universal R-module mapping compatibly to both E and M' over M, while $g_*E = N' \sqcup_N E$ is the universal R-module receiving compatible maps from both N' and E under N.

Remark 1.2.22. Given R-modules M, N and morphisms $f : M' \to M$ and $g : N \to N'$ we obtain the induced pullback and pushforward maps:

$$f^* : \mathrm{Ext}_R(M,N) \to \mathrm{Ext}_R(M',N), \; g_* : \mathrm{Ext}_R(M,N) \to \mathrm{Ext}_R(M,N').$$

There is an abelian group structure on $\mathrm{Ext}_R(M,N)$, which we will examine in the following. We first derive its law of composition: Let $(\mathcal{E}_1), (\mathcal{E}_2) \in \mathrm{Ext}_R(M,N)$, with middle terms E_1 and E_2 respectively. We define $(\mathcal{E}_1) \oplus (\mathcal{E}_2)$ to be the diagram

$$0 \to N \oplus N \to E_1 \oplus E_2 \to M \oplus M \to 0.$$

It is easy to see that $(\mathcal{E}_1) \oplus (\mathcal{E}_2) \in \mathrm{Ext}_R(M \oplus M, N \oplus N)$, i.e. the diagram is exact. We use the obvious canonical maps

$$\Delta : M \to M \oplus M \text{ ("diagonal")} , \nabla : N \oplus N \to N \text{ ("codiagonal")}$$

to get the pushforward of the pullback $\nabla_*(\Delta^*((\mathcal{E}_1) \oplus (\mathcal{E}_2)) := (\mathcal{E}_1) + (\mathcal{E}_2)$

Theorem 1.2.23. The law of composition $+ : \mathrm{Ext}_R(M,N) \times \mathrm{Ext}_R(M,N) \to \mathrm{Ext}_R(M,N)$ induced by the above construction endows $\mathrm{Ext}_R(M,N)$ with the structure of an abelian group with the neutral element being the equivalence class of the trivial extension $0 \to N \to N \oplus M \to M \to 0$.

Proof. Well-definedness. Suppose $[\mathcal{E}_1] = [\mathcal{E}_1']$ via an isomorphism $\phi\colon E_1 \xrightarrow{\sim} E_1'$ of extensions. Then $\phi \oplus \mathrm{id}_{E_2}$ is an isomorphism $\mathcal{E}_1 \oplus \mathcal{E}_2 \cong \mathcal{E}_1' \oplus \mathcal{E}_2$ of extensions of $M \oplus M$ by $N \oplus N$. Since pullback and pushforward are functorial, this induces an isomorphism $[\mathcal{E}_1] + [\mathcal{E}_2] = [\mathcal{E}_1'] + [\mathcal{E}_2]$.

Commutativity. The swap $E_1 \oplus E_2 \xrightarrow{\sim} E_2 \oplus E_1$ is an isomorphism $\mathcal{E}_1 \oplus \mathcal{E}_2 \cong \mathcal{E}_2 \oplus \mathcal{E}_1$ of extensions of $M \oplus M$ by $N \oplus N$. The diagonal $\Delta\colon M \to M \oplus M$ and codiagonal $\nabla\colon N \oplus N \to N$ are both invariant under swapping factors, so $[\mathcal{E}_1] + [\mathcal{E}_2] = [\mathcal{E}_2] + [\mathcal{E}_1]$.

Associativity. This follows from the associativity of direct sums together with the identities $(\mathrm{id} \oplus \Delta) \circ \Delta = (\Delta \oplus \mathrm{id}) \circ \Delta$ and $\nabla \circ (\nabla \oplus \mathrm{id}) = \nabla \circ (\mathrm{id} \oplus \nabla)$, which ensure that the two ways of bracketing a triple sum yield isomorphic extensions.

Neutral element. Let $(\mathcal{T})\colon 0 \to N \to N \oplus M \to M \to 0$ be the trivial (split) extension. We show $[\mathcal{E}] + [\mathcal{T}] = [\mathcal{E}]$.

The pullback $P := \Delta^*(E \oplus (N \oplus M))$ consists of triples (e, n, m) with $e \in E$, $n \in N$, $m \in M$ and $\pi(e) = m$, so m is determined by e. Hence $P \cong E \oplus N$ via $(e, n, m) \mapsto (e, n)$, and the inclusion $N \oplus N \hookrightarrow E \oplus N$ sends $(a, b) \mapsto (i(a), b)$.

Pushing forward along $\nabla\colon (a, b) \mapsto a + b$, we form

$$\nabla_*(E \oplus N) \;=\; (E \oplus N \oplus N) \,/\, \langle (i(a),\, b,\, -(a + b)) : a, b \in N \rangle.$$

Setting $a = 0$ and $b = -n_1$ in the relation shows every class has a representative of the form $(e, 0, n)$. Two such representatives satisfy $(e, 0, n) \sim (e', 0, n')$ if and only if $e' = e + i(a)$ and $n' = n - a$ for some $a \in N$. Therefore the map

$$\psi\colon (e, 0, n) \;\longmapsto\; e + i(n)$$

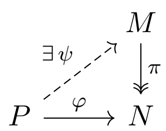
is well-defined on equivalence classes. It is clearly R-linear, and it is bijective: injectivity follows since $\psi(e, 0, n) = \psi(e', 0, n')$ gives $e + i(n) = e' + i(n')$, hence $i(n - n') = e' - e \in \mathrm{im}(i)$, so $n' = n - a$ and $e' = e + i(a)$ for $a = n - n'$, meaning $(e, 0, n) \sim (e', 0, n')$; surjectivity is clear. Finally, the diagram commutes: the inclusion $N \to \nabla_*(E \oplus N)$ sends $n \mapsto [(i(n), 0, 0)]$, and $\psi(i(n), 0, 0) = i(n) + i(0) = i(n)$; the projection $\nabla_*(E \oplus N) \to M$ sends $[(e, 0, n)] \mapsto \pi(e)$, and $\pi(\psi(e, 0, n)) = \pi(e + i(n)) = \pi(e)$. Hence ψ is an isomorphism $[\mathcal{E}] + [\mathcal{T}] \xrightarrow{\sim} [\mathcal{E}]$ of extensions.

Inverses. Define $-[\mathcal{E}] := [(-\mathrm{id}_N)_*\mathcal{E}]$, the pushforward of $\mathcal{E}$ along $-\mathrm{id}_N$. Explicitly, $(-\mathrm{id}_N)_*E = (E \oplus N)/\langle (i(a), a) : a \in N \rangle$, with inclusion $N \to (-\mathrm{id}_N)_*E$ given by $b \mapsto [(0, -b)]$ and projection $[(e, n)] \mapsto \pi(e)$.

One shows $[\mathcal{E}] + (-[\mathcal{E}]) = [\mathcal{T}]$ by an explicit construction analogous to the neutral element case: the pullback $\Delta^*(E \oplus (-\mathrm{id}_N)_*E)$ consists (after choosing lifts) of pairs $(e_1, e_2) \in E \times E$ with $\pi(e_1) = \pi(e_2)$, i.e., $e_1 - e_2 \in \mathrm{im}(i)$. Write $e_1 - e_2 = i(n)$; the assignment $(e_1, e_2) \mapsto (\pi(e_1), n)$ (where n is determined by $e_1 - e_2 = i(n)$ and the injectivity of i) descends after pushing forward along ∇ to an isomorphism of extensions onto $(\mathcal{T})$. □

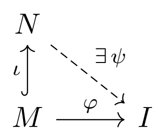
1.2.4 Projective and Injective R-modules

Definition 1.2.24. An R-module P is called **projective** if for any R-modules M and N with an epimorphism $\pi : M \twoheadrightarrow N$ and a map $\varphi : P \to N$, there is a lift $\psi : P \to M$ such that



commutes.

An R-module I is called **injective** if for any M and N with a monomorphism $\iota : M \hookrightarrow N$, and a map $\varphi : M \to I$, there is an extension $\psi : N \to I$ such that the following commutes:



Example 1.2.25. Free modules are always projective: Let S be a set, $R[S] = \bigoplus_{s \in S} R$ the free module over S. Let $\pi : M \twoheadrightarrow N$ be an epimorphism of R-modules and $\varphi : R[S] \to N$.
Notice that

$$\varphi \in \mathrm{Hom}_R(\bigoplus_{s \in S} R, N) \cong \prod_{s \in S} \mathrm{Hom}_R(R, N) \cong \prod_{s \in S} N,$$

because elements $f \in \mathrm{Hom}_R(R, N)$ are uniquely determined by $f(1) \in N$.

Also, π induces a surjection $\prod_{s \in S} M \twoheadrightarrow \prod_{s \in S} N$, where $\prod_{s \in S} M$ is analogously isomorphic to $\mathrm{Hom}_R(\bigoplus_{s \in S} R, M)$. Thus, we get a surjection

$$\Phi : \mathrm{Hom}_R(\bigoplus_{s \in S} R, M) \twoheadrightarrow \mathrm{Hom}_R(\bigoplus_{s \in S} R, N).$$

It is easy to see that any element of the nonempty preimage $\Phi^{-1}(\{\varphi\})$ is a lift $R[S] \to M$.

Lemma 1.2.26. Let P be an R-module. Then, P is projective if and only if it is a summand of a free R-module.

Proof. exercise. □

Example 1.2.27. We give examples of injective modules in R-**Mod**. An abelian group I is called **divisible** if for every $n \in \mathbb{Z} \setminus \{0\}$, the map $\times n \colon I \to I$ is surjective. One may show that in $\mathbf{Ab} = \mathbb{Z}$-**Mod**:

$$I \text{ is injective} \iff I \text{ is divisible.}$$

For the implication divisible $\Rightarrow$ injective: given a diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & I \\ \big\downarrow & & \\ B & & \end{array}$$

with I divisible, consider pairs (C, γ) with $A \subseteq C \subseteq B$ and $\gamma \colon C \to I$ extending f, ordered by extension. By Zorn's lemma there is a maximal such pair (C, γ); we claim $C = B$. If $x \in B \setminus C$, let $k = \min\{n > 0 : nx \in C\}$ if it exists, else $k = 0$. If $k = 0$, any $\alpha \in I$ yields a well-defined extension via $\tilde{\gamma}(c + nx) = \gamma(c) + n\alpha$. If $k > 0$, divisibility gives α with $k\alpha = \gamma(kx)$, and the same formula defines an extension to $C + \mathbb{Z}x \supsetneq C$, contradicting maximality.

1. $\mathbb{Q}$ is injective: given $q \in \mathbb{Q}$ and $n \in \mathbb{Z} \setminus \{0\}$, the element $q/n \in \mathbb{Q}$ satisfies $n \cdot (q/n) = q$, so $\mathbb{Q}$ is divisible.

2. $\mathbb{Q}/\mathbb{Z}$ is injective: given $x = \overline{\frac{a}{b}}$ and $m \in \mathbb{Z} \setminus \{0\}$, take $y = \overline{\frac{a}{mb}}$, so $my = x$, and $\mathbb{Q}/\mathbb{Z}$ is divisible.

3. An injective object I in a category $\mathcal{C}$ is called an *injective cogenerator* if every object $X \in \mathcal{C}$ admits a monomorphism $X \hookrightarrow \prod I$ into a product of copies of I. $\mathbb{Q}/\mathbb{Z}$ is an injective cogenerator of **Ab**: for any $A \in \mathbf{Ab}$ and $a \in A \setminus \{0\}$, injectivity of $\mathbb{Q}/\mathbb{Z}$ yields $\varphi_a \colon A \to \mathbb{Q}/\mathbb{Z}$ with $\varphi_a(a) \neq 0$, so the product map $A \hookrightarrow \prod_{a \neq 0} \mathbb{Q}/\mathbb{Z}$ is injective.

4. The module $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ is injective in R-**Mod**. Given a monomorphism $L \hookrightarrow M$ of R-modules and a map $f \colon L \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$, define $\tilde{f} \colon L \to \mathbb{Q}/\mathbb{Z}$ by $\tilde{f}(l) = f(l)(1)$. By $\mathbb{Z}$-injectivity of $\mathbb{Q}/\mathbb{Z}$, extend $\tilde{f}$ to $\tilde{g} \colon M \to \mathbb{Q}/\mathbb{Z}$, and define $g \colon M \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ by $g(m)(r) := \tilde{g}(rm)$. One checks g is R-linear and extends f.

1.2.5 The Tensor Product

Definition 1.2.28. Let M_1, M_2, N be R-modules. A map $\Phi : M_1 \times M_2 \to N$ is called **R-bilinear** if for $\lambda \in R$, $m_1, m_1' \in M_1$, $m_2, m_2' \in M_2$:

1. $\Phi(\lambda m_1, m_2) = \lambda\Phi(m_1, m_2) = \Phi(m_1, \lambda m_2)$
2. $\Phi(m_1 + m_1', m_2) = \Phi(m_1, m_2) + \Phi(m_1', m_2)$, $\Phi(m_1, m_2 + m_2') = \Phi(m_1, m_2) + \Phi(m_1, m_2')$

We denote by $\mathrm{Bil}_R(M_1, M_2; N)$ the set of R-bilinear maps $M_1 \times M_2 \to N$. It is clearly an R-module.

Bilinear maps to R are called **bilinear forms**.

Example 1.2.29.
1. Let M be an R-module with dual $M^* = \mathrm{Hom}_R(M, R)$. We obtain a bilinear form $M \times M^* \to R, (m, l : M \to R) \mapsto l(m)$. More generally, for R-modules M and N, we get $M \times \mathrm{Hom}_R(M, N) \to N$.
2. Given $M, N, Q \in R\text{-}\mathbf{Mod}$, we get a bilinear map $\mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(N, Q) \to \mathrm{Hom}_R(M, Q)$ by composing.

Remark 1.2.30. For any map $\Phi : M_1 \times M_2 \to N$, define $\tilde{\Phi} : M_1 \to \mathrm{Hom}_R(M_2, N)$ by $m_1 \mapsto \Phi(m_1, -)$. Then Φ is R-bilinear if and only if $\tilde{\Phi}$ is well-defined (i.e. each $\Phi(m_1, -)$ is R-linear) and R-linear as a map $M_1 \to \mathrm{Hom}_R(M_2, N)$. In this way we obtain an isomorphism

$$\mathrm{Bil}_R(M_1, M_2; N) \cong \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, N)).$$

We now construct a structure $M_1 \otimes_R M_2 \in R\text{-}\mathbf{Mod}$ for which $\mathrm{Hom}_R(M_1 \otimes_R M_2, N)$ is also isomorphic to $\mathrm{Bil}_R(M_1, M_2; N)$.

Definition 1.2.31. Let $M, N \in R\text{-}\mathbf{Mod}$. Let $R[M \times N] := \bigoplus_{M \times N} R$ be the free R-module on the set $M \times N$, with basis elements denoted (m, n). Let $\mathcal{R}_{M,N} \subseteq R[M \times N]$ be the submodule generated by the following elements, for all $\lambda \in R$, $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$:

1. $(\lambda m,\, n) - \lambda \cdot (m, n)$
2. $(m,\, \lambda n) - \lambda \cdot (m, n)$,
3. $(m_1 + m_2,\, n) - (m_1, n) - (m_2, n)$,
4. $(m,\, n_1 + n_2) - (m, n_1) - (m, n_2)$.

The **tensor product** of M and N over R is

$$M \otimes_R N \;:=\; R[M \times N] \,/\, \mathcal{R}_{M,N}.$$

For $(m, n) \in M \times N$ we write $m \otimes_R n$ (or simply $m \otimes n$) for the class of (m, n) in $M \otimes_R N$.

Lemma 1.2.32. Let S be a set, $T \subseteq R[S]$ a subset, and $C := R[S]/\langle T \rangle$ the quotient of the free R-module on S by the submodule generated by T. For every R-module Q, restricting along the basis inclusion $S \hookrightarrow R[S]$ induces a bijection

$$\mathrm{Hom}_R(C, Q) \;\cong\; \{\, f \in \mathrm{Hom}_{\mathbf{Set}}(S, Q) \mid \overline{f}(t) = 0 \text{ for all } t \in T \,\},$$

where $\overline{f} \colon R[S] \to Q$ is the unique R-linear map extending f.

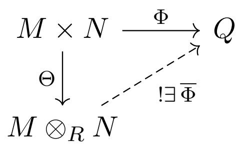
Proof. By the universal property of the quotient, a homomorphism $C \to Q$ is the same as a homomorphism $g \colon R[S] \to Q$ that vanishes on $\langle T \rangle$; and since g is linear, it vanishes on $\langle T \rangle$ iff it vanishes on the generating set T.

By the universal property of the free module, a homomorphism $g \colon R[S] \to Q$ is the same as a map of sets $f \colon S \to Q$, with $g = \overline{f}$ its unique linear extension, so there is an f corresponging to our morphism $C \to Q$ if and only if $g = \overline{f}$ vanishes on T. $\square$

Proposition 1.2.33 (Universal Property of the Tensor Product)**.** Let M, N, Q be R-modules. Let Θ be the canonical map $M \times N \to M \otimes_R N : (m, n) \mapsto m \otimes n$. By precomposing with Θ, we obtain an isomorphism of R-modules

$$\mathrm{Hom}_R(M \otimes_R N, Q) \xrightarrow{\cong} \mathrm{Bil}_R(M, N; Q).$$

In other words, given an R-bilinear map $\Phi \in \mathrm{Bil}_R(M, N; Q)$, there is a unique $\overline{\Phi} \in \mathrm{Hom}_R(M \otimes_R N, Q)$ such that



commutes.

Proof. Recall that $M \otimes_R N$ is defined as the quotient of the free module $R[M \times N]$ by the submodule generated by the subset $\mathcal{R}_{M,N}$. Thus, we can apply the above lemma, yielding a bijection

$$\mathrm{Hom}_R(M \otimes_R N, Q) \xrightarrow{\cong} \{\varphi \in \mathrm{Hom}_{\mathbf{Set}}(M \times N, Q) \mid \bar{\varphi} : R[M \times N] \to Q \text{ vanishes on } \mathcal{R}_{M,N}\}.$$

Let φ be defined as above. Since $\bar{\varphi}$ is the R-linear extension of φ, the equation $\bar{\varphi}(\rho) = 0$ for a generator $\rho \in \mathcal{R}_{M,N}$ is obtained by replacing each (m, n) in ρ with $\varphi(m, n)$. Thus

$$\begin{aligned}
\bar{\varphi}((m + m', n) - (m, n) - (m', n)) = 0 &\iff \varphi(m + m', n) = \varphi(m, n) + \varphi(m', n), \\
\bar{\varphi}((rm, n) - r\,(m, n)) = 0 &\iff \varphi(rm, n) = r\,\varphi(m, n), \\
\bar{\varphi}((m, n + n') - (m, n) - (m, n')) = 0 &\iff \varphi(m, n + n') = \varphi(m, n) + \varphi(m, n'), \\
\bar{\varphi}((m, rn) - r\,(m, n)) = 0 &\iff \varphi(m, rn) = r\,\varphi(m, n),
\end{aligned}$$

which are exactly the conditions that φ be R-bilinear. Hence $\bar{\varphi}$ vanishes on $\mathcal{R}_{M,N}$ if and only if $\varphi \in \mathrm{Bil}_R(M, N; Q)$, and composing with the bijection from the lemma gives $\mathrm{Hom}_R(M \otimes_R N, Q) \cong \mathrm{Bil}_R(M, N; Q)$. □

Remark 1.2.34.

1. An element of $M \otimes_R N$ of the form $m \otimes n$ (with $m \in M$, $n \in N$) is called a **simple tensor**. The simple tensors generate $M \otimes_R N$ as an R-module, being the images of the basis elements (m, n) of $R[M \times N]$ under the canonical surjection $R[M \times N] \to M \otimes_R N$. A general element is a finite sum $\sum_i m_i \otimes n_i$, in general not a single simple tensor.

2. It is clear that $0 \otimes n = n \otimes 0 = 0$ as well as $(-m) \otimes n = -(m \otimes n) = m \otimes (-n)$.

3. By the universal property, an R-linear map $\overline{\Phi}\colon M \otimes_R N \to Q$ corresponds to the R-bilinear map $\Phi\colon M \times N \to Q$ with $\Phi(m, n) = \overline{\Phi}(m \otimes n)$; the values on simple tensors and on pairs coincide. Thus a map out of $M \otimes_R N$ may be defined by prescribing it on simple tensors, $m \otimes n \mapsto \overline{\Phi}(m \otimes n)$, provided the resulting rule on $M \times N$ is bilinear, in which case $\overline{\Phi}$ is uniquely determined.

Proposition 1.2.35. Let M, N be R-modules.

1. If $(m_i)_{i \in I}$ and $(n_j)_{j \in J}$ generate M and N respectively, $M \otimes_R N$ is generated by $(m_i \otimes n_j)_{(i,j) \in I \times J}$. In particular, tensor products of finitely generated modules remain finitely generated.

2. $R \otimes_R N \cong N$ canonically. We treat both sides as being equal.

3. There is an isomorphism $\Psi : M \otimes_R N \xrightarrow{\cong} N \otimes_R M$. However, we do not treat both sides as being equal.

4. Given families of R-modules $(M_i)_{i\in I}$ and $(N_j)_{j\in J}$, there is an isomorphism
$$(\bigoplus_{i\in I} M_i)\otimes_R(\bigoplus_{j\in J} N_j)\xrightarrow{\cong}\bigoplus_{(i,j)\in I\times J} M_i\otimes_R N_j.$$
We treat both sides as being equal. In particular, if M is free of rank m and N is free of rank n, $M\otimes_R N$ is free of rank $m\cdot n$.

5. Given ideals $\mathcal{I}$ and $\mathcal{J}$ in R, $R/\mathcal{I}\otimes_R R/\mathcal{J}\cong R/(\mathcal{I}+\mathcal{J})$.

Proof. 1. Writing $m=\sum_i \lambda_i m_i$ and $n=\sum_j \mu_j n_j$, bilinearity gives $m\otimes n=\sum_{i,j}\lambda_i\mu_j\,(m_i\otimes n_j)$. Hence the $(m_i\otimes n_j)_{(i,j)\in I\times J}$ generate all simple tensors, and thus the entirety of $M\otimes_R N$.

2. The multiplication $R\times N\to N$, $(\lambda,n)\mapsto\lambda n$, is R-bilinear and induces $\mu\colon R\otimes_R N\to N$, $\lambda\otimes n\mapsto\lambda n$. The map $\nu\colon N\to R\otimes_R N$, $n\mapsto 1\otimes n$, is R-linear, and the $1\otimes n$ generate $R\otimes_R N$ by (1), so ν is surjective. Since $\mu\circ\nu=\mathrm{id}_N$, ν is also injective, hence an isomorphism.

3. The map $M\times N\to N\otimes_R M$, $(m,n)\mapsto n\otimes m$, is R-bilinear and induces $\Psi\colon M\otimes_R N\to N\otimes_R M$. The analogous map induces $\Psi'\colon N\otimes_R M\to M\otimes_R N$, and both composites fix simple tensors which generate the entire product hence Ψ is an isomorphism.

4. Write $P=\bigoplus_i M_i$ and abbreviate $\iota_i\colon M_i\to P$ for the canonical inclusions. The map
$$P\times(\textstyle\bigoplus_j N_j)\longrightarrow\bigoplus_{i,j} M_i\otimes_R N_j,\qquad ((m_i)_i,\,(n_j)_j)\longmapsto\sum_{i,j} m_i\otimes n_j,$$
is R-bilinear, so by the universal property it induces an R-linear map
$$\Phi\colon(\bigoplus_i M_i)\otimes_R(\bigoplus_j N_j)\to\bigoplus_{i,j} M_i\otimes_R N_j.$$
Conversely, for each (i,j), the map
$$M_i\otimes_R N_j\to P\otimes_R(\bigoplus_j N_j),\ m_i\otimes n_j\mapsto\iota_i(m_i)\otimes\iota_j(n_j)$$
is induced by a bilinear map; assembling these over all (i,j) via the universal property of the direct sum gives an R-linear map Ψ in the other direction. On simple tensors both composites $\Phi\circ\Psi$ and $\Psi\circ\Phi$ fix the simple tensors, so by 1) they are the identity. Hence Φ is an isomorphism.

5. *(exercise.)*

□

Remark 1.2.36. Both Hom_R and $\otimes_R$ are functorial in each variable; we record how they act on morphisms, as the adjunction and the results below use this.

For Hom, a morphism $f\colon M\to M'$ induces by $f^*(\varphi)=\varphi\circ f$ and $f_*(\varphi)=f\circ\varphi$:
$$f^*=\mathrm{Hom}_R(f,Q)\colon\ \mathrm{Hom}_R(M',Q)\to\mathrm{Hom}_R(M,Q),$$
$$f_*=\mathrm{Hom}_R(Q,f)\colon\ \mathrm{Hom}_R(Q,M)\to\mathrm{Hom}_R(Q,M').$$
We see that $\mathrm{Hom}_R(-,Q)$ is contravariant and $\mathrm{Hom}_R(Q,-)$ is covariant.

For $\otimes$, a morphism $f\colon M\to M'$ should induce $f\otimes\mathrm{id}_N\colon M\otimes_R N\to M'\otimes_R N$ with $m\otimes n\mapsto f(m)\otimes n$. This is not immediate: by the universal property, a rule on simple tensors defines a map out of $M\otimes_R N$ only once the corresponding rule on $M\times N$ is bilinear. Here $(m,n)\mapsto f(m)\otimes n$ is R-bilinear since f is linear and $\otimes$ is bilinear, so the universal property yields $f\otimes\mathrm{id}_N$ as claimed. Symmetrically $g\colon N\to N'$ induces $\mathrm{id}_M\otimes g$, so $-\otimes_R N$ and $M\otimes_R -$ both are covariant.

Remark 1.2.37. Recall the isomorphism $\mathrm{Bil}_R(M,N;Q) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,Q))$, for $M,N,Q \in R$-**Mod**, established in Remark 1.2.30. Composing with the universal property of the tensor product gives a natural isomorphism

$$\mathrm{Hom}_R(M \otimes_R N, Q) \;\cong\; \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,Q)).$$

This is called the **tensor-hom adjunction** between the functors $- \otimes_R N$ and $\mathrm{Hom}_R(N,-)$.

Definition 1.2.38. Let $F\colon R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$ be a covariant functor. We say that F is **left exact** if for every short exact sequence $0 \to A \to B \to C \to 0$, the sequence $0 \to F(A) \to F(B) \to F(C)$ is exact, **right exact** if for every short exact sequence $0 \to A \to B \to C \to 0$, the sequence $F(A) \to F(B) \to F(C) \to 0$ is exact, and **exact** if it is both left and right exact, i.e. if it sends short exact sequences to short exact sequences.

Remark 1.2.39.

1. For a contravariant functor the definition is the same after reversing the arrows: F is **left exact** if it sends $A \to B \to C \to 0$ to the exact sequence $0 \to F(C) \to F(B) \to F(A)$, and similarly for the rest. For instance, the next lemma in particular shows that the contravariant functor $\mathrm{Hom}_R(-,Q)$ is left exact.
2. In the tutorials, it was shown that the Hom-functors in both variables are left exact for arbitrary modules, and that $\mathrm{Hom}(P,-)$ and $\mathrm{Hom}(-,Q)$ are right exact if and only if P is projective/Q is injective.

Lemma 1.2.40. Let $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ be a sequence in R-**Mod**. Then $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is exact if and only if for every R-module Q the sequence

$$0 \to \mathrm{Hom}_R(M_3,Q) \xrightarrow{g^*} \mathrm{Hom}_R(M_2,Q) \xrightarrow{f^*} \mathrm{Hom}_R(M_1,Q),$$

obtained by applying the contravariant functor $\mathrm{Hom}_R(-,Q)$, is exact.

Proof. Note that $f^*(\varphi) = \varphi \circ f$ and $g^*(\psi) = \psi \circ g$.
($\Rightarrow$) Assume $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is exact, i.e. g is surjective and $\mathrm{im}\, f = \ker g$.

Injectivity of g^*. If $g^*(\psi) = \psi \circ g = 0$, then ψ vanishes on $\mathrm{im}\, g = M_3$ (as g is surjective), so $\psi = 0$.

Exactness at $\mathrm{Hom}_R(M_2,Q)$. First, $f^* \circ g^* = (g \circ f)^* = 0$ since $g \circ f = 0$, so $\mathrm{im}\, g^* \subseteq \ker f^*$. Conversely, let $\varphi \in \mathrm{Hom}_R(M_2,Q)$ with $f^*(\varphi) = \varphi \circ f = 0$, i.e. φ vanishes on $\mathrm{im}\, f = \ker g$. Hence φ factors through $M_2/\ker g$. Since g is surjective, the induced map $M_2/\ker g \to M_3$ is an isomorphism, so φ descends to a map $\psi\colon M_3 \to Q$ with $\psi \circ g = \varphi$, that is $\varphi = g^*(\psi) \in \mathrm{im}\, g^*$.

($\Leftarrow$) Assume the displayed sequence is exact for every Q.

g is surjective. Take $Q := \mathrm{coker}\, g = M_3/\mathrm{im}\, g$ and let $\pi\colon M_3 \to Q$ be the projection. Then $g^*(\pi) = \pi \circ g = 0$, and injectivity of g^* forces $\pi = 0$, i.e. $\mathrm{coker}\, g = 0$, so g is surjective.

$\mathrm{im}\, f \subseteq \ker g$. Take $Q := M_3$. Exactness at $\mathrm{Hom}_R(M_2,M_3)$ gives $f^* \circ g^* = 0$; applied to $\mathrm{id}_{M_3} \in \mathrm{Hom}_R(M_3,M_3)$ this yields $f^*(g^*(\mathrm{id}_{M_3})) = g \circ f = 0$, hence $\mathrm{im}\, f \subseteq \ker g$.

$\ker g \subseteq \mathrm{im}\, f$. Take $Q := M_2/\mathrm{im}\, f$ and let $\pi\colon M_2 \to Q$ be the projection, so $f^*(\pi) = \pi \circ f = 0$, i.e. $\pi \in \ker f^*$. By exactness at $\mathrm{Hom}_R(M_2,Q)$ there is $\psi\colon M_3 \to Q$ with $\pi = g^*(\psi) = \psi \circ g$. Then π vanishes on $\ker g$, which means $\ker g \subseteq \ker \pi = \mathrm{im}\, f$.

Together, g is surjective and $\mathrm{im}\, f = \ker g$, i.e. the original sequence is exact. $\square$

Corollary 1.2.41. For every R-module N, the covariant functor $- \otimes_R N$ is right exact.

Proof. Let $M_1 \to M_2 \to M_3 \to 0$ be exact. By the previous lemma applied to

$$M_1 \otimes_R N \to M_2 \otimes_R N \to M_3 \otimes_R N \to 0,$$

it suffices to show that for every R-module Q the sequence

$$0 \to \mathrm{Hom}_R(M_3 \otimes_R N, Q) \to \mathrm{Hom}_R(M_2 \otimes_R N, Q) \to \mathrm{Hom}_R(M_1 \otimes_R N, Q)$$

is exact. By the tensor-hom adjunction, this sequence is naturally isomorphic to

$$0 \to \mathrm{Hom}_R(M_3, \mathrm{Hom}_R(N, Q)) \to \mathrm{Hom}_R(M_2, \mathrm{Hom}_R(N, Q)) \to \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(N, Q)).$$

Setting $Q' := \mathrm{Hom}_R(N, Q)$, this is exactly the sequence obtained by applying $\mathrm{Hom}_R(-, Q')$ to $M_1 \to M_2 \to M_3 \to 0$, which again by the Lemma is exact. $\square$

Remark 1.2.42. In general $- \otimes_R N$ is *not* left exact: it need not preserve injectivity. For example, the injection $\mathbb{Z}/2 \xrightarrow{\cdot 2} \mathbb{Z}/4$ becomes, after applying $- \otimes_{\mathbb{Z}} \mathbb{Z}/2$, the map $\mathbb{Z}/2 \to \mathbb{Z}/2$ sending $\bar{1} \otimes \bar{x} \mapsto \bar{2} \otimes \bar{x} = \bar{1} \otimes \overline{2x} = 0$, i.e. the zero map, which is not injective.

Definition 1.2.43. An R-module N is called **flat** if the functor $- \otimes_R N$ is exact.

Remark 1.2.44. We have shown that $- \otimes_R N$ is always right exact, so the only possible failure of exactness is at the left. Hence N is flat if and only if for every injection $M_1 \hookrightarrow M_2$, $M_1 \otimes_R N \to M_2 \otimes_R N$ is injective.